Lemieux Nolet, comptables professionnels agréés S.E.N.C.R.L.

LÉVIS

1610, boul. Alphonse-Desjardins
Bureau 400
Lévis (Québec) G6V 0H1

Téléphone 418 833-2114
Télécopieur 418 833-9983

Mars 2024

Saviez-vous que…

Loi sur la protection des renseignements personnels

La Loi sur la protection des renseignements personnels, aussi appelée Loi 25, vise à protéger la population québécoise en responsabilisant les entreprises quant aux informations personnelles qu'elles détiennent. Les obligations et responsabilités qui en découlent entrent progressivement en vigueur depuis septembre 2022. En cas de besoin, un juriste spécialisé en protection de la vie privée ou un spécialiste en sécurité de l'information peut vous accompagner selon les spécificités propres à votre secteur d'activité.

Comme cette Loi impose certaines responsabilités aux entreprises privées progressivement, vous devez avoir mis en place en septembre 2023, notamment :

- Désigner une personne responsable de la protection des renseignements personnels et publier le titre et les coordonnées du responsable sur le site Web de l'entité.

- Faire l'inventaire des renseignements personnels détenus par votre entité et évaluer leur sensibilité. L'inventaire des renseignements personnels étant évolutif, il importe de le tenir à jour.

- En cas d'incident de confidentialité impliquant un renseignement personnel :

  - Prendre des mesures raisonnables pour diminuer les risques qu'un préjudice soit à nouveau causé et éviter que de nouveaux incidents ne se produisent.

  - Aviser la Commission d'accès à l'information (Commission) et la personne concernée si l'incident présente un risque de préjudice sérieux.

  - Tenir un registre des incidents dont une copie devra être transmise à la Commission à sa demande.

- Avoir établi des politiques et des pratiques encadrant la gouvernance des renseignements personnels et publier de l'information détaillée sur celles-ci sur le site Web de l'entité.

- Respecter les nouvelles règles entourant le consentement, la communication ou l'utilisation des renseignements personnels.

- Publier une politique de confidentialité sur le site Web de votre entité si vous collectez des renseignements personnels à l'aide d'un moyen technologique tel un site Web.

- Traiter les demandes et les plaintes des citoyens concernant votre gestion des renseignements personnels.

- Détruire les renseignements personnels lorsque la finalité de leur collecte est accomplie sous réserve des conditions et d'un délai de conservation prévus par une Loi.

- Surveiller l'application de ces mesures et les réviser.

Les organisations qui ne respectent pas les dispositions de la Loi 25 et ses règlements d'application s'exposeront à des pénalités qui varient en fonction de la taille de l'entité, mais suivent généralement les lignes directrices suivantes :

- 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.

Pour en savoir davantage, contactez Joanne Lalonde, CPA auditrice, directrice principale, certification au 1 866 833-2114.