Récemment publié, le règlement de la LPRPDE concernant les atteintes aux mesures de sécurité fait l'objet d'une consultation

08 septembre 2017

Le 15 juin 2015, le projet de loi S-4, intitulé *Loi sur la protection des renseignements* personnels numériques, a modifié la *Loi sur la protection des renseignements* personnels et les documents électroniques (la « LPRPDE »). En vertu des nouveaux articles 10.1, 10.2 et 10.3, qui ne sont pas encore en vigueur, la *Loi sur la protection des* renseignements personnels numériques prévoit l'obligation expresse de signaler aux personnes intéressées toute atteinte aux mesures de sécurité et de la déclarer au Commissariat à la protection de la vie privée du Canada (le « CPVP ») « 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 ». En outre, l'organisation qui informe une personne d'une atteinte à la sécurité doit aussi en aviser toute autre organisation gouvernementale capable d'atténuer le préjudice causé aux intéressés et tenir un registre de toute atteinte à la protection des données dont elle a connaissance. Le projet de loi S-4 permet l'ajout de précisions par voie de règlement.

Au moment d'élaborer ce règlement, le gouvernement a entrepris une consultation, qui comprenait la publication d'un document de consultation en mars 2016 et d'un résumé des réponses à la consultation en octobre de la même année.

Le Règlement concernant les atteintes aux mesures de sécurité (le « règlement ») a finalement été publié le 2 septembre 2017, en même temps que le Résumé de l'étude d'impact de la réglementation que l'on peut trouver dans la Gazette du Canada. Quiconque souhaite communiquer ses commentaires sur le règlement proposé a 30 jours pour le faire. Le règlement entrera en vigueur au même moment que l'article 10 de la Loi sur la protection des renseignements personnels numériques.

Objectifs du règlement

Le règlement vise à faire en sorte que, d'une part, tous les Canadiens reçoivent des informations cohérentes au sujet des atteintes à la protection des données présentant un risque réel de préjudice grave à leur endroit et que, d'autre part, les avis renferment suffisamment d'information pour permettre aux individus de comprendre l'importance de l'atteinte et de ses conséquences possibles. Il a également pour but de faire en sorte

que le CPVP reçoive des informations cohérentes et comparables au sujet des atteintes à la protection des données présentant un risque de préjudice grave et soit capable d'exercer une surveillance efficace et de s'assurer que les organisations se conforment aux nouvelles obligations pour ce qui est d'aviser les intéressés d'une atteinte à la protection des données.

Exigences en matière de signalement au CPVP

L'article 2 du règlement présente les exigences concernant le contenu et les modalités de la déclaration lorsqu'il s'agit de signaler au CPVP une atteinte aux mesures de sécurité. La déclaration d'atteinte doit être faite par écrit et contenir les renseignements suivants :

- les circonstances de l'atteinte et, si elle est connue, la cause de l'atteinte;
- la date ou la période où il y a eu atteinte;
- la nature des renseignements personnels visés par l'atteinte;
- une estimation du nombre d'individus à l'égard desquels l'atteinte présente un risque réel de préjudice grave;
- les mesures que l'organisation a prises afin de réduire le risque de préjudice à l'endroit d'un individu résultant de l'atteinte ou afin d'atténuer un tel préjudice;
- les mesures que l'organisation a prises ou qu'elle entend prendre afin d'aviser l'intéressé de toute atteinte;
- le nom et les coordonnées d'une personne qui peut répondre au nom de l'organisation aux questions du CPVP au sujet de l'atteinte.

On ne devrait pas s'étonner de ces exigences puisqu'elles reproduisent pour l'essentiel l'information à inclure dans le Rapport d'atteinte à la vie privée, tel que le recommande le CPVP.

Obligations d'aviser les intéressés

Selon l'article 10.1(4) de la *Loi sur la protection des renseignements personnels* numériques, « [l']avis […doit contenir] suffisamment d'information pour permettre à l'intéressé de comprendre l'importance, pour lui, de l'atteinte et de prendre, si cela est possible, des mesures pour réduire le risque de préjudice qui pourrait en résulter ou pour atténuer un tel préjudice. Il […doit aussi contenir] tout autre renseignement réglementaire ».

