

8 novembre 2018

Le 1^{er} novembre 2018, les modifications annoncées à la *Loi sur la protection des renseignements personnels et les documents électroniques* (Canada) (LPRPDE) sont entrées en vigueur. Ces nouvelles dispositions exigent des organisations assujetties à la LPRPDE qu'elles déclarent toute atteinte aux mesures de sécurité lorsqu'elle crée un « risque réel de préjudice grave » à des individus. Une telle déclaration doit être faite le plus tôt possible après que l'organisation a conclu qu'il y a eu atteinte et ce tant au Commissariat à la protection de la vie privée du Canada (au moyen d'un formulaire prescrit) qu'au individus touchés. Chaque individu doit être avisé directement, bien qu'il soit possible d'aviser un individu indirectement (par exemple, publicité dans les journaux ou en ligne) si l'avis direct est impossible, peu pratique ou inapproprié.

Les modifications définissent la notion de « risque réel de préjudice grave » de manière très large : le « préjudice grave » comprend les dommages physiques, mentaux, de réputation, professionnels et économiques, tandis que les facteurs pertinents pour évaluer s'il y a un risque réel comprennent la sensibilité des renseignements personnels et la probabilité d'un mauvais usage. Par conséquent, les organisations doivent être très prudentes avant de décider qu'une atteinte ne crée aucun risque réel de préjudice grave et ne déclenche pas l'obligation de déclaration. Même s'il est déterminé qu'aucune déclaration n'est requise, la LPRPDE exige maintenant que les organisations tiennent un registre de toutes atteintes aux mesures de sécurité pendant une période d'au moins 24 mois après leur découverte.

En plus d'aviser le Commissariat et les individus touchés, la LPRPDE exige qu'une organisation dont les mesures de sécurité ont été violées avise toute autre organisation (incluant une institution gouvernementale) si cela peut réduire ou atténuer le risque de préjudice découlant de l'atteinte. Par exemple, une entreprise se faisant voler les données de ses clients pourrait avoir à contacter les autorités policières pour empêcher que ces données soient mal utilisées.

Le Commissariat a publié un document d'orientation intitulé *Ce que vous devez savoir sur la déclaration obligatoire des atteintes aux mesures de sécurité*, qui clarifie son interprétation de certaines particularités des nouvelles exigences. Il est d'avis, notamment, que si des données en possession d'un tiers fournisseur de services sont violées (par exemple, un fournisseur de services d'hébergement ou de traitement de cartes de crédit), la responsabilité de signaler l'atteinte incombe à l'organisation qui a initialement recueilli les renseignements personnels, et non à la tierce partie. De plus, le document fournit des directives supplémentaires en ce qui constitue des renseignements « sensibles » et sur la façon de déterminer s'il y a une réelle probabilité d'un mauvais usage des données.

Il est important de rappeler que la Colombie-Britannique, l'Alberta et le Québec ont chacun leur équivalent provincial de la LPRPDE qui régit les organisations assujetties exclusivement aux lois de ces provinces. Ces organisations ne sont pas assujetties à la LPRPDE et ces nouvelles règles ne s'appliquent pas à elles. Il est à noter que la loi de l'Alberta comporte ses propres exigences en matière de déclaration obligatoire

Nous suggérons trois pratiques afin de se préparer à une atteinte aux mesures de sécurité : (i) assurez-vous d'avoir un plan de réponse qui attribue clairement les responsabilités de chacun et qui détermine les procédures à appliquer dès que la survenance d'un incident à la sécurité est soupçonné, (ii) distribuez ce plan à votre personnel pour qu'il

puisse être mis en œuvre adéquatement et (iii) adresser l'incident à la sécurité sans délai et avec sérieux et transparence afin de démontrer votre caractère éthique et votre résilience.

Pour obtenir de plus amples renseignements sur ces nouvelles exigences et des conseils pratiques sur la façon de vous conformer aux obligations de votre organisation en matière de renseignements personnels, veuillez communiquer avec Chantal Bernier de notre bureau d'Ottawa, responsable de notre pratique canadienne en matière de Cybersécurité et protection de la vie privée et des renseignements personnels, ou Adam Allouba, associé à notre bureau de Montréal et membre de ce groupe.

Vos contacts clés



Chantal Bernier

Avocate-conseil, Ottawa

D +1 613 783 9684

chantal.bernier@dentons.com