PROJET DE LOI NO 64 : AIDE-MÉMOIRE À L'INTENTION DES ENTREPRISES

Publié le 7 décembre, 2021

Catégories: Perspectives, Publications

Le projet de loi n° 64, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (la « ***Loi modernisant la protection des renseignements personnels*** » ou la « ***Loi modifiée*** »)[1], qui a reçu la sanction royale le 22 septembre, apporte à la *Loi sur la protection des renseignements personnels dans le secteur privé* du Québec (la « ***Loi*** »)[2] des modifications qui la mettent au diapason de la nouvelle ère de protection des données et des dernières avancées mondiales en la matière.

Les modifications visent notamment à renforcer l'application de la *Loi* par l'ajout de mécanismes comme des sanctions administratives pécuniaires, un droit d'action privé et des amendes pouvant atteindre 25 millions de dollars pour les organisations contrevenantes.

Nous avons déjà consacré un bulletin aux nouveautés de la *Loi modernisant la protection des renseignements personnels*. Cette fois, nous présentons une liste de mesures concrètes à prendre en vue de leur entrée en vigueur, qui s'échelonnera sur trois ans.

La *Loi* s'applique-t-elle à mon organisation?

La Commission d'accès à l'information (la « **CAI** »), l'organisme de réglementation chargé de la protection de la vie privée au Québec, interprète largement le champ d'application de la *Loi*. Si une organisation recueille, utilise ou communique les renseignements personnels de personnes **situées au Québec**, la *Loi* s'appliquera fort probablement à son traitement de ces renseignements, et ce, même si elle n'a pas de bureau ni aucune autre installation dans la province[3]. La *Loi* s'appliquera concurremment avec la *Loi sur la protection des renseignements personnels et les documents électroniques* (la « **LPRPDE** »)[4] dans le cas des organisations de régie fédérale normalement visées par cette deuxième loi, comme les banques, les entreprises ferroviaires et les compagnies aériennes[5].

Par conséquent, toute organisation qui traite des renseignements personnels de personnes situées au Québec doit évaluer les effets que les modifications auront sur ses activités et mettre en place les changements nécessaires dès que possible.

Résumé des mesures à prendre pour respecter les nouvelles obligations

(cliquez ici pour voir toutes les mesures en une seule page)

D'ici le 22 septembre 2022

¨ Nommer un responsable de la protection des renseignements personnels (si ce rôle n'existe pas déjà).

- Le rôle de cette personne sera de veiller à ce que votre organisation respecte les obligations imposées par la *Loi modifiée*. Par défaut, cette responsabilité incombe à la personne exerçant la plus haute autorité dans l'entreprise (vraisemblablement le chef de la direction), mais elle peut être déléguée, en tout ou en partie, à une autre personne (à l'interne ou à l'externe).
- Au besoin, demandez au responsable par défaut de déléguer cette responsabilité par écrit au responsable que vous avez nommé.
- Publiez le titre et les coordonnées du responsable de la protection des renseignements personnels sur votre site Web.

¨ Revoir et mettre à jour votre plan d'intervention en cas d'atteinte à la protection des données.

- Dès que vous avez des raisons de croire qu'un incident de confidentialité (ex. : violation de données) impliquant des renseignements personnels dont vous avez la garde s'est produit, prenez des mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que des incidents de même nature ne se répètent.
    - Dans la *Loi modifiée*, « incident de confidentialité » s'entend de l'utilisation ou de la communication non autorisée par la loi de renseignements personnels, de l'accès non autorisé par la loi à des renseignements personnels, ainsi que de la perte de tels renseignements ou de tout manquement à leur protection.
- Avisez la CAI et toute personne concernée s'il y a un risque de préjudice sérieux[6].
- Certains facteurs doivent obligatoirement être pris en compte lors de l'évaluation du risque[7]. Les règlements qui seront pris ultérieurement donneront sans doute plus d'information quant à la forme que devra prendre l'avis. La CAI pourrait aussi publier des lignes directrices[8].

¨ Prendre connaissance des obligations associées à la communication de renseignements personnels dans le cadre d'une transaction commerciale.

- Lorsque la communication de renseignements personnels est nécessaire pour réaliser une transaction commerciale (ex. : fusion, vente d'actifs ou financement), vous pouvez les communiquer à une partie à la transaction sans le consentement de la personne concernée.

- Si votre entreprise transfert des renseignements personnels pour faciliter une telle transaction, concluez une entente (répondant à certains critères) visant à protéger les renseignements. Ces exigences se trouvent dans des régimes de protection de la vie privée partout au Canada.

