Loi 64 : Le Québec modernise ses dispositions législatives en matière de protection des renseignements personnels

Pourquoi est-ce important et de quelle façon pouvez-vous vous préparer?

Partie 1 - Jeudi 14 octobre 2021

大成 DENTONS

Conférencières

Chantal Bernier
Avocate-conseil, Ottawa
chantal.bernier@dentons.com

Chantal Bernier dirige le groupe de pratique canadien Cybersécurité et protection de la vie privée de Dentons et est membre du groupe Affaires et politiques gouvernementales du cabinet.

Elle conseille des entreprises nationales et internationales de premier plan dans le cadre de l'expansion de leurs activités au Canada et en Europe, de leur entrée sur le marché du commerce électronique, de la mise en place d'outils d'analyse des données et du déploiement d'initiatives de mise en marché fondées sur les données.

Elle compte parmi ses clients des sociétés de technologies publicitaires, des institutions financières, des sociétés de biotechnologie, des entreprises spécialisées dans l'analyse des données et des institutions gouvernementales.

Alexandra Quigley
Avocate principale, Montréal
alexandra.quigley@dentons.com

Alexandra Quigley est membre du groupe Litiges et règlement des différends du bureau de Montréal de Dentons. Elle se spécialise dans les litiges civils et commerciaux.

Alexandra a été appelée à effectuer divers mandats en litige civil et commercial et a plaidé devant la Cour du Québec, la Cour Supérieure et la Cour d'appel.

Elle conseille plusieurs entreprises en matière de protection des renseignements personnels et est inscrite à la maîtrise en droit des technologies de l'information à l'Université de Montréal.

Agenda

1. La pertinence de la nouvelle loi québécoise au-delà du Québec
2. Le coup de barre: l’introduction de risques financiers
3. Des obligations accrues
4. De nouveaux droits individuels
5. La règlementation des données dépersonnalisées et anonymisées
6. Les transformations organisationnelles qui s’imposent
7. 5 leçons apprises de la révision de programmes de la PRP

L’importance de la Loi 64

La Loi 64 s’applique au Québec avec une incidence hors Québec

- La Commission d’accès à l’information (CAI) exerce régulièrement sa compétence même sur des organisations qui relèvent de la *Loi sur la protection des renseignements personnels et documents électroniques* (LPRPDÉ)

- La loi 64 crée un précédent au Canada qui pourrait se refléter dans les autres réformes provinciales.

Un nouvel enjeu : les risques financiers

1. Sanctions administratives pécuniaires

La CAI peut imposer une amende maximale de 10 M$ ou de 2 % du chiffre d'affaires de l'organisme, selon le montant le plus élevé

Violations :

- Refus de communiquer l'information en vertu de l'obligation de transparence du traitement des renseignements personnels
- Traitement des renseignements personnels en contravention de la Loi
- Défaut d'aviser la CAI ou les personnes concernées d'un incident de confidentialité présentant un risque de préjudice sérieux
- Défaut de mettre en place les mesures de sécurité nécessaires
- Refus de communiquer les motifs d'une décision automatisée
- Contravention aux obligations applicables aux agents de renseignements personnels

2. Nouvelles infractions pénales et amendes

Un tribunal peut imposer une amende maximale de 25 M$ ou de 4 % du chiffre d’affaires de l’organisme responsable, selon le montant qui est le plus élevé

Violations :

- Traitement de renseignements personnels en contravention à la loi
- Défaut d’aviser la CAI ou les personnes concernées d’un incident de confidentialité qui présente un risque de préjudice sérieux
- Demande de communication de renseignements protégés par un gel de sécurité
- Défaut de protéger les renseignements
- Ré-identification ou tentative de ré-identification sans autorisation
- Contravention aux obligations des agents de renseignements personnels
- Obstruction à une enquête de la CAI
- Rétribution contre un plaignant ou une personne collaborant avec la CAI
- Refus de produire des documents exigés par la CAI ou de se conformer à une ordonnance de la CAI

3. Droit privé d’action

Les tribunaux peuvent octroyer des dommages punitifs d’au moins 1 000 $ lorsque l’atteinte est intentionnelle ou résulte d’une faute intentionnelle.

