大成 DENTONS

Modernisation des dispositions législatives du Québec en matière de protection des renseignements personnels (projet de loi 64)

Un guide pratique

Le projet de loi n° 64 (PL64) du gouvernement du Québec, la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, a été adopté à l'unanimité par l'Assemblée nationale du Québec le 21 septembre 2021 et a reçu la sanction royale dès le lendemain, soit le 22 septembre 2021. Le temps est donc venu pour bon nombre de sociétés et d'organisations de commencer à se préparer, car bien que la majorité des dispositions entreront en vigueur dans deux ans, la transformation organisationnelle que la nouvelle loi entraîne est importante (vous devrez y consacrer le temps et les ressources nécessaires). Pour se conformer à la nouvelle loi, les organisations doivent : i) établir des processus de gouvernance des données, y compris des processus destinés à aider les particuliers à exercer leurs nouveaux droits en matière de protection de la vie privée, ii) élaborer des politiques de gestion des données, iii) adopter des solutions technologiques permettant de désindexer ou de transférer les renseignements personnels sur demande, et iv) publier des lignes directrices internes pour aider les membres de leur personnel et leurs fournisseurs de services à se conformer au nouveau régime de protection de la vie privée.

Le Québec est l'une des premières provinces au Canada à entreprendre une réforme en profondeur de ses lois en matière de protection des renseignements personnels. Vous devez vous préparer en vue des changements que la nouvelle loi instaure, même si vous êtes d'avis que votre organisation n'est pas régie par le droit québécois.

Table des matières

Pourquoi la nouvelle loi québécoise s'applique-t-elle au-delà du Québec?

Deux facteurs principaux font que la nouvelle loi déborde des frontières du Québec. Premièrement, le Québec considère que ses lois sur la protection des renseignements personnels s'appliquent à toute collecte de renseignements personnels effectuée au Québec, quel que soit le cadre général régissant l'organisation qui recueille les renseignements. Par conséquent, l'organisme de réglementation de la protection de la vie privée du Québec, la Commission d'accès à l'information (CAI), exerce régulièrement sa compétence sur les activités commerciales exercées par des entreprises, affaires ou ouvrages qui relèvent de la compétence fédérale, à savoir des entités qui sont régies par la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) du Canada. Cette position élargit considérablement la portée de la nouvelle loi.

Deuxièmement, comme cela a été dit plus haut, la nouvelle loi établit un précédent au Canada dans le domaine de la protection des renseignements personnels. Inspirée du *Règlement général sur la protection des données* (RGPD) de l'Union européenne, la nouvelle loi québécoise place la barre plus haut en introduisant de nouvelles normes pour les droits individuels à la vie privée. Ces normes gagnent déjà du terrain au-delà des frontières de la province. En lisant le livre blanc du gouvernement de l'Ontario concernant les intentions de la province à l'égard d'une loi provinciale pour le secteur privé ainsi que la réponse de la commissaire à l'information et à la protection de la vie privée de l'Ontario à ce livre blanc, on ne peut que remarquer le nombre de références qui sont faites au PL64 afin de soutenir l'adoption de protections similaires pour les particuliers en Ontario.

La question est donc de savoir comment se préparer au mieux à ces changements substantiels qui sont apportés au cadre réglementaire canadien en matière de protection des renseignements personnels.

Comment se préparer, maintenant que le PL64 a reçu la sanction royale

Certains des changements que le PL64 proposait sont des pratiques courantes depuis plusieurs années (même si leur application n'était pas encore obligatoire au Québec), ce qui veut dire que leur mise en œuvre ne devrait pas présenter un trop grand défi. Par exemple, les organisations seront désormais tenues de désigner une personne responsable de la conformité avec la législation applicable en matière de protection des renseignements personnels. D'autres lois, comme la LPRPDE, imposent déjà une telle obligation, ce qui fait que de tels responsables ont déjà été désignés dans bon nombre d'organisations. De même, le PL64 introduit l'obligation de signaler toute violation de la vie privée, une obligation que prévoient déjà d'autres lois canadiennes, dont la *Personal Information Protection Act* de l'Alberta et la LPRPDE. Toutefois, le PL64 introduit de nouveaux droits et obligations en matière de protection des renseignements personnels, ce qui obligera les organisations à s'assurer que leurs processus, leurs politiques et leurs technologies sont adéquats.