D'ici le 22 septembre 2023

¨ Créer votre cadre de protection des renseignements et mettre à jour votre politique de confidentialité en ligne.

- Créez et mettez en œuvre un cadre de protection des renseignements personnels comprenant des politiques et des pratiques régissant l'utilisation et la protection de renseignements personnels par votre organisation[9]. Le cadre devrait prévoir un plan d'intervention en cas d'atteinte à la protection des données, des calendriers de conservation, les rôles et responsabilités des membres de l'organisation tout au long du cycle de vie des renseignements et des procédures pour les demandes d'accès et le traitement des plaintes.
- Publiez sur votre site Web de l'information détaillée, claire et simple sur ces politiques et pratiques[10].
- Si vous recueillez des renseignements personnels par des moyens technologiques, publiez une politique de confidentialité en langage clair et simple sur votre site Web[11].

¨ Établir un processus d'évaluation des facteurs relatifs à la vie privée.

- La réalisation d'une évaluation des facteurs relatifs à la vie privée (**EFVP**) est obligatoire pour tout projet d'acquisition, de développement ou de refonte de systèmes d'information ou de prestation de services électroniques impliquant des renseignements personnels[12].
    - Consultez votre responsable de la protection des renseignements personnels dès le début de l'EFVP. Il pourrait vous suggérer d'autres mesures de protection pertinentes pour le projet concerné[13].
    - Assurez-vous que le projet permet la communication, dans un format structuré et couramment utilisé, de renseignements personnels informatisés à la personne qu'ils concernent (la portabilité des données deviendra elle aussi obligatoire en 2024)[14].
- Procédez à une EFVP avant de communiquer des renseignements personnels à l'extérieur du Québec. L'EFVP doit tenir compte de certains facteurs, dont la sensibilité des renseignements, les fins auxquelles ils seront utilisés et le cadre juridique étranger applicable là où ils seront communiqués[15].
    - Si vous communiquez des renseignements personnels à l'extérieur du Québec, rédigez et utilisez une entente écrite qui aborde les résultats de l'EFVP et, le cas échéant, qui contient des modalités sur l'atténuation des risques qui y ont été décelés.
- Consultez le guide d'accompagnement de la CAI[16] pour vérifier que votre processus d'EFVP répond aux

attentes de l'organisme de réglementation.
- Pensez à embaucher des experts en matière de protection de la vie privée qui vous aideront à réaliser vos EFVP et à vous conformer à la *Loi modifiée*, surtout si vous exploitez une entreprise d'envergure. Si, dans le cours normal de vos activités, vous faites affaire avec beaucoup de fournisseurs de services ou réalisez beaucoup de projets technologiques, cette obligation pourrait être très lourde.

¨ Conclure des contrats avec vos fournisseurs de services ou réviser les contrats existants.

- La *Loi modifiée* n'exige pas de consentement lorsque des renseignements sont transmis à un tiers (comme un fournisseur de services), dans la mesure où ils sont nécessaires à l'exécution d'un mandat ou d'un contrat d'entreprise ou de services[17].
- Si vous communiquez des renseignements personnels à un fournisseur de services, vous devez conclure avec lui un contrat écrit qui prévoit : (i) une liste des mesures qu'il doit prendre pour protéger les renseignements personnels qui lui sont communiqués, (ii) une obligation pour le fournisseur d'utiliser les renseignements uniquement dans le but d'exécuter le contrat, (iii) une obligation pour le fournisseur de ne pas conserver les renseignements après l'expiration du contrat, et (iv) une obligation pour le fournisseur d'informer sans délai le responsable de la protection des renseignements personnels de toute atteinte ou tentative d'atteinte à la confidentialité des renseignements personnels et de lui permettre de procéder à une vérification du respect des mesures de protection[18].
- Si le fournisseur traite des renseignements personnels à l'extérieur du Québec, une EFVP doit être réalisée (voir la section sur les EFVP ci-dessus)[19].

¨ Évaluer vos mesures de protection physiques, organisationnelles et technologiques.

- Si l'obligation de mettre en place des mesures de protection n'a pas changé[20], les sanctions imposées en cas de non-conformité seront bien plus importantes sous le régime de la *Loi modernisant la protection des renseignements personnels*. Les amendes salées et la prolifération de la cybercriminalité attribuable à la pandémie justifient de revoir vos mesures de protection pour confirmer qu'elles sont toujours adéquates.

¨ Revoir votre protection d'assurance.

- Les risques de responsabilité sont accentués vu les amendes, les sanctions et le droit d'action privé introduits par la *Loi modifiée*.
- Renégociez votre assurance contre les cyberrisques pour vous assurer que votre organisation est adéquatement protégée.