Violations :

- Des dispositions de la Loi
- Des dispositions des articles du Code civil du Québec sur le droit au respect de la réputation et de la vie privée.

Des obligations accrues

1. Obligations relatives aux incidents de confidentialité

Obligation de signalement

- Aviser la CAI et les personnes concernées s'il y a risque d'un préjudice sérieux
- Tenir un registre des incidents
- Envoyer le registre à la CAI, sur demande

Obligations subséquentes au signalement

- Diminuer les risques de préjudice
- Prévenir les incidents subséquents de même nature

« Incident de confidentialité » :

- Accès, utilisation ou communication non autorisé;
- Perte; ou
- Toute autre atteinte à la protection d'un renseignement personnel.

« Préjudice sérieux », s'évalue selon :

- Sensibilité du renseignement;
- Conséquences appréhendées; et
- Probabilité qu'ils soient utilisés à des fins préjudiciables.

2. Une structure de gouvernance robuste

Assurer le respect de la Loi

- La personne en plus haute autorité de l’entreprise doit veiller au respect de la Loi
- Cette responsabilité peut être déléguée à un responsable de la protection des renseignements personnels (PRP)
- Les coordonnées de la personne responsable de la PRP doivent être rendues publiques

2. Une structure de gouvernance robuste (suite)

Politiques et pratiques

- Établir et mettre en œuvre des politiques et des pratiques encadrant sa gouvernance à l'égard de la PRP
- Proportionnées à la nature et à l'importance du traitement
- Approuvées par le responsable de la PRP
- Publiées sur le site Web de l'entreprise

Les pratiques et politiques exigées doivent prévoir :

- Règles applicables à la conservation et à la destruction des renseignements
- Rôles et responsabilités des membres du personnel tout au long du cycle de vie des renseignements
- Processus de traitement des plaintes relatives à la PRP

3. De nouvelles exigences relatives au consentement

- Le consentement doit être manifeste, libre, éclairé et donné à des fins spécifiques
- Le consentement doit être obtenu pour chaque type d'utilisation de renseignements personnels
- Lorsqu'il vise un renseignement sensible, le consentement doit être manifesté de façon expresse
- Un renseignement est sensible lorsque, de par sa nature ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de vie privée

- Le consentement implicite n'est accepté que dans certaines situations
- Le consentement doit être demandé distinctement de toute autre information communiquée à la personne concernée
- Le consentement d'un mineur de moins de 14 ans est donné par le titulaire de l'autorité parentale ou par son tuteur

3. De nouvelles exigences relatives au consentement (suite)

Situations où un renseignement personnel peut être utilisé à une autre fin, sans consentement :

- À des fins compatibles avec les fins de la collecte initiale;
- Utilisation manifestement au bénéfice de la personne;
- Nécessaire à la prévention de fraude ou à la sécurité;
- Nécessaire à la prestation d’un service ou livraison d’un produit;
- Nécessaire à des fins d’étude, de recherche ou de production de statistiques et qu’il est dépersonnalisé.

4. De nouvelles exigences relatives à la transparence

- La transparence est assurée par la divulgation d'information sur les pratiques et politiques de PRP
- La politique de confidentialité de l'entreprise doit être publiée sur son site Web
- Rédiger la politique de confidentialité en termes simples et clairs

Divulguer les renseignements suivants aux personnes concernées au moment de la collecte :

- Les fins;
- Les moyens utilisés;
- Les droits d'accès et de rectification; et
- Le droit de retirer le consentement.

5. Règlementation de la dépersonnalisation et de l'anonymisation des renseignements

« Dépersonnalisé » : le renseignement « ne permet plus d'identifier directement la personne concernée ».

« Anonymisé » : le renseignement « ne permet plus, de façon irréversible, d'identifier directement ou indirectement cette personne ».