Évaluation des facteurs relatifs à la vie privée (EFVP)

Dorénavant, les organisations seront tenues de réaliser une évaluation des facteurs relatifs à la vie privée :

i) pour tout projet de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels; ii) avant de communiquer un renseignement personnel à l'extérieur du Québec; et iii) avant de communiquer des renseignements personnels sans le consentement des personnes concernées à une personne ou un organisme qui souhaite les utiliser à des fins d'étude, de recherche ou de production de statistiques.

Cette nouvelle exigence obligera bon nombre d'organisations à apporter des changements sur le plan de la gouvernance des données, à réviser leurs politiques internes et à communiquer aux membres de leur personnel des lignes directrices sur l'EFVP.

QUOI FAIRE POUR VOUS PRÉPARER :

En ce qui concerne la gouvernance des données, nous vous recommandons d'établir un processus de communication et de collaboration entre les membres de votre personnel et le responsable de la protection des renseignements personnels que vous désignerez, à l'égard de tout projet ou initiative qui pourrait nécessiter une EFVP.

De plus, vous devriez réfléchir aux façons dont vous allez procéder aux EFVP requises, en fonction de vos activités et de votre mode de fonctionnement. Étant donné que des EFVP doivent être réalisées à l'égard des programmes et initiatives des institutions fédérales depuis des décennies, nous vous invitons à lire la **Directive sur l'évaluation des facteurs relatifs à la vie privée** du Conseil du Trésor du Canada et à vous en servir comme point de départ pour élaborer et mettre en œuvre une politique similaire.

Les membres de votre personnel auront besoin de lignes directrices lorsqu'ils auront à prendre des décisions concernant le traitement, y compris le stockage, de renseignements personnels à l'extérieur du Québec. Les organisations sont désormais tenues de prendre en compte le « cadre juridique applicable dans l'État où l'information serait communiquée, y compris les principes de protection des données dans l'État étranger » ainsi que la sensibilité des informations avant de les communiquer à l'extérieur du Québec. Elles doivent s'assurer que les renseignements bénéficieront d'une protection « adéquate » dans le pays étranger. Comme cela peut être complexe, les membres de votre personnel qui seront chargés d'effectuer de telles évaluations et de négocier avec les prestataires de services auront besoin de lignes directrices claires. Il serait bon notamment d'établir un processus d'examen et des critères précis, voire d'établir la liste des pays qui offrent des protections que votre organisation juge acceptables en ce qui a trait au transfert licite de renseignements personnels.

Obligations plus sévères en matière de consentement et de transparence

Le PL64 précise les exigences de transparence existantes et en introduit de nouvelles en matière de consentement. Le consentement doit être obtenu pour chaque utilisation de renseignements personnels et le consentement implicite n'est accepté que dans certaines situations. Par exemple, le consentement implicite ne peut pas être invoqué pour le traitement de renseignements personnels sensibles (le consentement explicite est requis dans un tel cas). Dans le cadre de la nouvelle loi, les renseignements personnels de nature « *médicale, biométrique ou autrement intime* » sont désormais considérés comme des renseignements personnels sensibles. Le contexte reste un facteur à considérer dans la détermination du caractère sensible d'un renseignement personnel.

