AIDE-MÉMOIRE

Signaler un incident en lien avec la protection des renseignements personnels (PRP) et déclaration obligatoire

Objectif du document

Renseigner sur la notification obligatoire sur les atteintes aux mesures de sécurité.

Le 1er novembre 2018 entrait en vigueur le Règlement sur les atteintes aux mesures de sécurité, qui oblige dorénavant les entreprises assujetties à la Loi sur la protection des renseignements personnels et des documents électroniques (LPRPDE) à déclarer les atteintes aux mesures de sécurité et à tenir un registre de ces atteintes.

En vertu de ces nouvelles exigences, la LPRPDE oblige les organisations à aviser les personnes visées par l'atteinte lorsqu'il y a un risque réel de préjudice grave pour ces derniers. Que l'atteinte aux mesures de sécurité touche une seule personne ou plusieurs, celle-ci devra être signalée, si votre évaluation indique qu'il y a un risque réel de préjudice grave découlant de l'atteinte. Parmi les facteurs pertinents pour déterminer si une atteinte aux mesures de sécurité présente un risque réel de préjudice grave, on retrouve le degré de sensibilité des renseignements personnels en cause dans l'atteinte aux mesures de sécurité et la probabilité que ceux-ci aient été mal utilisés ou soient en train ou sur le point de l'être. Lorsque le critère est rencontré, l'incident doit être déclaré au Commissaire à la protection de la vie privée du Canada.

Destinataire du document : Organisations qui « gèrent » des renseignements personnels impliqués dans l'atteinte et soumises à la LPRPDE

Les renseignements personnels (RP)

Un renseignement personnel comprend tout renseignement concernant une personne identifiable ou qui, pris séparément ou combiné avec d'autres données, permet d'identifier une personne. L'information doit se rapporter à un individu (personne physique).

Les atteintes aux mesures de sécurité impliquant des renseignements personnels

Une atteinte aux mesures de sécurité se produit notamment lorsqu'il y a communication non autorisée ou perte de renseignements personnels, un accès non autorisé à des renseignements personnels à la suite d'une atteinte aux mesures de sécurité mises en place, ou encore un défaut d'avoir mis en place de telles mesures de sécurité.

Les obligations du *Règlement*

- Ces obligations s'appliquent aux petites et aux grandes entreprises
- Des sanctions pécuniaires pourraient être imposées à toute organisation qui contrevient sciemment aux obligations en matière de déclaration, d'avis et de tenue de registre des atteintes aux mesures de sécurité
- Il faut consigner dans un registre toute atteinte aux mesures de sécurité, qu'elle rencontre le critère de *risque réel de préjudice grave* ou non. Des formalités s'appliquent à la tenue de ce registre.
- La loi exige de conserver le registre pendant deux ans. Il se peut que vous ayez d'autres obligations juridiques nécessitant que vous les conserviez plus longtemps.
- Le Commissariat a émis des directives sur les modalités et formalités de déclaration obligatoire. Vous pourrez les trouver sur son site web.
- À moins que la loi ne l'interdise, chaque fois que vous déterminez qu'une atteinte aux mesures de sécurité présente un risque réel de préjudice grave pour un individu, vous devez aviser la ou les personnes concernées. L'avis doit être apparent et il doit être donné directement à l'individu, sauf en certaines circonstances prévues au *Règlement*.
- La loi prévoit que l'avis aux intéressés doit être remis dès que possible après avoir déterminé qu'une atteinte aux mesures de sécurité impliquant un risque réel de préjudice grave a eu lieu.
- L'avis devrait comprendre les renseignements suivants précisés dans le Règlement :
    - les circonstances de l'atteinte;
    - la date ou la période où il y a eu atteinte ou, si elle n'est pas connue, une approximation de la période;
    - la nature des renseignements personnels visés par l'atteinte, pour autant qu'elle soit connue;
    - les mesures que l'organisation a prises afin de réduire le risque de préjudice qui pourrait résulter de l'atteinte;
    - les mesures que peut prendre tout intéressé afin de réduire le risque de préjudice qui pourrait résulter de l'atteinte ou afin d'atténuer un tel préjudice;
    - les coordonnées permettant à l'intéressé de se renseigner davantage au sujet de l'atteinte.
- L'organisation qui avise un intéressé d'une atteinte aux mesures de sécurité qui présente un risque réel de préjudice grave doit également aviser toute autre organisation ou institution gouvernementale qui, selon elle, est en mesure de réduire le risque de préjudice qui pourrait découler de l'atteinte ou qui pourrait atténuer un tel préjudice.

Bonnes pratiques en matière de PRP

- Contre-vérifier le destinataire de tout courriel, télécopie ou lettre
- Utiliser la fonction copie conforme invisible (cci) lors d'envoi massif de courriels
- Ne pas laisser de document contenant des RP sans surveillance
- Verrouiller son poste de travail dès qu'on s'absente, et ce, même si c'est pour quelques instants
- Laisser son bureau libre de tout document contenant des RP
- Identifier l'interlocuteur téléphonique et s'assurer d'avoir le consentement pour transmettre toute information confidentielle par téléphone
- S'assurer de la conformité des échanges de RP au sein de votre organisation

Pour aller plus loin, le Commissariat à la protection de la vie privée a publié l'article *Comment réagir à une atteinte à la vie privée dans votre entreprise*, vous pouvez le consulter au https://www.priv.gc.ca