- Le droit d'utilisation est distinct selon le type de renseignement
- L'utilisation des renseignements dépersonnalisés est assujettie à des restrictions et à la protection contre la réidentification
- Les renseignements anonymisés doivent l'être selon les meilleures pratiques généralement reconnues

De nouveaux droits individuels

1. Le droit à la portabilité des données

- Droit de la personne concernée de demander la communication des renseignements personnels recueillis à son sujet
- Informations transmises dans un format technologique structuré et couramment utilisé
- En vigueur dans trois ans, à compter du 22 septembre 2021

Exceptions :

- Le transfert peut être refusé s'il entraine de sérieuses difficultés
- Le droit ne s'applique PAS aux renseignements créés ou dérivés des renseignements personnels du requérant

2. Le droit à l’oubli

- Droit d’exiger la cessation de la diffusion d’un renseignement personnel
- Droit d’exiger la désindexation d’un renseignement personnel
- Droit d’exiger la correction des renseignements personnels « inexacts, incomplets ou équivoques » ou si leur collecte, leur communication ou leur conservation ne sont pas autorisées par la loi

Conditions :

- la diffusion de ce renseignement contrevient à la loi ou à une ordonnance judiciaire;
- la diffusion cause un préjudice grave; et
- ce préjudice est manifestement supérieur à l’intérêt du public de connaitre le renseignement.

3. Décisions fondées exclusivement sur un traitement automatisé

- Obligation d'informer la personne concernée qui fait l'objet d'une décision fondée exclusivement sur un traitement automatisé de ses renseignements personnels

- Traitement automatisé s'entend de l'usage des renseignements personnels sans l'intervention d'un être humain

- La personne concernée a le droit de soumettre ses observations quant à la décision

- Sur demande, l'organisation doit informer la personne concernée des :

  - Renseignements personnels utilisés

  - Motifs de la décision

  - Son droit de faire rectifier les renseignements personnels utilisés pour rendre la décision

Les transformations organisationnelles qui s’imposent

Une tendance : le renforcement des obligations de responsabilité qui entraîne des changements structurels

Le Règlement européen sur la protection des données (2018) :

- Désignation obligatoire d'un responsable de la protection des données pour certaines entreprises
- Registre des activités de traitement
- Analyse obligatoire d'impact relative à la protection des données pour certaines initiatives

Ancien projet de loi C-11 :

- Incorporation de la norme nationale du Canada intitulée *Code type sur la protection des renseignements personnels,* incluant le Principe de Responsabilité

Loi 64 s'inscrit dans la même démarche :

- Responsable de la protection des renseignements personnels (PRP)
- Politiques des pratiques encadrant la PRP

1. Révision du programme de PRP

Avez–vous un(e) Chef de la PRP ? Si oui,

- Êtes-vous sûrs que la désignation est au bon niveau ?

  À considérer :

  - L’expertise de la personne désignée;
  - Son niveau d’autorité afin d’assurer la conformité dans l’organisation;
  - Son indépendance face à la mise en œuvre des politiques et pratiques de PTP pour éviter les conflits d’intérêts.

Avez-vous un plan de réponse aux incidents à la confidentialité ? Si oui,

- Correspond-t-il aux exigences de la Loi 64 ?
- A-t-il été partagé avec les employés ?

1. Révision du programme de PRP (suite)

Avez-vous un inventaire de vos bases de données ?

- Quels renseignements personnels détenez-vous ?
- Comment les utilisez-vous et à quelles fins ?
- Certains sont-ils de nature sensible ?

Avez-vous des politiques et des pratiques internes pour assurer la PRP ?

- Sur la limite de renseignements personnels à être recueillis ?
- Sur les restrictions d'usage des données ?
- Sur la nature et la forme du consentement à recevoir ?
- Sur les périodes de conservation et les pratiques d'élimination ?
- Sur la protection des renseignements personnels ?
  - Un programme de gestion de la protection de la vie privée : la clé de la responsabilité

    (https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/lois-sur-la-protection-des-renseignements-personnels-au-canada/la-loi-sur-la-protection-des-renseignements-personnels-et-les-documents-electroniques-lprpde/aide-sur-la-facon-de-se-conformer-a-la-lprpde/conformite-a-la-lprpde-et-outils-de-formation/gl_acc_201204)

.