QUOI FAIRE POUR VOUS PRÉPARER :

Vous devriez revoir vos mécanismes de consentement et vos politiques de protection des renseignements personnels pour vous assurer qu'ils sont conformes aux nouvelles obligations législatives, comme celle d'obtenir un consentement distinct pour chaque finalité. Vous devriez également revoir les politiques de protection des renseignements personnels que vous publiez à l'externe pour vous assurer qu'elles communiquent les renseignements requis aux particuliers. Ces politiques devraient par exemple expliquer dans un langage clair et simple dans quels cas votre organisation prend des décisions fondées exclusivement sur un traitement automatisé des renseignements.

Dépersonnalisation et anonymisation des renseignements

La nouvelle loi réglemente l'utilisation de renseignements dépersonnalisés et anonymisés. Pour l'application de la nouvelle loi, un renseignement personnel est « *dépersonnalisé* » lorsque ce renseignement « *ne permet plus d'identifier directement la personne concernée* » (le mot-clé ici est « *directement* »). Un renseignement concernant une personne physique est « *anonymisé* » lorsqu'il « *ne permet plus, de façon irréversible, d'identifier directement ou indirectement cette personne* » (les mots-clés ici sont « *irréversible* » et « *directement ou indirectement* »). La distinction est essentielle, car c'est ce qui permet de déterminer l'utilisation qui est permise pour chaque type de renseignement. Par exemple, une exception au consentement à l'utilisation de renseignements dépersonnalisés est prévue dans la loi lorsque l'utilisation est nécessaire à des fins d'étude, de recherche ou de production de statistiques. Les renseignements dépersonnalisés sont toujours des renseignements personnels, ce qui veut dire qu'ils sont soumis à des restrictions et à des exigences, telles que l'obligation pour les organisations utilisant des renseignements dépersonnalisés de prendre des mesures raisonnables pour réduire le risque que quiconque puisse identifier une personne physique en utilisant des renseignements dépersonnalisés.

Lorsque les fins auxquelles un renseignement personnel a été recueilli sont accomplies, voici les deux options qui s'offrent à l'organisation : elle peut détruire les renseignements ou elle peut les anonymiser « *en raison d'un intérêt sérieux et légitime* » selon « *les meilleures pratiques généralement acceptées* ».

QUOI FAIRE POUR VOUS PRÉPARER :

En vertu des nouvelles définitions qui clarifient la signification de « *renseignements dépersonnalisés* » et de « *renseignements anonymisés* », les organisations qui s'engagent dans des pratiques d'anonymisation doivent examiner attentivement leurs processus technologiques afin de s'assurer qu'elles respectent toutes les normes visées et que l'utilisation qu'elles font de chaque type de renseignements est conforme à la loi.

Il est important de prendre note que la loi prévoit l'imposition de sanctions pécuniaires élevées à quiconque procéderait ou tenterait de procéder à l'identification d'une personne à partir de renseignements dépersonnalisés ou anonymisés sans l'autorisation de la personne concernée. L'amende maximale rattachée aux sanctions pénales est de 100 000 $ CA pour un particulier et de 25 millions $ CA ou 4 % du chiffre d'affaires mondial de l'exercice financier précédent pour une société. Compte tenu du montant des amendes auxquelles votre organisation s'expose, vous devriez vous assurer que vos mesures de conformité internes sont fiables.

Décision fondée exclusivement sur un traitement automatisé

S'inspirant du RGPD, la nouvelle loi introduit des exigences relatives aux décisions fondées exclusivement sur un traitement automatisé de renseignements personnels, c'est-à-dire sans l'intervention d'un être humain.

QUOI FAIRE POUR VOUS PRÉPARER :

Pour répondre aux exigences de la nouvelle loi, les organisations qui utilisent des renseignements personnels afin que soit rendue une décision fondée exclusivement sur un traitement automatisé devront mettre à jour leurs politiques de protection des renseignements personnels et créer de nouveaux mécanismes pour l'exercice de droits individuels. Plus précisément, elles devront s'assurer que leurs politiques prévoient des mécanismes pour informer les particuliers que la décision est fondée exclusivement sur un traitement automatisé des renseignements au moment où la décision est rendue ou avant. Elles devront également établir un processus permettant aux particuliers de demander l'accès aux renseignements personnels utilisés pour rendre la décision, les motifs et les principaux facteurs et paramètres qui ont conduit à la décision, ainsi que les renseignements utilisés pour corriger la décision, le cas échéant. Les organisations devront également établir un processus afin de permettre à un particulier de « présenter ses observations » concernant la décision.

