Croissance | **Protection** | **Exploitation** | Financement

大成 DENTONS

Modernisation des lois québécoises sur la protection des renseignements personnels

Protection de votre organisation et recours

Mardi 15 février 2022 | 12 h à 13 h

Ordre du jour

1. Nos objectifs
2. Le pont avec notre webinaire précédent : réponses à vos questions
3. Protection de votre organisation – Prévention
4. Protection de votre organisation – Recours
5. Leçons clés

Nos objectifs

Vous appuyer dans la gestion de la conformité

- Pleins feux sur :
  - les **nouvelles** obligations et les conséquences **organisationnelles**
  - leur pertinence pour la protection de l'entreprise
- Différence entre :
  - La prévention : Mise en relief des transformations organisationnelles nécessaires à la démonstration de la conformité
  - Les recours : Description du mécanisme d'exécution de la loi et des recours accessibles aux entreprises
- Mais avant : Quelques réponses à vos questions

Le pont avec notre webinaire précédent

Réponses à vos questions

Portée de l’application de la Loi 25

S’applique-t-elle aux banques sous compétence fédérale?

- Non, mais…
- Débat constitutionnel : La compétence législative sur la protection des renseignements personnels (RP) dans le secteur privé selon les lois constitutionnelles du Canada :
  - Compétence fédérale, selon l’article 91.2 sur la « Réglementation du trafic et du commerce »? OU
  - Compétence provinciale, selon l’article 92.13 sur la « Propriété et les droits civils dans la province »?
- Les banques sont des « entreprises fédérales »
  - Selon 91.15 : « Les banques, l’incorporation des banques et l’émission du papier-monnaie »
  - Selon 4.1 de la *Loi sur la protection des renseignements personnels et documents électroniques* (LPRPDÉ) : elle s’applique aux RP des consommateurs et des employés de toute « entreprise fédérale », MAIS
- Selon la Loi 25, article 1, elle s’ applique à toute « entreprise » soit « l’exercice, par une ou plusieurs personnes, d’une activité économique organisée »
- La Commission d'accès à l'information (CAI) a régulièrement exercé sa compétence sur les banques fédérales

Portée de l’application de la Loi 25 (suite)

Quelles considérations s’appliquent aux chargés de la réglementation des autres provinces dans la gestion de RP de personnes au Québec?

- Les lois sur le secteur public
- Les chargés de la réglementation des autres provinces et du fédéral sont assujettis à leurs lois provinciales ou fédérales sur l’accès à l’information et la protection de la vie privée dans le secteur public
- Elles s’appliquent quelle que soit l’origine de l’individu auquel les RP se rapportent

Amendes et pénalités

Existe-t-il des pénalités et amendes particulières pour les violations résultant d'acteurs malveillants ou de virus?

- Non
- Les entreprises ont l'obligation d'appliquer les mesures de protection nécessaires selon le risque et le niveau de sensibilité des RP
- L'administration d'une peine ou d'une amende résultera de tout manquement à cette obligation, quelle que soit la cause de la violation

Les fournisseurs de service

Existe-t-il des obligations particulières qui s'appliquent aux fournisseurs de service?

- Pas dans la loi, mais dans les faits :
  - La loi s'applique aux RP transmis à un tiers comme un fournisseur de service (article 1)
  - Le tiers doit assurer :
    - La protection des RP qui lui sont confiés à un niveau équivalent à celui imposé à son client
    - L'utilisation des RP exclusivement à des fins compatibles
    - Le respect des obligations contractuelles sur la protection des RP selon le contrat de service

Organismes à but non lucratif

La Loi 25 s'applique-t-elle aux organismes à but non lucratif?

- Cela dépend
  - Si l'organisme se livre à une activité commerciale, OUI
  - Si non, les obligations de l'organisme en matière de protection des RP relève des articles 35 à 40 du Code civil
    - La collecte, l'utilisation et la communication des RP sont assujetties au consentement ou à l'autorisation par la loi
    - L'utilisation ne peut être qu'à des fins compatibles
    - Les erreurs de RP doivent être corrigées et l'individu doit y avoir accès à moins d'une interdiction

➢ La violation des droits relatifs à la vie privée fait l'objet d'un droit de recours

Transferts hors Québec

Comment la Province traitera-t-elle les transferts transfrontaliers sous le nouveau régime, particulièrement à l'égard des transactions financières vers les États-Unis et autres pays n'ayant pas une législation équivalente?