2. Révision des mécanismes de consentement et des politiques de confidentialité

- Le consentement est-il spécifique à chaque finalité d’utilisation ?
- Les renseignements recueillis sont-ils assujettis au niveau de consentement requis par la Loi ?
- Les politiques de confidentialité reflètent-elles les nouvelles exigences de transparence ?

2. Développement de nouveaux processus : 2.1 Évaluation des facteurs relatifs à la vie privée (EFVP)

- Pour tout projet de système d'information ou de prestation électronique de services impliquant le traitement de renseignements personnels;

- Avant de communiquer un renseignement personnel à l'extérieur du Québec; et

- Avant de communiquer des renseignements personnels sans le consentement des personnes concernées à des fins d'étude, de recherche ou de production de statistiques

Mise en œuvre :

- Détermination des critères de nécessité
- Assignation de la responsabilité
- Processus de consultation auprès de la personne responsable de la PRP
- Adoption d'un modèle d'analyse
- Mise en place d'un processus d'élaboration et d'approbation

- Directive sur l'évaluation des facteurs relatifs à la vie privée du Conseil du Trésor du Canada

2.2 L’EFVP pour transférer des renseignements personnels hors Québec

Contexte :

- Le Bureau du Surintendant des institutions financières exige déjà cette diligence raisonnable des institutions financières
- Le CPVP a adopté la même démarche dans ses lignes directrices Transfert transfrontalier de renseignements personnels
- Vos clients manifesteront de plus en plus cette exigence

La Loi 64 :

- Transfert soumis à la vérification d’une protection « adéquate »

Mise en œuvre :

- Détermination de critères d’évaluation de la sensibilité du renseignement, la finalité de son utilisation et les mesures de protection
- Établissement de critères « d’adéquation »
- Évaluation du risque par pays
- Adoption d’une politique d’engagement des fournisseurs de service en conséquence

2.3. Dépersonnalisation et anonymisation

Critères :

- Dépersonnalisation :
  - Remplacement des identifiants réels par des codes
  - Usage limité
- Anonymisation :
  - Séparation irréversible des identifiants
  - Usage pour des motifs sérieux et légitimes
- Adoption de technologies fiables
- Encadrement de l’utilisation à l’interne
- Définition des motifs sérieux et légitimes
- Développement de documents publics à propos des pratiques

2.4 Mécanismes de réponse aux droits individuels

Établissement de processus pour respecter :

- Droit d’accès aux raisons d’une décision fondée exclusivement sur un traitement automatisé
- Droit à l’oubli
- Droit à la portabilité

- Lignes directrices sur l’information à rendre accessible
- Processus permettant à un particulier de « présenter ses observations » concernant la décision
- Lignes directrices afin de tenir compte d’autres considérations de préjudice, d’intérêt public, de légalité
- Lignes directrices sur les renseignements à fournir et ceux « créés ou dérivés »

En somme – 5 leçons apprises de la révision de programmes internes de conformité

Ce que nous avons appris de l'étude des processus de conformité chez nos clients :

1. « Rien ne sert de courir, il faut partir à point »
2. La désignation de la personne responsable de la PRP est une décision critique et les options sont variées
3. La planification de l'exercice de conformité doit partir d'une analyse des écarts et d'une analyse du risque pour chaque écart
4. L'allocation des ressources doit être proportionnelle à l'effort
5. La conformité doit être appuyée d'une culture de PRP à travers l'organisation

Nos prochains webinaires à surveiller

- *Privacy regulation of de-identifcation and anonymsation is a game – changer – How to make it work in practice – Dr Khaled El-Emam*, 4 novembre 2021

- *Les recours des entreprises en vertu de la Loi 64 sur la protection des renseignements personnels – Comment vous protéger et comment vous défendre*, novembre 2021

大成 DENTONS

Merci

Chantal Bernier
Chef du groupe national Cybersécurité et protection des renseignements personnels, Ottawa
D +1 613 783 9684
chantal.bernier@dentons.com

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

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