LES CINQ PRINCIPALES MESURES QUE VOUS N'APPLIQUEZ PROBABLEMENT PAS (MAIS QUE VOUS DEVRIEZ) POUR VOUS CONFORMER AUX LOIS CANADIENNES SUR LA PROTECTION DE LA VIE PRIVÉE : *MESURE Nº 3 : GESTION DES FOURNISSEURS*

Publié le 10 septembre, 2024

Catégories: Perspectives, Publications

En vertu des lois canadiennes sur la protection de la vie privée, les organisations qui transfèrent des renseignements personnels au sujet de clients, d'employés ou d'autres parties à un tiers fournisseur aux fins de traitement demeurent responsables de leur protection.

Par exemple, selon la *Loi sur la protection des renseignements personnels et les documents électroniques* (« **LPRPDE** ») du gouvernement fédéral, les organisations doivent fournir, par voie contractuelle ou autre, un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie. De même, la législation relative à la protection de la vie privée dans le secteur privé en Alberta et en Colombie-Britannique, ainsi que les lois provinciales sur la protection de la vie privée dans les secteurs public et de la santé, énoncent que les organisations demeurent responsables des renseignements personnels traités par les fournisseurs de services.

La *Loi sur la protection des renseignements personnels dans le secteur privé* du Québec (la « **Loi du Québec** ») permet à une personne qui exploite une entreprise de communiquer des renseignements personnels à un tiers fournisseur sans le consentement de la personne concernée si ces renseignements sont nécessaires à l'exécution d'un mandat ou d'un contrat d'entreprise ou de service. Toutefois, la personne qui exploite l'entreprise doit conclure avec le tiers fournisseur un contrat écrit comprenant les mesures que ce dernier doit prendre pour assurer la protection du caractère confidentiel, pour que ces renseignements ne soient utilisés que dans l'exercice de son mandat ou l'exécution de son contrat et pour qu'il ne les conserve pas après son expiration.

La Loi du Québec exige également qu'une personne qui exploite une entreprise procède à une évaluation des facteurs relatifs à la protection de la vie privée (« **EFVP** ») avant de confier à une personne ou à un organisme situé à l'extérieur du Québec la collecte, l'utilisation, la communication ou la conservation des renseignements

personnels en son nom. Le contrat écrit entre les parties (comme susmentionné) doit comprendre des modalités visant l'atténuation de tout risque relevé lors de l'EFVP. Pour obtenir plus d'information sur la réalisation d'une EFVP, veuillez consulter notre bulletin précédent ici.

La mauvaise gestion des renseignements personnels par un fournisseur peut exposer une organisation à des risques importants, notamment des plaintes en matière de protection de la vie privée, des enquêtes par les autorités de réglementation, des amendes et/ou des litiges, en plus des répercussions possibles sur la réputation de l'organisation et ses relations avec ses clients, ses employés et ses partenaires commerciaux. Par exemple, si un fournisseur fait l'objet d'une atteinte à la protection des renseignements personnels contrôlés par votre organisation, celle-ci pourrait être tenue de signaler l'incident aux autorités de réglementation de la protection de la vie privée, d'aviser les personnes concernées, de prendre des mesures pour atténuer les conséquences potentielles pour ces personnes et même d'engager des frais juridiques coûteux dans le cadre des procédures d'enquêtes de la part des autorités de réglementation ou de réclamations, ou des deux.

La protection des renseignements personnels transférés aux fournisseurs aux fins de traitement exige une approche à multiples volets, notamment :