Contenu de l'avis

Les articles 3, 4 et 5 du règlement prévoient que « [l]'avis fourni par l'organisation à un intéressé touché par l'atteinte aux mesures de sécurité [… doit contenir] les renseignements suivants :

- les circonstances de l'atteinte;
- la date ou la période où il y a eu atteinte;
- la nature des renseignements personnels visés par l'atteinte;
- les mesures que l'organisation a prises afin de réduire le risque de préjudice à l'endroit de l'intéressé résultant de l'atteinte ou afin d'atténuer un tel préjudice;

- les mesures que peut prendre l'intéressé afin de réduire le risque de préjudice qui pourrait résulter de l'atteinte ou afin d'atténuer un tel préjudice;
- un numéro de téléphone sans frais ou une adresse de courriel pour permettre à l'intéressé de se renseigner davantage au sujet de l'atteinte;
- des renseignements sur le processus interne de traitement des plaintes de l'organisation, ainsi que sur le droit d'un intéressé de déposer une plainte auprès du CPVP. »

Ces exigences sont en outre assez standard et, en attendant l'entrée en vigueur des nouveaux articles, les organisations touchées par une atteinte seraient avisées de se conformer à cet article du règlement proposé si elles choisissent d'informer les intéressés. En outre, ces exigences sont pour ainsi dire le reflet de l'information à inclure dans un avis aux intéressés tel que le recommande le CPVP dans les Principales étapes à suivre par les organisations en cas d'atteintes à la vie privée. Dans ce document, le CPVP recommande que les sources d'information visant à aider les personnes à se protéger contre le vol d'identité (p. ex. les conseils offerts sur le site Web du CPVP et celui d'Innovation, Sciences et Développement économique Canada) figurent également dans l'avis.

Avis direct et avis indirect à l'intéressé, en quoi diffèrent-ils?

Avis direct : En ce qui a trait à la manière dont les organisations doivent aviser directement les individus, l'article 4 du règlement précise que « l'avis […doit être] donné à l'intéressé directement (i) par courriel ou par tout autre moyen de communication sécurisé auquel l'intéressé a consenti pour recevoir des renseignements de l'organisation, (ii) par courrier à la dernière adresse de résidence connue de l'intéressé, (iii) par téléphone, (iv) en personne ».

Nous constatons que l'exigence selon laquelle l'intéressé doit avoir donné son consentement à recevoir des avis par courriel correspond à l'exigence précisée dans les Lignes directrices sur les atteintes à la vie privée du gouvernement du Canada aux termes de la *Loi sur la protection des renseignements personnels*, qui dit que « [l']institution ne doit utiliser le courrier électronique que si la personne a consenti à recevoir des avis électroniques ». Une exigence analogue figure également dans les lois de certains États américains concernant les avis d'atteinte aux mesures de sécurité. Un avis par courriel peut, du moins dans certaines situations, constituer le meilleur moyen d'informer un intéressé. Espérons que la notion de « consentement à recevoir des avis électroniques » soit interprétée avec souplesse, de façon à inclure une forme implicite de consentement – par exemple lorsqu'une personne a fourni son adresse de courriel à l'organisation et que le courriel constitue le mode de communication privilégié entre les parties.

Avis indirect : La *Loi sur la protection des renseignements personnels* numériques prévoit également que l'avis, dans les circonstances prévues par règlement, « […doit être] donné à l'intéressé indirectement, selon les modalités réglementaires ». L'article 5 du règlement proposé laisse entendre que l'avis peut être donné à l'intéressé indirectement par l'organisation lorsque le fait de le donner directement causerait davantage de préjudices à l'intéressé, que les coûts de l'avis donné directement sont excessifs pour l'organisation ou que l'organisation n'a pas les coordonnées de l'intéressé ou que celles qu'elle détient sont désuètes. Lorsque l'avis indirect est autorisé, le règlement prévoit qu'il doit être donné soit par la publication d'un

message bien en vue sur le site Web de l'organisation pendant au moins 90 jours, soit par la publication d'une annonce susceptible de joindre l'intéressé.

