DÉCLARATION ET TENUE D'UN REGISTRE DES ATTEINTES AUX MESURES DE SÉCURITÉ : LE CPVP LANCE DE NOUVELLES RESSOURCES POUR LES ENTREPRISES

Publié le 28 septembre, 2020

Catégories: Perspectives, Publications

Plus tôt ce mois-ci, le Commissariat à la protection de la vie privée du Canada (« CPVP ») a lancé de nouvelles ressources pour aider les entreprises à s'acquitter des obligations d'évaluation, de déclaration et de tenue d'un registre des atteintes que leur impose la *Loi sur la protection des renseignements personnels et les documents électroniques* (« **LPRPDE** »), notamment :

1. une série de vidéos explicatives pour le personnel des entreprises;
2. le rapport final de son premier exercice d'inspection des registres d'atteintes (le « **Rapport du CPVP** »);
3. un portail sécurisé de soumission de déclarations d'atteinte.

Ces ressources sont décrites ci-dessous.

Série de vidéos

Le CPVP a créé une série de six vidéos sur les atteintes aux mesures de sécurité au sens de la LPRPDE. Ces vidéos portent sur les sujets suivants :

- introduction à la déclaration des atteintes;
- évaluation des risques de préjudices graves;
- obligations des entreprises relativement à la déclaration des atteintes;
- comment soumettre une déclaration d'atteinte;
- quand et comment informer les personnes et les organisations;
- tenue des registres nécessaires.

Ces vidéos ne durent que quelques minutes et présentent des principes de base relatifs aux obligations imposées par la LPRPDE. Elles sont donc particulièrement utiles aux gens qui connaissent peu ces obligations.

Rapport final du CPVP concernant les inspections des registres d'atteintes 2019

Le Rapport du CPVP présente les conclusions et recommandations émanant du premier exercice d'inspection

des registres d'atteintes que doivent tenir les entreprises en vertu de la LPRPDE. En effet, l'article 10.3 de la LPRPDE indique que « [l']organisation tient et conserve, conformément aux règlements, un registre de toutes les atteintes aux mesures de sécurité qui ont trait à des renseignements personnels dont elle a la gestion ». Par ailleurs, aux termes du Règlement, ce registre doit :

- contenir tout renseignement permettant au CPVP de vérifier la conformité aux obligations en matière de déclaration et de notification des atteintes de l'organisation;
- être conservé pendant au moins 24 mois.

La première évaluation du CPVP a porté sur les obligations de tenue de registre de sept entreprises de télécommunications canadiennes (les « **Télécoms** ») par l'entremise d'un échantillon de 237 dossiers.

Son rapport détaillé peut être consulté sur son site Web.

Points saillants

Dans l'ensemble, le CPVP a trouvé que les Télécoms semblaient prendre leurs obligations en vertu de la LPRPDE au sérieux. Cela dit, le Rapport du CPVP fait état de quelques problèmes importants.

- **Information insuffisante pour l'évaluation du risque réel de préjudice grave (« RRPG »)**. Les inspections ont révélé que 40 % des dossiers de l'échantillon ne contenaient pas suffisamment d'information pour permettre au CPVP de bien comprendre comment est évalué le RRPG d'une atteinte. À cet égard, le CPVP indique que si une entreprise refuse de divulguer une partie d'un dossier en invoquant le secret professionnel de l'avocat, elle doit tout de même s'assurer que le dossier fourni contient tous les renseignements prescrits par la LPRPDE.
- **Possible erreur d'évaluation du RRPG**. Le rapport indique que 20 % des dossiers de l'échantillon mentionnaient des atteintes pour lesquelles le CPVP était en désaccord avec le constat d'absence de RRPG ou n'avait pas suffisamment d'information pour déterminer si l'atteinte avait causé ou non un RRPG. Malheureusement, le CPVP ne donne aucune précision sur ces cas de désaccord avec l'évaluation du RRPG; il aurait pu en profiter pour donner aux entreprises des lignes directrices utiles sur les critères minimaux à appliquer.
- **L'erreur humaine, une cause importante d'atteintes**. Le CPVP indique que 39 % des atteintes sont causées par une erreur humaine (tandis que seulement 21 % sont susceptibles d'impliquer une divulgation intentionnelle non autorisée). Ce constat démontre, une fois de plus, que la formation des employés est essentielle à la sécurité des données et à la prévention des atteintes.

Le Rapport du CPVP donne également quatre exemples d'atteintes, accompagnés d'une évaluation du RRPG. Ces exemples illustrent des situations courantes, soit le furetage par un employé, l'envoi d'un message au

mauvais destinataire, la perte d'un ordinateur portable et l'échange de cartes SIM. Malheureusement, le CPVP ne traite pas des attaques par rançongiciel qui semblent crypter les données sans les exfiltrer, ce qui aurait été utile à bon nombre d'entreprises vu l'essor récent de ce type d'attaque.

Le CPVP donne toutefois des conseils pour l'évaluation du RRPG. Il recommande notamment aux entreprises de consulter plusieurs membres de l'équipe de gestion des atteintes et d'utiliser une liste de contrôle ou une matrice pour uniformiser le processus. Le CPVP souligne l'importance de toujours tenir compte de la sensibilité des renseignements et de la probabilité qu'ils soient utilisés à mauvais escient. Le registre des atteintes doit d'ailleurs traiter de ces questions.

Enfin, le Rapport du CPVP contient quelques suggestions pour aider les entreprises à mettre au point et à améliorer leur programme de gestion des atteintes. Plus précisément, il exhorte les organisations à améliorer leur capacité à détecter et à corriger les tendances ou problèmes systémiques, en prenant notamment les mesures suivantes :

- S'assurer de tenir un registre suffisamment détaillé et de le conserver assez longtemps.
- Vérifier les angles morts qui peuvent indiquer une sous-déclaration au sein de l'entreprise.
- Transmettre au personnel des différents secteurs d'activité des connaissances sur la protection de la vie privée et les atteintes, et partager son expérience en la matière avec d'autres entreprises du même secteur.
- Faire appel aux cadres supérieurs et aux dirigeants qui peuvent contribuer à intégrer le respect de la vie privée à la culture et aux processus décisionnels de l'organisation.

Le Rapport du CPVP donne un aperçu de la position du CPVP quant aux obligations de déclaration et de tenue d'un registre des atteintes prévues dans la LPRPDE.

Portail de soumission de déclarations d'atteinte

Le nouveau portail du CPVP permet aux entreprises de soumettre leurs déclarations d'atteinte et de recevoir aussitôt un numéro de dossier pour leurs futures communications à ce sujet avec le CPVP. Pour soumettre une déclaration sur le portail, elles doivent fournir une adresse courriel, puis utiliser le lien qu'elles reçoivent à cette adresse.

Conclusion

Les atteintes aux mesures de sécurité constituent l'une des principales sources de préoccupation des entreprises de divers secteurs. La plupart d'entre elles trouveront les nouvelles ressources du CPVP fort utiles dans leurs démarches pour mettre en place ou améliorer leur cadre de prévention et de gestion des atteintes.

Or, il y a encore beaucoup de questions sans réponse. Par exemple, les critères minimaux de détermination d'un RRPG demeurent nébuleux. Les quatre exemples fournis par le CPVP donnent quelques indications, mais certaines situations courantes mériteraient des précisions. Enfin, le constat selon lequel le CPVP est (ou semble être) en désaccord avec les Télécoms dans environ 20 % des cas est problématique, notamment parce qu'il porte à croire que le CPVP considère que le seuil de déclaration est relativement bas.

par Lyndsay A. Wasser et Chiedza Museredza

Mise en garde