LAPOINTE ROSENSTEIN MARCHAND MELANÇON
S.E.N.C.R.L. Avocats

Bulletin

Droit commercial

Mai 2018

M^e^ Marissa Carnevale

Le présent bulletin d'information a été rédigé en collaboration avec Tania L. Pinheiro, étudiante en droit.

Mise à jour des lois sur la protection des renseignements personnels : nouvelles règles relatives à l'atteinte aux mesures de sécurité

Le 18 juin 2015, la *Loi sur la protection des renseignements personnels numériques*[1] (Canada) a apporté de nombreux changements à la *Loi sur la protection des renseignements personnels et les documents électroniques*[2] (Canada) (la « **LPRPDE** »), notamment l'établissement d'un régime obligatoire de tenue de registres et de signalement des atteintes à la protection des données. Ces obligations, ainsi que les formalités régissant leur application, prévues par le *Règlement concernant les atteintes aux mesures de sécurité*[3] (le « **Règlement** ») entreront en vigueur le **1^er^ novembre 2018**.

À compter de cette date, les organisations qui recueillent, utilisent ou communiquent des renseignements personnels concernant des résidents canadiens auront l'obligation de conserver un registre de toute atteinte aux mesures de sécurité qu'elles subissent. Une atteinte aux mesures de sécurité s'entend de toute *communication non autorisée*, *perte* de renseignements personnels, ou tout *accès non autorisé* à ceux-ci, par suite d'une atteinte aux mesures de sécurité d'une organisation ou du fait que ces mesures n'ont pas été mises en place (une « **atteinte** »)[4].

De plus, lorsqu'une atteinte présente « un risque réel de préjudice grave » à l'endroit d'un individu, l'organisation aura l'obligation de déclarer cette atteinte au commissaire à la protection de la vie privée du Canada (le « **commissaire** ») et d'aviser les individus dont les renseignements personnels ont été visés par l'atteinte (les « **individus concernés** ») ainsi que d'autres organisations susceptibles de pouvoir réduire le risque ou mitiger les dommages causés par l'atteinte.

Exigences en matière de tenue de registres

Le Règlement prévoit une période obligatoire de conservation de données et exige que les organisations conservent et maintiennent un registre de *toutes* les atteintes mettant en cause des renseignements personnels qui leur sont confiés, que les atteintes présentent ou non « un risque réel de préjudice grave ». Le registre des atteintes doit être conservé pendant au moins **24 mois** suivant la date de l'atteinte, telle que déterminée par l'organisation ayant subi l'atteinte, et doit comprendre suffisamment de renseignements pour permettre de démontrer que l'organisation surveille les intrusions dont elle fait l'objet. Le commissaire doit également être en mesure de vérifier si l'organisation a respecté ses obligations et avoir accès au registre sur demande[5].

Déclarations et avis

En vertu des nouvelles règles, une organisation devra déclarer au commissaire et aviser les individus concernés de toute atteinte mettant en cause des renseignements personnels qui lui sont confiés, lorsqu'elle croit raisonnablement que l'atteinte présente « un risque réel de préjudice grave à l'endroit d'un individu »[6]. Dans ce cas, l'organisation sera aussi tenue d'aviser toute autre organisation ou institution gouvernementale si elle croit que ces dernières

pourraient réduire le risque de préjudice ou atténuer le préjudice[7] découlant de l'atteinte.

Un « préjudice grave » comprend notamment une lésion corporelle, une humiliation, un dommage à la réputation ou aux relations, une perte financière, un vol d'identité, un effet négatif sur un dossier de crédit, un dommage aux biens ou leur perte, ainsi qu'une perte de possibilités d'emploi, d'occasions d'affaires ou d'activités professionnelles[8]. Afin d'évaluer si une atteinte présente un « risque réel de préjudice grave », les organisations doivent tenir compte notamment du degré de sensibilité des renseignements personnels en cause et de la probabilité que ces renseignements aient été mal utilisés ou soient en train ou sur le point de l'être[9].