Registre – modalités

Le règlement proposé traite également des exigences relatives à la tenue d'un registre, car la Loi sur la protection des renseignements personnels numériques exige que les organisations tiennent et conservent un registre de toutes les atteintes aux mesures de sécurité qui ont trait à des renseignements personnels dont elles ont la gestion « conformément aux règlements ». L'article 6 du règlement proposé stipule que « l'organisation [doit] conserve[r] le registre de toute atteinte aux mesures de sécurité pendant 24 mois après la date à laquelle elle a conclu que l'atteinte a eu lieu et [que] le registre [… doit contenir] tout renseignement qui, eu égard à l'atteinte, permet au […CPVP] de vérifier la conformité [aux paragraphes 10.1(1) et (3) de la LPRPDE] ». Le projet de réglementation précise aussi qu'« une déclaration au [… CPVP] peut être utilisée, par l'organisation, à titre de registre de l'atteinte aux mesures de sécurité ».

Conclusion

La publication du règlement proposé semble indiquer que les nouveaux articles 10.1, 10.2 et 10.3 présentés dans la *Loi sur la protection des renseignements personnels* numériques entreront en vigueur dans un avenir rapproché. Étant donné que le règlement proposé fait l'objet d'une consultation étalée sur 30 jours, les organisations devraient envisager de communiquer leurs préoccupations dans le délai imparti. En outre, elles devraient finaliser leur plan d'intervention en cas d'atteinte à la protection des renseignements personnels et se préparer en vue de l'entrée en vigueur de cette nouvelle exigence en matière d'avis, surtout compte tenu du fait que celles qui omettent de signaler les atteintes comme le prévoit la LPRPDE, ou de tenir le registre requis, s'exposent à des amendes.

Par

Services

Cybersécurité, respect de la vie privée et protection des renseignements personnels

BLG | Vos avocats au Canada

Borden Ladner Gervais S.E.N.C.R.L., S.R.L. (BLG) est le plus grand cabinet d'avocats canadien véritablement multiservices. À ce titre, il offre des conseils juridiques pratiques à des clients d'ici et d'ailleurs dans plus de domaines et de secteurs que tout autre cabinet canadien. Comptant plus de 800 avocats, agents de propriété intellectuelle et autres professionnels, BLG répond aux besoins juridiques d'entreprises et d'institutions au pays comme à l'étranger pour ce qui touche les fusions et acquisitions, les marchés financiers, les différends et le financement ou encore l'enregistrement de brevets et de marques de commerce.

blg.com

Bureaux BLG

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000, rue De La Gauchetière Ouest
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749

Les présents renseignements sont de nature générale et ne sauraient constituer un avis juridique, ni un énoncé complet de la législation pertinente, ni un avis sur un quelconque sujet. Personne ne devrait agir ou s'abstenir d'agir sur la foi de ceux-ci sans procéder à un examen approfondi du droit après avoir soupesé les faits d'une situation précise. Nous vous recommandons de consulter votre conseiller juridique si vous avez des questions ou des préoccupations particulières. BLG ne garantit aucunement que la teneur de cette publication est exacte, à jour ou complète. Aucune partie de cette publication ne peut être reproduite sans l'autorisation écrite de Borden Ladner Gervais S.E.N.C.R.L., S.R.L. Si BLG vous a envoyé cette publication et que vous ne souhaitez plus la recevoir, vous pouvez demander à faire supprimer vos coordonnées de nos listes d'envoi en communiquant avec nous par courriel à desabonnement@blg.com ou en modifiant vos préférences d'abonnement dans blg.com/fr/about-us/subscribe. Si vous pensez avoir reçu le présent message par erreur, veuillez nous écrire à communications@blg.com. Pour consulter la politique de confidentialité de BLG relativement aux publications, rendez-vous sur blg.com/fr/ProtectionDesRenseignementsPersonnels.

© 2026 Borden Ladner Gervais S.E.N.C.R.L., S.R.L. Borden Ladner Gervais est une société à responsabilité limitée de l'Ontario.