



Loi 25 au Québec : votre organisation est-elle bien préparée?

En quoi consiste la Loi 25?

La Loi 25 est la nouvelle loi stricte régissant la protection des renseignements personnels au Québec. Elle comprend différentes exigences qui auront une incidence sur les organisations détenant des renseignements personnels de résidents du Québec.

Que devez-vous savoir?

Exigences législatives

Voici quelques-unes des modifications apportées par la Loi 25. L'obligation pour toutes les organisations de :

- Désigner un responsable de la protection des renseignements personnels ou de créer un poste équivalent;
- Définir des politiques et des procédures sur la protection des renseignements personnels;
- Effectuer une évaluation des facteurs relatifs à la vie privée si votre organisation planifie l'un des quatre types de projets suivants :
 - Tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels;
 - Communiquer des renseignements personnels à l'extérieur du Québec;
 - Utiliser des données biométriques;
 - Effectuer des études, de la recherche, de la production de statistiques.
- Signaler à la Commission d'accès à l'information certaines atteintes à la protection des renseignements personnels;
- Démontrer une plus grande transparence en ce qui a trait à la collecte et à l'usage fait des renseignements personnels;
- Mettre en œuvre des principes de confidentialité programmés dans la technologie et les systèmes;
- Obtenir des consentements précis sur l'usage qui sera fait des renseignements personnels;
- Encadrer l'application des nouveaux droits pour les personnes dont les renseignements personnels sont recueillis, notamment :
 - Le droit à la portabilité des données;
 - Les droits liés à la prise de décision automatisée;
 - Les droits liés au profilage de données;
 - Le droit à l'oubli (à l'exception des renseignements d'intérêt public).

Pénalités

Les organisations qui ne respectent pas les dispositions de la Loi 25 et ses règlements d'application s'exposeront à des pénalités plus lourdes qu'aux termes du régime actuel. Ces pénalités varient en fonction de la taille de l'entreprise, mais suivent généralement les lignes directrices ci-dessous :

- 10 millions de dollars, ou un montant correspondant à 2 % du chiffre d'affaires mondial de l'exercice financier précédent, pour les entreprises privées qui omettent d'appliquer la réglementation;
- Un montant correspondant à 4 % des ventes de l'organisation — ou se situant entre 15 000 \$ et 25 millions de dollars — pour les entreprises privées qui s'exposent à des sanctions pénales;
- Deux catégories de pénalités pour les institutions publiques qui ne respectent pas la réglementation :
 - de 3 000 \$ à 30 000 \$;
 - de 15 000 \$ à 150 000 \$;
 - de 5 000 \$ à 100 000 \$ pour les infractions commises par une personne physique.

À quel moment la Loi 25 entre-t-elle en vigueur?

La Loi 25 entre progressivement en vigueur sur une période de trois ans. Les exigences des deux premières années (2022 et 2023) sont déjà en vigueur. Les exigences de la troisième année entreront en vigueur en septembre 2024.

Quelles sont les incidences de la Loi 25 sur les autres provinces qui font affaire au Québec?

La Loi 25 peut vous toucher, même si votre organisation ne se trouve pas au Québec. Les entreprises qui traitent des renseignements personnels divulgués par des organisations du Québec doivent faire le nécessaire pour que leurs pratiques respectent la Loi 25 et répondre de façon satisfaisante aux évaluations des facteurs relatifs à la vie privée menée par des organisations du Québec.