- Elle exigera une évaluation formelle des facteurs relatifs à la vie privée (EFVP)

- Le nouveau régime :
  - L' entreprise doit procéder à une EFVP pour s'assurer d'une « protection adéquate » selon la destination

- Le régime actuel :
  - L'entreprise ne peut pas communiquer les RP à l'extérieur du Québec à moins de « prendre tous les moyens raisonnables pour s'assurer que les renseignements ne seront pas utilisés à des fins non pertinentes ni communiqués à des tiers sans le consentement des personnes concernées »

➢ Tout RP provenant d'un pays d'Europe ne peut être transféré en-dehors du Canada sans autorisation, comme le transfert autorisé en vertu des clauses contractuelles types approuvées par la Commission européenne

Transformation organisationnelle

Puisque certaines dispositions entrent en vigueur le 22 septembre 2022, quand les entreprises doivent-elles commencer à mettre à jour leurs politiques de confidentialité?

- Maintenant!

➢ **Notre Guide :**

Projet de loi 64 : Le Québec modernise ses dispositions législatives en matière de protection des renseignements personnels : Un guide pratique

https://www.dentons.com/fr-ca/insights/guides-reports-and-whitepapers/2021/october/29/bill-64-on-modernizing-quebec-privacy-law-a-practical-guide

Principales différences entre la L25 et les autres lois canadiennes

- Exigences accrues en matière de consentement et de transparence*
- Clarification du concept de « renseignements dépersonnalisés » et de « renseignements anonymisés »
- Droit à la portabilité / mobilité*
- Obligation de procéder à des évaluations des facteurs relatifs à la vie privée (EFVP) en certaines circonstances, dont le transfert de RP hors du Québec
- Accord parental obligatoire pour les mineurs de moins de 14 ans
- Droit à la « désindexation »
- Pénalités financières administrées par l'organisme de réglementation*

*Également proposé dans l'ancien projet de réforme C-11 au fédéral de la *Loi sur sur la protection des renseignements personnels et documents électroniques (*LPRPDE)

Protection de votre organisation

La prévention

1. Le mot-clé : diligence raisonnable

(en vigueur 22.9.2022)

- Une structure de gouvernance pour assurer et démontrer la conformité : Articles 3.1 et 3.2
  - La personne ayant la plus haute autorité veille à assurer le respect et la mise en œuvre de la loi
  - Elle peut déléguer cette fonction par écrit, en tout ou en partie
  - Le titre et les coordonnées du responsable de la protection des RP sont publiés
  - L'entreprise doit établir et mettre en œuvre des politiques et des pratiques encadrant sa gouvernance à l'égard des RP dont :
    - Les modes de traitement et les mesures de protection des RP
    - L'encadrement applicable à la conservation et à la destruction de ces renseignements
    - L'assignation des rôles et des responsabilités des membres du personnel
    - L'établissement d'un processus de traitement des plaintes relatives à la protection des RP

➢ Proportionnelle à la nature et à l'importance des activités de l'entreprise

➢ Approuvée par le responsable de la protection des RP

1. Le mot-clé : diligence raisonnable (suite)

(en vigueur 22.9.2022)

- Un Plan de réponse aux incidents de sécurité (Article 3.5) pour :
  - Être alerté le plus tôt possible qu'un incident de confidentialité s'est produit
  - Prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent
  - Déterminer si l'incident présente un risque de préjudice sérieux
  - Si oui, aviser
    - la Commission d'accès à l'information (CAI)
    - toute personne affectée
    - tout organisme à même de diminuer le risque

1. Le mot-clé : diligence raisonnable (suite)

(en vigueur 2023)

- Un processus de développement de l'évaluation des facteurs relatifs à vie privée (EFVP) (Article 3.3)
  - Applicable à tout projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels.
  - Assujetti, dès le début du projet, à la consultation du responsable de la protection des RP
  - Proportionnel à la sensibilité des renseignements concernés, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support.
- Une EFVP en vue des transferts de RP en dehors du Québec (Article 17)

2. Rehausser les modalités de consentement

(en vigueur en 2023)

- (Article 4.1) : Développer des mécanismes de consentement pour les mineurs
  - Moins de 14 ans : consentement du titulaire de l'autorité parentale ou du tuteur
  - Entre 14 et 18 ans : consentement par le mineur, par le titulaire de l'autorité parentale ou par le tuteur

- (Article 14) : Obtenir le consentement spécifique à chaque fin
  - Demandé à chacune des fins, en termes simples et clairs
  - Présentée distinctement de toute autre information

- (Article 22) : Mettre en évidence le droit de retirer le consentement

3. Rehausser la transparence

- Mettre à jour les politiques de confidentialité selon l'article 7
- (Article 8.1) Décrire l'utilisation des technologies
  - Décrire toute technologie comprenant des fonctions permettant de l'identifier
  - Mettre en évidence les moyens offerts pour activer ces fonctions
- (Article 12.1) Déclarer les mécanismes automatisés
  - Déclarer l'utilisation des RP afin que soit rendue une décision fondée exclusivement sur un traitement automatisé au plus tard au moment où il l'informe de cette décision.