Le Règlement prévoit diverses précisions concernant les renseignements devant se retrouver dans les déclarations d'atteinte remises au commissaire et dans les avis aux individus concernés[10], ainsi que leurs modalités d'envoi. Dans tous les cas, les déclarations et les avis d'atteinte aux mesures de sécurité doivent être envoyés le plus tôt possible suivant la date où l'organisation conclut qu'il y a eu atteinte[11]. Il est aussi possible pour une organisation de transmettre au commissaire tout nouveau renseignement concernant une atteinte lorsque l'organisation en prend connaissance, même après la remise de la déclaration initiale[12].

En ce qui concerne les individus concernés, l'avis d'atteinte doit contenir suffisamment de renseignements pour permettre à l'intéressé de comprendre l'importance de l'atteinte et de prendre des mesures pour réduire le risque de préjudice résultant de l'atteinte ou atténuer le préjudice[13]. Le Règlement prévoit que l'avis doit être donné directement aux individus concernés, soit en personne, par téléphone, par courrier, par courriel ou par tout autre moyen de communication raisonnable[14]. Cependant, lorsque l'avis direct est susceptible de causer un préjudice accru aux individus concernés ou de représenter une contrainte excessive pour l'organisation, notamment lorsqu'elle ne possède pas les coordonnées de l'individu[15], l'avis peut être donné indirectement, c'est-à-dire par communication publique ou par toute mesure semblable raisonnable, comme la publication d'une annonce[16].

Législation provinciale

Au Québec, la *Loi sur la protection des renseignements personnels dans le secteur privé*[17] réglemente la collecte, l'utilisation et la communication de renseignements personnels. Ainsi, les nouvelles obligations en matière de protection des données ne s'appliquent pas à une organisation recueillant, utilisant ou communiquant des renseignements personnels au Québec, sauf si elle le fait dans le cadre d'une entreprise fédérale ou si elle communique ces renseignements pour contrepartie à l'extérieur de la province[18].

Conclusion

Bien que les exigences du Règlement soient similaires aux recommandations actuelles du commissaire en matière de déclaration volontaire d'atteinte à la sécurité de données[19], les organisations devraient s'assurer d'être prêtes à se conformer aux nouvelles exigences en matière de protection des données **au plus tard le 1er novembre 2018**.

Afin de se conformer aux exigences, les organisations devraient se doter de politiques écrites relatives aux marches à suivre en cas d'atteinte aux mesures de sécurité et s'assurer que des systèmes permettant la surveillance interne, le suivi, la tenue de dossiers et le signalement de toute atteinte à la sécurité de données soient établis. Les organisations devraient également mettre en place des politiques écrites et des systèmes permettant de procéder à des évaluations de risques et d'établir la présence d'un « risque réel de préjudice grave » aux fins des exigences obligatoires de déclaration et d'avis.

En cas de manquement à ces nouvelles obligations, les organisations pourraient se voir imposer des amendes allant de 10 000 $ à 100 000 $, selon la nature de l'infraction.

Il est donc primordial pour les organisations de demander rapidement conseil afin d'évaluer les risques juridiques auxquels elles peuvent être exposées en raison de l'évolution du cadre législatif, et de vérifier que leurs programmes de sécurité des données respectent les nouvelles exigences.

---

1. LRC, 2015, c 32.
2. LRC, 2000, c 5.
3. Gazette du Canada, Partie 1, Vol. 151, No 35, 2 septembre 2017.
4. *Supra* note 2, art 2(1).
5. *Ibid*, art 10.3(2).
6. *Ibid*, art 10.1(1) et 10.1(3).
7. *Ibid*, art 10.2(1).
8. *Ibid,* art 10.1(7).
9. *Ibid,* art 10.1(8).
10. *Supra* note 3, art 2(1) et 3.
11. *Supra* note 2, art 10.1(6) et 10.2(2).
12. *Supra* note 3, art 2(2).
13. *Supra* note 2, art 10.1(4).

14. *Supra* note 2, art 10.1(5); *Supra* note 3, art 4.
15. *Supra* note 2, art 10.1(5); *Supra* note 3, art 5(1).
16. *Supra* note 3, art 5(2).
17. RLRQ, c P-39.1.
18. *Supra note 2*, art 30(1).
19. « Résumé de l'étude d'impact de la réglementation », section Déclaration d'atteinte à la protection des données au commissaire.

Pour obtenir de plus amples renseignements, veuillez communiquer avec :

Marissa Carnevale
514 925-6324
marissa.carnevale@lrmm.com