Un nouveau droit à la portabilité des données

Les États-Unis ont déjà légiféré sur le droit à la portabilité dans certains domaines, ce qui a mis en lumière les défis technologiques importants à relever et la complexité du développement de l'infrastructure interopérable nécessaire pour y donner effet. La nouvelle loi du Québec donne trois ans aux organisations, à compter 22 septembre (date à laquelle le projet de loi 64 a reçu la sanction royale), pour développer et installer les mécanismes nécessaires à la communication de renseignements personnels « *dans un format technologique structuré et couramment utilisé* ». L'expérience nous montre qu'il s'agit d'une tâche lourde et complexe, qui nécessite du temps et des ressources.

QUOI FAIRE POUR VOUS PRÉPARER :

En plus de travailler à développer l'infrastructure technologique nécessaire pour répondre aux demandes de portabilité des données, vous devrez élaborer des lignes directrices à l'intention des membres de votre personnel afin que ces derniers puissent répondre adéquatement aux demandes en question. Étant donné que la loi ne s'applique qu'aux « *renseignements personnels informatisés recueillis auprès du requérant* » et « *non pas créés ou inférés à partir d'un renseignement personnel le concernant* », vous devriez former les membres de votre personnel et leur fournir les outils et l'information dont ils ont besoin pour bien identifier les renseignements personnels à communiquer et les moyens à prendre pour les communiquer.

Droit à l'oubli

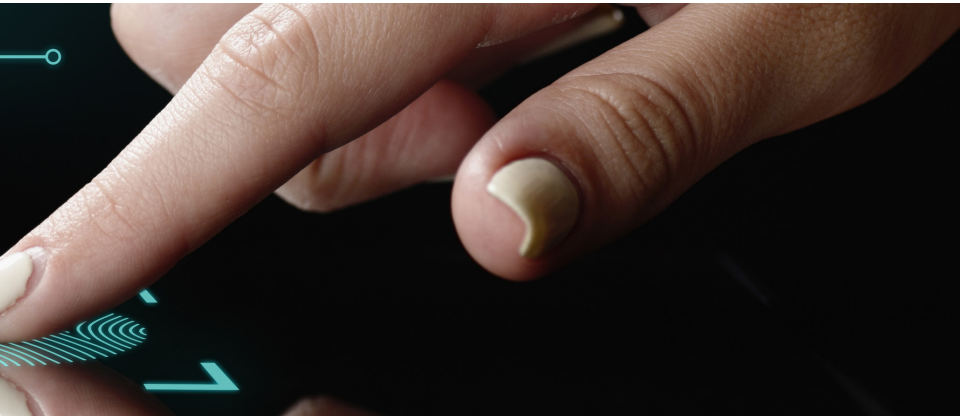
La nouvelle loi introduit le « *droit à l'oubli* » (qui n'est pas sans rappeler un droit similaire prévu par le RGPD), qui permettra à une personne d'exiger d'une organisation qu'elle cesse de distribuer ses renseignements personnels ou qu'elle « *désindexe* » un hyperlien donnant accès à ces renseignements par des moyens technologiques, sous réserve de certaines conditions.

Outre le « *droit à l'oubli* », la personne pourra exiger d'une organisation qu'elle corrige les renseignements la concernant si ces renseignements sont « *inexacts, incomplets ou équivoques* » ou si leur collecte, leur communication ou leur conservation ne sont pas autorisées par la loi. Lorsque les renseignements sont périmés ou lorsqu'ils ne sont plus nécessaires pour l'atteinte d'une fin déterminée, la personne pourra demander à ce qu'ils soient supprimés.

