

LPRPDE

Loi fédérale sur la protection des renseignements personnels (LPRPDE/PIPEDA) – Obligation de déclarer les atteintes à la sécurité des renseignements personnels

Les nouvelles dispositions sur les atteintes aux mesures de sécurité des renseignements personnels adoptées en vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) sont entrées en vigueur le 1er novembre 2018. Elles énoncent les règles et exigences pouvant être applicables en cas de perte, d'accès ou de divulgation non autorisé de renseignements personnels (atteinte à la sécurité des renseignements personnels).

Les organisations assujetties qui subissent une atteinte à la sécurité des renseignements personnels, présentant « un risque réel de préjudice grave » pour les individus, devront avertir les personnes visées, le signaler au Commissaire à la protection de la vie privée du Canada et tenir un registre des violations pour une durée de 24 mois suivant la découverte de l'atteinte. Le défaut de divulguer est punissable d'une amende pouvant aller jusqu'à 100 000 \$ en plus des dommages réputationnels que peut entraîner un processus de divulgation.

Loi sur la protection de la vie privée au Canada

La LPRPDE s'applique à la collecte, l'utilisation et la divulgation de renseignements personnels par des organisations privées dans le cadre d'une activité commerciale au Canada, sauf lorsqu'une loi provinciale sur la protection des renseignements personnels jugée essentiellement similaire à la LPRPDE a été adoptée. Actuellement le Québec, la Colombie-Britannique et l'Alberta ont adopté des législations similaires. L'Ontario, le Nouveau-Brunswick, la Nouvelle-Écosse et Terre-Neuve-et-Labrador ont aussi adopté des législations similaires mais qui s'appliquent principalement aux renseignements personnels liés à la santé.

Il est important de noter que la LPRPDE s'applique aux activités commerciales d'une organisation, mais non aux renseignements personnels de ses employés, sauf pour les entreprises sous réglementation fédérale (telles que les banques, les compagnies aériennes, les entreprises de télécommunications et les autres entités œuvrant dans des secteurs d'activité de compétence fédérale).

Renseignements sur les avantages sociaux des employés

Les renseignements personnels concernant les régimes d'avantages sociaux des employés détenus par un employeur peuvent être considérés comme des renseignements liés à l'emploi auxquels la LPRPDE ne s'applique pas, sauf en ce qui concerne les employeurs assujettis à la réglementation fédérale.

Les provinces peuvent toutefois avoir en vigueur des dispositions relatives à la vie privée qui s'appliqueront aux informations sur les employés, y compris les informations relatives aux régimes d'avantages sociaux, comme c'est le cas pour le Québec, la Colombie-Britannique et l'Alberta. Pour l'instant, l'Alberta est la seule province à imposer des obligations en matière de signalement des atteintes à la sécurité des renseignements personnels. Les provinces ayant adopté des législations similaires pourraient éventuellement faire de même.

Même si aucune disposition formelle sur le signalement des violations de données personnelles n'est applicable, il est reconnu que de divulguer les atteintes à la sécurité des renseignements personnels constitue une saine pratique commerciale souvent bénéfique pour limiter les dommages subis par une personne victime d'une atteinte relative aux informations personnelles.

Lorsque des informations relatives à la participation à un régime d'avantages sociaux sont transférées à une tierce partie, y compris un assureur, ces informations peuvent devenir assujetties à la LPRPDE fédérale et rendre les exigences de notification et déclaration potentiellement applicables, du moins dans les provinces n'ayant pas adopté de législation similaire. L'identité de la partie alors responsable du respect des obligations de notification et de déclaration peut alors dépendre des particularités de la situation, du contrôle effectif de l'information et des dispositions contractuelles applicables.

Les atteintes aux mesures de sécurité des renseignements personnels constituent plus que jamais une préoccupation pour les entreprises. Les coûts de réponse et de gestion associés aux potentielles exigences de notification peuvent être décuplés lorsqu'un volume important de dossiers est affecté simultanément.

Pour réduire les risques liés aux renseignements personnels, une organisation devrait mettre en œuvre des pratiques et des politiques appropriées en matière de gestion et de protection des données, instaurer des plans conformes de réponse aux incidents et pourrait devoir réviser ses ententes contractuelles en conséquence. L'éducation de ses employés sur la protection des données personnelles s'impose et une couverture d'assurance contre les cyber-risques pourrait être envisagée.

À propos d'Aon

Aon plc (NYSE : Aon) est un des principaux cabinets mondiaux de services professionnels, fournissant un vaste éventail de solutions de risques, de retraite et de santé. Nos 50 000 employés dans 120 pays donnent à nos clients les moyens de prospérer en utilisant des données exclusives et analytiques pour communiquer des informations qui réduisent la volatilité et améliorent le rendement.

© Aon Hewitt inc. 2018. Tous droits réservés.

L'information contenue dans le présent document et les déclarations qui y sont exprimées sont de nature générale et ne visent pas à traiter la situation d'une personne ou d'une entité en particulier. Bien que nous nous efforcions de fournir des renseignements exacts et à jour et d'utiliser des ressources que nous jugeons fiables, nous ne pouvons garantir ni l'exactitude desdits renseignements à la date à laquelle vous les recevez ni le fait qu'ils demeureront exacts à l'avenir. Personne ne doit donner suite à ces renseignements sans obtenir des conseils professionnels appropriés et pertinents après l'examen minutieux de la situation particulière.