4. Nouveaux mécanismes de réponse aux droits individuels et lignes directrices

- (Article 12.1) : Droits relatifs aux décisions automatisées:
  - Accès aux RP utilisés pour rendre la décision et aux raisons, principaux facteurs et paramètres, ayant mené à la décision
  - Rectification des RP utilisés pour rendre la décision
  - Présentation d'observations à un membre du personnel de l'entreprise en mesure de réviser la décision

- (Article 28.1) Droit « à l'oubli »
  - Cessation de la diffusion ou désindexation

- (Article 28) Droit à la communication à un autre organisme
  - Les RP recueillis auprès du requérant (et non ceux qui sont créés ou inférés par l'organisation) dans un format structuré et couramment utilisé

➢ Chacun de ces droits est soumis à des conditions qui doivent faire l'objet de lignes directrices

Protection de votre organisation
Les recours

Demandes d’autorisation

- (Article 46) Les demandes abusives
  - Une entreprise peut demander à la CAI l’autorisation de ne pas tenir compte de demandes manifestement abusives :
    - Par leur nombre,
    - Par leur caractère répétitif ou systématique
    - Parce qu’elles ne sont pas conformes à l’objet de la loi

- L’entreprise peut demander à la CAI de circonscrire la demande ou de prolonger le délai de réponse
- L’entreprise peut faire valoir à la CAI que la demande est frivole ou faite de mauvaise foi pour qu’elle refuse de la traiter

Contestation d’une demande de rectification

- (Article 53)
- L’entreprise peut prouver qu’un RP n’a pas à être rectifié à moins qu’il ne lui ait été communiqué par la personne concernée ou avec l’accord de celle-ci.

Appel et contestation

- (Article 61)
  - Appel
    - d’une décision finale de la CAI devant un juge de la Cour du Québec, sur toute question de droit ou de compétence
    - d’une décision interlocutoire avec la permission d’un juge
  - Contestation
    - Une entreprise peut aussi contester devant un juge de la Cour du Québec une ordonnance prise par la section de surveillance de la CAI.

Observations

- (Article 90.4)

- Avant qu'une sanction administrative pécuniaire soit imposée, l'entreprise doit
  - avoir été notifiée et
  - avoir eu l'occasion de présenter ses observations et de produire tout document pour compléter son dossier.

➢ D'où l'importance de la structure de gouvernance et des politiques internes pour démontrer la conformité

Demande de réexamen

- (Article 90.6)
- L’entreprise peut, par écrit, demander à la CAI le réexamen de la décision d’imposer une sanction administrative pécuniaire dans les 30 jours de la notification de l’avis de réclamation.

Arguments de défense

- (Article 92.3). Dans la détermination de la peine, le juge tient notamment compte des facteurs suivants :
- la nature, la gravité, le caractère répétitif et la durée de l'infraction : **L'entreprise pourrait donc invoquer le caractère unique de l'infraction et ses efforts pour y remédier dans les meilleurs délais, par exemple avec un Plan de réponse aux incidents de sécurité et un rapport qui documente son intervention dans les détails selon un gabarit bien établi**
- le fait que l'entreprise a fait preuve de négligence ou d'insouciance : **L'entreprise pourrait présenter la documentation de sa diligence raisonnable**
- le caractère prévisible de l'infraction ou le défaut d'avoir donné suite aux recommandations ou aux avertissements visant à la prévenir : **L'entreprise pourrait présenter son plan de sécurité pour faire valoir qu'il est adéquat selon l'évaluation du risque**
- les tentatives de dissimuler l'infraction ou le défaut de tenter d'en atténuer les conséquences : **L'entreprise devrait être en mesure de démontrer qu'elle a été transparente**
- le nombre de personnes concernées par l'infraction et le risque de préjudice auquel ces personnes sont exposées : **En réagissant vite à un incident, l'entreprise peut atténuer le risque de préjudice.**

Leçons clés sur la conformité

1. La meilleure protection est la démonstration de la diligence raisonnable.

2. On démontre la diligence raisonnable avec une structure de gouvernance claire et efficace et avec des politiques internes exhaustives et précises.

3. « Rien ne sert de courir, il faut partir à point »; ces mesures doivent être développées maintenant pour être adoptées à temps.

4. La planification de l'exercice de conformité doit partir d'une analyse des écarts et d'une analyse du risque pour chaque écart.

5. La conformité doit être documentée pour être démontrée.

大成DENTONS

Merci

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

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

Dentons, le plus grand cabinet d'avocats au monde, compte plus de 20 000 professionnels de haut calibre, dont 12 000 avocats, œuvrant dans plus de 200 bureaux répartis dans plus de 80 pays, qui offrent à ses clients les solutions dont ils ont besoin pour relever les défis et saisir les occasions qui se présentent. Fort de sa démarche polycentrique axée sur les résultats, de son engagement à favoriser l'inclusion et la diversité et de son service à la clientèle maintes fois reconnu, Dentons défie le statu quo pour défendre les intérêts de ses clients.

dentons.com