QUOI FAIRE POUR VOUS PRÉPARER :

En ce qui concerne l'application du droit à l'oubli, un juste équilibre doit être trouvé entre le droit des particuliers de faire supprimer des renseignements et les répercussions que la suppression de renseignements qui circulent librement sur Internet entraînera.

La nouvelle loi fournit une liste de facteurs dont vous devez tenir compte lorsque vous évaluez des demandes de suppression de renseignements, mais vous devriez élaborer vos propres lignes directrices afin de tenir compte d'autres considérations qui pourraient s'appliquer. L'établissement de ces lignes directrices sera un élément essentiel de la structure de gouvernance de chaque organisation afin de garantir une mise en œuvre adéquate et d'éviter les plaintes.



Mise en application

S'éloignant du modèle de l'ombudsman, en vertu duquel l'organisme de réglementation fait des recommandations aux organisations, la nouvelle loi québécoise permet à la Commission d'accès à l'information (CAI) du Québec d'imposer de lourdes sanctions administratives pécuniaires en cas de violation de la loi. Ces sanctions peuvent atteindre 50 000 $ CA pour les personnes physiques et 10 millions $ CA ou 2 % du chiffre d'affaires mondial de l'exercice financier précédent, si ce dernier est plus élevé, pour les organisations. Lorsque la violation constitue une infraction, le montant des amendes pourra atteindre 100 000 $ CA pour une personne physique et 25 millions $ CA ou 4 % du chiffre d'affaires mondial de l'exercice financier précédent pour les organisations.

QUOI FAIRE POUR VOUS PRÉPARER :

Le nouveau risque financier lié aux violations de la vie privée exige une réponse proportionnelle, qui passe par le renforcement de vos processus de conformité internes. Vous devez vous assurer que votre structure de gouvernance des données et que les responsabilités à l'égard de ces dernières sont claires et mettre à jour vos programmes de protection des renseignements personnels de façon à assigner les obligations visées. Si vous ne l'avez pas encore fait, vous devriez adopter des mesures de protection administratives robustes et vous doter d'un protocole de gestion et d'intervention en cas d'atteinte à la vie privée conforme à ce que la loi prévoit.

Ces mesures organisationnelles favoriseront la conformité afin d'éviter les sanctions et permettront à votre organisation de démontrer qu'elle fait preuve de diligence raisonnable.

ET MAINTENANT?

Commencez dès maintenant à planifier les prochaines étapes. Vous devriez confier à une personne (un membre de votre personnel ou un expert externe) la tâche d'identifier les changements qui seront requis au sein de votre organisation pour vous conformer à la nouvelle loi, les ressources dont vous aurez besoin pour y arriver et les processus que vous devez suivre. Les périodes de transition d'un an, de deux ans et de trois ans prévues par la loi s'écouleront rapidement.

Si vous avez des questions, veuillez communiquer avec

Chantal Bernier
Avocate-conseil, Ottawa
D +1 613 783 9684
chantal.bernier@dentons.com

Alexandra Quigley
Avocate principale, Montréal
D +1 514 878 5856
alexandra.quigley@dentons.com

Sasha Coutu
Avocate, Ottawa
D +1 613 288 2708
sasha.coutu@dentons.com

Á PROPOS DE DENTONS

Cabinet d'avocats le plus important au monde, Dentons relève tous les défis et répond à chaque opportunité grâce au talent de ses 20 000 professionnels, dont 12 000 avocats, répartis dans plus de 200 bureaux et 80 pays. L'approche polycentrique de Dentons, sa culture de l'objectif, son engagement en faveur de l'inclusion et de la diversité, son service client primé défient le statu quo pour faire progresser les intérêts des clients.

dentons.com

CSBrand-71633-Bill-64-on-modernizing-Québec-privacy-A-law-A-practical-guide-5x7-FR-07 — 29/10/2021