¨ Prendre connaissance des nouvelles exigences et exceptions en matière de consentement.

- Le consentement doit être « manifeste, libre et éclairé »[21], comme l'exige actuellement la *Loi*[22], mais la nouvelle version signale l'acceptabilité du consentement implicite dans certaines circonstances[23].
- Un consentement exprès est nécessaire en présence de renseignements sensibles[24]. Sont notamment considérés comme sensibles les renseignements pour lesquels il y a un haut degré d'attente raisonnable de respect de la vie privée, comme les renseignements médicaux, biométriques ou autrement intimes[25].
- Prenez connaissance des nouvelles exceptions, surtout si vous utilisez des renseignements personnels à d'autres fins que celles pour lesquelles ils ont été recueillis[26]. Aux termes de la *Loi modifiée*, il n'est pas nécessaire d'obtenir un consentement lorsque la nouvelle utilisation est, selon le cas :

    i. à des fins compatibles avec celles pour lesquelles ils ont été recueillis;
    ii. manifestement au bénéfice de la personne concernée;
    iii. nécessaire aux fins de prévention de la fraude ou de l'évaluation ou l'amélioration des mesures de protection et de sécurité;
    iv. nécessaire à la fourniture ou à la livraison de produits ou à la prestation de services demandés par la personne concernée;
    v. nécessaire à des fins d'étude, de recherche ou de production de statistiques et que les renseignements sont dépersonnalisés[27].

- Obtenez le consentement d'une personne titulaire de l'autorité parentale à la collecte, l'utilisation ou la communication de renseignements concernant un mineur de moins de 14 ans, sauf si elle est manifestement dans l'intérêt du mineur[28].

¨ Mettre à jour vos formulaires de consentement et mettre en œuvre un système de gestion du consentement.

- Lorsque vous recueillez des renseignements auprès d'une personne, vous devez l'informer :

    i. des fins auxquelles ces renseignements sont recueillis;
    ii. des moyens par lesquels les renseignements sont recueillis;
    iii. de ses droits d'accès et de rectification;
    iv. de son droit de retirer son consentement[29].

- Le cas échéant, donnez-lui le nom du tiers pour qui la collecte est effectuée. La personne doit être informée du nom du tiers ou de la catégorie à laquelle il appartient, ainsi que de la possibilité que ses renseignements soient communiqués à l'extérieur du Québec.
- Pour être valide, une demande de consentement doit être faite en termes clairs et simples et préciser toutes les fins auxquelles la personne doit consentir. Si la demande est faite par écrit, elle doit être

présentée indépendamment de toute autre information communiquée à la personne.
- Tout consentement ne respectant pas les exigences de la *Loi modifiée* sera nul et sans effet[30]. Vous auriez donc avantage à mettre en place un système de gestion du consentement pour consigner les consentements qui ont été donnés et repérer les situations où un consentement supplémentaire est nécessaire.

¨ Prendre connaissance de vos obligations de transparence (notamment en matière de suivi et de profilage).

- Informez la personne qui le demande des renseignements personnels que vous recueillez à son sujet, des catégories de personnes qui y ont accès au sein de votre entreprise, de la durée de leur conservation et des coordonnées de la personne chargée de les protéger[31].
- Si vous recueillez de l'information sur une personne à l'aide d'une technologie permettant de l'identifier, de la localiser ou d'effectuer son profilage, informez cette personne de votre utilisation de la technologie et des moyens permettant de l'activer (elle devrait par défaut être désactivée)[32].
- Lorsque les circonstances l'exigent, informez les personnes concernées de votre utilisation de processus de prise de décision automatisés (voir la section sur les avis relatifs à la prise de décision automatisée ci-dessous).

¨ Établir des paramètres de confidentialité par défaut.

- Configurez les produits ou services technologiques destinés au public de façon à ce qu'ils offrent par défaut le plus haut niveau de confidentialité[33]. Les témoins ne sont pas visés par cette exigence[34].

¨ Revoir et mettre à jour vos calendriers de conservation.

- Vous devez conserver les renseignements personnels utilisés pour prendre une décision à propos d'une personne pendant au moins un (1) an. Cette exigence s'arrime à celle qui est prévue dans la LPRPDE et les autres lois sur la protection de la vie privée au Canada[35].
- Lorsque les renseignements ne sont plus nécessaires, et sous réserve de toute période de conservation imposée par la loi, vous devez les détruire ou les anonymiser pour les utiliser à des fins sérieuses et légitimes[36].

¨ Revoir votre processus d'anonymisation des données (le cas échéant).

