

La notification obligatoire des violations en vertu de la LPRPDE approche à grands pas – votre société est-elle prête?

Novembre 2017

Les dispositions tant attendues relatives à la notification obligatoire des violations en vertu de la *Loi sur la protection des renseignements personnels numériques* (projet de loi S-4) entreront bientôt en vigueur. Faisant partie des modifications à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) en 2015, ces dispositions exigent la signalisation obligatoire des violations au Commissariat à la protection de la vie privée et aux personnes concernées dans les cas où une intrusion aurait compromis des renseignements personnels. En septembre 2017, le règlement d'application, longtemps attendu, qui présente le régime de notification des violations, a été publié sous forme de projet pour une période de commentaires de 30 jours. Cette période a expiré le 2 octobre 2017, et la plupart des analystes juridiques et experts de l'industrie prédisent que le règlement entrera en vigueur d'ici la fin du deuxième trimestre de 2018.

Notification obligatoire des violations

Le régime obligatoire de notification des violations de la vie privée prévu dans le règlement oblige les sociétés fermées assujetties à la LPRPDE à signaler une atteinte « s'il est raisonnable de croire, dans les circonstances, que l'atteinte présente un risque réel de préjudice grave à l'endroit d'un individu ». La violation doit être signalée « le plus tôt possible » au Commissariat à la protection de la vie privée (le Commissariat) et aux personnes dont les renseignements personnels ont été compromis. La notification des personnes concernées doit contenir, entre autres, la description des mesures adoptées par l'entreprise pour réduire le risque de préjudice à leur égard, le numéro sans frais ou l'adresse électronique d'un service auprès duquel ces personnes touchées pourraient obtenir de plus amples informations. Une entreprise a également l'obligation de tenir des registres de toutes les atteintes aux mesures de sécurité dans les 24 mois suivant la date à laquelle elle détermine que l'atteinte a eu lieu; ces registres doivent être fournis au Commissariat sur demande.

Les facteurs à considérer par l'entreprise pour déterminer si une violation a créé un « risque réel de préjudice grave » comprennent le degré de sensibilité des renseignements personnels en cause et la probabilité que les renseignements aient été mal utilisés, ou soient en train ou sur le point de l'être. Il est important de noter, cependant, que ces facteurs n'ont pas encore été interprétés par les tribunaux. Le « préjudice grave » lui-même a été défini de façon assez générale : notamment la lésion corporelle, l'humiliation, le dommage à la réputation ou aux relations, la perte financière, le vol d'identité, l'effet négatif sur le dossier de crédit, le dommage aux biens ou leur perte, et la perte de possibilités d'emploi, d'occasions d'affaires ou d'activités professionnelles. Compte tenu de cette définition et de l'absence actuelle de directives judiciaires, il est prudent que les organisations pèchent par excès de prudence en décidant de signaler les violations. À ce stade-ci, il semble que l'obligation de notification sera très probable lorsqu'une entreprise subit une quelconque atteinte aux renseignements personnels.

Application et sanctions

Omettre sciemment de signaler des atteintes à la vie privée conformément à la *LPRPDE* pourrait entraîner une infraction passible d'une amende pouvant atteindre 100 000 \$ CA. Le Commissariat peut aussi divulguer les dossiers ou les rapports portant sur les atteintes aux organismes d'application de la loi ou au Service des poursuites pénales du Canada à des fins d'enquêtes et de poursuites.

De plus, le Commissariat a récemment présenté au Parlement son rapport annuel de 2016-2017 sur la *Loi sur la protection des renseignements personnels et les documents électroniques* et la *Loi sur la protection des renseignements personnels*. Le rapport était accompagné d'un message écrit du commissaire dans lequel il mentionnait le besoin de moderniser le régime de protection des renseignements personnels du Canada, ce qui exigerait d'apporter des modifications à la législation en vigueur et au

cadre de la sécurité nationale du pays, mais aussi un changement au rôle du Commissariat, de celui de médiateur gérant les plaintes à un organisme d'application préventive de la loi. Pour effectuer ce changement, le Commissariat chercherait probablement à proposer des modifications à la *LPRPDE* qui lui permettraient d'émettre des ordonnances et d'imposer des amendes administratives en cas de non-conformité.

Bien que la modification de l'actuelle législation sur la protection des renseignements personnels du Canada pourrait prendre un certain temps afin d'octroyer au Commissariat des mesures d'application supplémentaires, les entreprises pourront toujours écoper d'une amende relativement aux exigences de signalisation obligatoire d'une violation et de tenue des dossiers en vertu de la *LPRPDE*.

Ce que cela signifie pour votre entreprise

Le paysage de la protection des renseignements personnels au Canada tend vers une protection et une réglementation accrues dans un proche avenir, ce qui nécessiterait une plus grande vigilance de la part des organisations assujetties à la *LPRPDE*. Dans d'autres territoires où un régime obligatoire de notification des violations avait été imposé, on a constaté une légère hausse des enquêtes réglementaires et des coûts relatifs aux incidents. Cette preuve anecdotique laisse fortement entendre que les entreprises feraient bien d'établir activement des politiques et procédures internes ou de les réviser dans le but de respecter les exigences de la *LPRPDE* en matière de notification des violations.

Complément aux robustes mécanismes internes de conformité, l'assurance des risques cybernétiques peut aider les entreprises qui cherchent à transférer certains de leurs risques pouvant découler d'une intrusion ou d'une atteinte à la vie privée ou de la

non-conformité aux lois de protection des renseignements personnels. Une telle assurance couvre les frais qu'une entreprise pourrait engager afin de gérer une intrusion ou une atteinte à la vie privée. Elle couvre aussi les frais de défense, les montants octroyés par jugement, les montants négociés à l'amiable si l'entreprise est impliquée dans une action intentée par un tiers ou une procédure réglementaire. Si l'assurance des risques cybernétiques que votre entreprise souscrit contient un libellé solide, vous aurez peut-être la possibilité de faire valoir que les amendes et sanctions non pénales, comme celles imposées en vertu de la *LPRPDE*, sont assurables et donc couvertes en vertu de la police.

Mis à jour par

Jessica Foster J.D.

Conseillère juridique,

Service des affaires juridiques et des recherches

Toronto, Ontario

t +1.416.868.5977

jessica.foster@aon.ca

À propos d'Aon Risk Solutions Canada

Aon Reed Stenhouse

Depuis plus de 160 ans, Aon Reed Stenhouse est, d'une manière ou d'une autre, un chef de file du secteur canadien des assurances.

Aon Reed Stenhouse, faisant affaire sous le nom commercial d'Aon Risk Solutions, est le premier courtier d'assurance et cabinet de services de gestion des risques au Canada. Nous servons une vaste clientèle, traitant plus de 2 milliards de dollars de primes annuelles au nom de nos clients. Par l'intermédiaire des canaux de distribution mondiaux que nous exploitons directement, nos conseillers offrent aux clients une vaste gamme de services, notamment :

- Courtage de détail
- Réassurance
- Courtage en gros et de produits de spécialité
- Solutions de financement des risques non traditionnelles
- Services-conseils en avantages sociaux et en ressources humaines

Nos 1 600 professionnels de l'assurance servent notre clientèle depuis 23 succursales situées dans l'ensemble du Canada. Nous offrons à nos clients une large gamme de solutions innovantes, un service à la clientèle, ainsi que des services de traitement des sinistres, de contrôle des risques et de gestion des risques. Chaque jour, les professionnels d'Aon œuvrent à offrir les meilleures solutions à nos clients.

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 Reed Stenhouse inc. 2017. 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.

aon.ca

