HSB BI&I

Munich RE

Les lois fédérales sur la notification obligatoire des violations de données entrent en vigueur le 1er novembre 2018

Ce que vous devez savoir

À compter du 1er novembre 2018, la Loi sur la protection des renseignements personnels numériques (Loi S-4) modifie la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), obligeant ainsi tous les organismes à déclarer les cas de violations de données aux individus affectés et au Commissariat à la protection de la vie privée du Canada. Des règlements prescrits accompagnent la législation et définissent les exigences relatives à la notification des violations de données et à la tenue d'un registre.

Cette loi s'applique-t-elle aux petites organisations?

Les entreprises et les organisations de toutes tailles détiennent des renseignements d'identification personnels des individus, tels que les employés, les clients, les membres et les fournisseurs. En conséquence, la loi ne fait aucune distinction entre les grandes et les petites entreprises.

Les violations de données ne se produisent-elles pas uniquement dans les grandes entreprises?

Une étude réalisée par Zogby Analytics en 2017 a révélé que 29 % des petites entreprises avaient subi au moins une violation de données. Les petites entreprises sont des cibles de choix pour les voleurs de données, car leurs systèmes de sécurité sont perçus comme étant moins sophistiqués que ceux des grandes entreprises.

Que signifie « Renseignements d'identification personnels »?

« Renseignements d'identification personnels » signifie des renseignements, incluant les renseignements sur la santé, qui pourraient être utilisés pour commettre une fraude ou toute autre activité illégale portant sur le crédit, l'accès aux soins de santé ou l'identité d'un individu affecté.

Voici quelques exemples :

- Adresse courriel
- Numéro de compte de crédit / débit
- Renseignements sur le permis de conduire
- Numéro d'assurance sociale
- Renseignements médicaux et sur la santé
- Autres renseignements personnels sensibles

Pourquoi une organisation déclarerait-elle une violation de données si la mauvaise publicité peut causer des dommages à sa réputation?

Il est vrai qu'une violation de données peut nuire à une image de marque. Mais ce qui est pire pour une entreprise, c'est de tenter de dissimuler qu'une telle violation s'est produite et que les clients s'en rendent compte par la suite. Au moindre indice de tromperie ou de non-divulgation, les consommateurs ont le pouvoir d'infliger de sérieux dommages à une marque, par le biais des médias sociaux par exemple. De plus, les médias grand public se nourrissent de ces types d'histoires. Le fait de contrevenir aux exigences de la Loi constitue également une infraction.

Quels types de violations de données les petites entreprises peuvent-elles subir?

- Des cambrioleurs entrent dans le bureau d'un courtier d'assurance et volent des ordinateurs portables et des dossiers d'employés.
- Un pirate informatique vole des centaines de dossiers de cartes de crédit client sur un site de vente en ligne.
- Le vol d'un ordinateur portable dans un bureau de comptable expose les dossiers fiscaux de centaines de clients.
- Des demandes de location comportant des noms, des coordonnées et des numéros d'assurance sociale sont volées du système informatique d'un gestionnaire immobilier.
- Une maison de soins infirmiers est piratée et perd des renseignements essentiels sur les patients ainsi que les renseignements personnels à propos des membres de la famille.

Quel est le coût d'une violation de données pour une organisation?

Les violations de données peuvent être coûteuses. Une étude de Ponemon Institute en 2017 a détaillé les dépenses moyennes d'une violation de données pour une organisation canadienne, **par individu affecté,** à :

Coût direct : 108 $

- Les dépenses réelles engagées, telles que l'embauche de personnel juridique et de consultants en TI, notifiant et fournissant des services aux individus affectés.

Coût indirect : 147 $

- Les coûts reliés au temps utilisé, aux efforts et aux autres ressources organisationnelles nécessaires pour résoudre la violation.

Une organisation peut également subir des dommages à sa réputation et une perte de clientèle à la suite d'une violation.

L'assurance peut-elle couvrir ces coûts?

Oui. L'assurance contre la Compromission des données peut être ajoutée à la police d'assurance multirisque des entreprises, pour couvrir :

- L'évaluation judiciaire des TI afin de déterminer l'étendue de la violation et les personnes affectées.
- L'évaluation juridique pour informer les personnes affectées par la violation.
- Les services de notification aux individus affectés et au Commissaire à la protection de la vie privée.
- Les services aux individus affectés, comprenant :
  - L'alerte à la fraude pour les individus affectés, et
  - La gestion de cas de restauration d'identité pour les victimes de vol d'identité.
- Les services de relations publiques pour répondre à l'impact potentiel de la violation sur les relations d'affaires.

Que devrait faire un titulaire de police s'il soupçonne qu'une violation de données a eu lieu?

Si une violation de données présumée a eu lieu, un titulaire de police qui a souscrit la garantie Compromission des données doit communiquer avec son courtier d'assurance, afin d'alerter le service des sinistres de BI&I. Les spécialistes en violation de données de BI&I communiqueront avec lui.

Pour de plus amples renseignements, ou pour ajouter la garantie Compromission des données, veuillez communiquer avec votre Représentant, développement des affaires de BI&I.

Pour toutes les garanties, les termes, les dispositions et les exclusions, veuillez vous référer à la police d'assurance en vigueur.

390, rue Bay, bureau 2000
Toronto (Ontario) M5H 2Y2
Téléphone : (416) 363-5491
biico.com

Branchez-vous