- L'anonymisation des données vous permet de les utiliser à des fins non initialement prévues sans obtenir de consentement supplémentaire. Notez qu'il est très difficile de réaliser une anonymisation effective.
- Aux termes de la *Loi modifiée*, les renseignements personnels sont réputés « anonymisés » à partir du moment où on peut raisonnablement s'attendre à ce qu'ils ne permettent plus d'identifier la personne

concernée, directement ou indirectement, et ce de manière irréversible[37].
- Anonymisez les données conformément aux pratiques exemplaires généralement acceptées. Des règlements à venir préciseront la teneur de ces pratiques[38].

¨ Préparer des avis et des explications relativement à la prise de décision automatisée.

- Avisez la personne concernée lorsque vous prenez une décision fondée uniquement sur le traitement automatisé de renseignements personnels recueillis à son sujet[39].
- À la demande de cette personne, vous devez l'informer (i) des renseignements personnels utilisés pour prendre la décision, (ii) des raisons, ainsi que des principaux facteurs et paramètres, ayant mené à la décision, et (iii) de son droit de faire rectifier les renseignements[40].
- Évaluez votre utilisation de processus décisionnels automatisés et préparez-vous à les expliquer en termes clairs et simples.

D'ici le 22 septembre 2024

¨ Veiller à ce que vos systèmes de gestion des données permettent leur extraction et leur transfert.

- La *Loi modifiée* prévoit qu'une personne peut demander que ses renseignements personnels lui soient communiqués ou transférés, à elle-même ou à une entreprise tierce, dans un format structuré et couramment utilisé.
- Ce droit ne s'applique pas aux renseignements générés et déduits à partir de renseignements personnels (ex. : statistiques concernant la personne) ni lorsqu'il y a des difficultés pratiques sérieuses.
- Le respect de cette obligation pourrait nécessiter beaucoup de temps, et peut-être même une refonte des systèmes de traitement des données, selon, par exemple, le format des données et le degré de dissociabilité des renseignements personnels de la personne concernée, des renseignements exclusifs et des renseignements sur d'autres personnes.

Pour savoir comment bien vous préparer à ces changements, communiquez avec un avocat de notre groupe Protection de la vie privée et cybersécurité.

(cliquez ici pour voir toutes les mesures en une seule page)

[1]*Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, LQ 2021, c 25.
[2] *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ, c P-39.1.

[3] Conclusions en vertu de la LPRPDE n° 2021-001, 2 février 2021, paragr. 34.
[4] *D'Allaire c. Transport Robert (Québec) 1973 ltée*, 2020 QCCAI 152.

[5] *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5.
[6] *Loi modifiée*, art 3.5.
[7] *Loi modifiée*, art 3.7.
[8] *Loi modifiée*, art 3.5. La CAI a également conçu une page consacrée à la *Loi modernisant la protection des renseignements personnels*; voir en ligne.
[9] *Loi modifiée*, art 3.2.
[10] *Loi modifiée*, art 3.2.
[11] *Loi modifiée*, art 8.2.
[12] *Loi modifiée*, art 3.3.
[13] *Loi modifiée*, art 3.4.
[14] *Loi modifiée*, art 3.3.
[15] *Loi modifiée*, art 17.
[16] Commission d'accès à l'information du Québec, *Guide d'accompagnement. Réaliser une évaluation des facteurs relatifs à la vie privée*, mars 2021, accessible en ligne.
[17] *Loi modifiée*, art 18.3.
[18] *Loi modifiée*, art 18.3.
[19] *Loi modifiée*, art 17.
[20] *Loi*, art 10.
[21] *Loi modifiée*, art 14.
[22] *Loi*, art 14.
[23] Voir, par exemple, l'article 8.3 de la *Loi modifiée*, qui indique qu'une personne qui soumet ses renseignements après avoir reçu les avis nécessaires consent à leur utilisation et à leur communication aux fins qui ont été déclarées.
[24] *Loi modifiée*, art 12.
[25] *Loi modifiée*, art 12.
[26] *Loi modifiée*, art 12.
[27] *Loi modifiée*, art 12.
[28] *Loi modifiée*, art 4.1.
[29] *Loi modifiée*, art 8.
[30] *Loi modifiée*, art 14.
[31] *Loi modifiée*, art 8.
[32] *Loi modifiée*, art 8.1.
[33] *Loi modifiée*, art 9.1.
[34] *Loi modifiée*, art 9.1.

[35] *Loi modifiée*, art 11.
[36] *Loi modifiée*, art 23.
[37] *Loi modifiée*, art 23.
[38] *Loi modifiée*, art 23.
[39] *Loi modifiée*, art 12.1.
[40] *Loi modifiée*, art 12.1.

par Robbie Grant et Marie-Eve Jean

Mise en garde