- Effectuer une vérification diligente rigoureuse pour comprendre les politiques et pratiques du fournisseur en matière de protection de la vie privée et sa position relativement à la cybersécurité, ainsi que pour savoir si, par le passé, il a subi des atteintes à la protection des données, reçu des plaintes en matière de protection de la vie privée ou fait l'objet d'enquêtes, de réclamations ou d'autres litiges.
- La conclusion de modalités contractuelles appropriées avec les fournisseurs, y compris l'ensemble des modalités exigées par les lois applicables et recommandées dans les indications réglementaires pertinentes (voir, par exemple, les lignes directrices de l'autorité fédérale de réglementation de la protection de la vie privée sur le contenu des contrats écrits avec les fournisseurs dans les Conclusions en vertu de la LPRPDE n° 2019-001).
- Surveiller et, s'il y a lieu, vérifier périodiquement les fournisseurs pour s'assurer qu'ils respectent les lois sur la protection de la vie privée et des données et les modalités contractuelles applicables.
- S'assurer que les fournisseurs retournent ou détruisent de façon sécuritaire les renseignements personnels lorsqu'ils ne sont plus nécessaires pour fournir les services du fournisseur.

Si vous êtes un fournisseur offrant vos services à des entreprises canadiennes, il est tout aussi important de confirmer que vos contrats avec vos clients respectent les lois canadiennes applicables en matière de protection de la vie privée et les indications réglementaires, attribuent adéquatement la responsabilité et les risques liés aux atteintes à la protection des données, obtiennent un consentement valide, gèrent les demandes de droits d'utilisation des données et d'autres questions liées à la protection des renseignements

personnels et des données, et ne contiennent aucun engagement en matière de cybersécurité ou autre que votre organisation ne peut honorer. Vous devez également vous assurer que vos politiques et procédures en matière de protection de la vie privée et de cybersécurité peuvent résister à l'examen minutieux des clients potentiels et, en particulier, qu'elles tiennent compte des dispositions particulières des lois canadiennes sur la protection de la vie privée.

Mesures à adopter

Une gestion efficace des fournisseurs qui traitent des renseignements personnels au nom de votre organisation exige la prise des mesures proactives suivantes : (1) élaborer un questionnaire ou une liste de contrôle standard pour vérifier les pratiques en matière de protection des renseignements personnels et de sécurité des données des fournisseurs potentiels, ainsi que leurs produits et services; (2) élaborer des politiques et procédures internes concernant l'engagement de fournisseurs qui traitent des renseignements personnels; (3) rédiger un modèle d'addenda visant la protection des données et/ou établir des modalités des renseignements personnels et des données qui peuvent être incluses dans les contrats avec les fournisseurs; (4) examiner si les modalités contractuelles avec les fournisseurs actuels sont suffisantes, notamment pour tenir compte des récentes modifications statutaires et des indications réglementaires; (5) avant de retenir les services d'un fournisseur, réaliser les EFVP requises par les lois applicables ou par vos politiques et procédures internes; (6) élaborer un programme structuré pour contrôler le respect par les fournisseurs des lois applicables et de leurs obligations contractuelles; (7) former les employés aux processus de sélection et de contrôle des fournisseurs de votre organisation; (8) veiller à ce que les politiques de protection de la vie privée, les avis et la formulation du consentement de votre organisation décrivent avec précision la manière dont les fournisseurs traitent les données personnelles pour le compte de votre organisation.

Si vous êtes un fournisseur offrant vos services à des entreprises canadiennes, votre organisation devrait : (1) élaborer un modèle de contrat de protection des données et/ou établir un ensemble de dispositions relatives à la protection de la vie privée pouvant être inclus dans les contrats avec les clients pour lesquels votre organisation traite des renseignements personnels; (2) concevoir et maintenir un système de suivi du respect de vos engagements contractuels en matière de protection de la vie privée et de cybersécurité; et (3) veiller à ce que votre programme de conformité en matière de protection de la vie privée tienne compte des lois canadiennes applicables et des indications réglementaires, ainsi que des pratiques exemplaires en matière de cybersécurité, afin que vous soyez prêt à répondre aux demandes de vérification diligente de vos clients.

L'équipe du groupe Protection de la vie privée et des données de McMillan peut aider votre organisation à adopter les mesures ci-dessus. Nous vous invitons à communiquer avec votre représentant.e chez McMillan pour obtenir le soutien dont votre organisation a besoin en vue de respecter ces questions essentielles de conformité en matière de protection de la vie privée.

Par Lyndsay A. Wasser et Kristen Pennington

Mise en garde