大成 DENTONS

Les Matinées Dentons

Projet de loi 64 modernisant la protection des renseignements personnels : les répercussions potentielles pour votre entreprise

Chantal Bernier, avocate-conseil, Dentons Ottawa

Alexandra Quigley, avocate, Dentons Montréal

9 décembre 2020

Nos objectifs aujourd’hui

1. Présenter **les enjeux** sous-jacents au projet de loi 64, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* qui guident ses dispositions pour mieux les comprendre

2. Décrire **les dispositions** qui auront les plus grandes répercussions

3. Faire le lien avec le **projet de loi fédéral C-11** et le droit européen applicable aux entreprises canadiennes

4. Cerner les **principaux défis** et proposer des **stratégies** de mise en œuvre par ordre d’urgence

1. Les enjeux

À travers le monde, la protection du droit à la vie privée est renforcé en réponse à trois grandes préoccupations:

1. Le déséquilibre de pouvoir sans précédent entre l'individu et les organisations détentrices de ses données;

2. La valeur des données personnelles comme monnaie de l'économie numérique;

3. La vulnérabilité des supports numériques aux cyber-attaques et pertes de données personnelles.

La réponse du projet de loi 64 à ces grands enjeux

1. Le renforcement du consentement

- Consentement manifeste, libre et éclairé;
- Doit être obtenu pour chaque fin spécifique, distinctement de toute autre information;
  - Exception:
    - Utilisation à des fins compatibles (lien pertinent et direct) avec celles pour lesquelles il a été recueilli;
    - Utilisation manifestement au bénéfice de la personne concernée;
    - Utilisation nécessaire à des fins d'étude, de recherche ou de production de statistiques **et** qu'il est dépersonnalisé.
- La prospection commerciale ou philanthropique ne peuvent être considérées comme des fins compatibles
- Le consentement ne vaut que pour la durée nécessaire à la réalisation des fins auxquelles il a été demandé.

1. Le renforcement du consentement

- Consentement doit être demandé en termes simples et clairs
- Obligation de prêter assistance à la personne concernée afin de l'aider à comprendre la portée du consentement demandé;

- Consentement du mineur:
  - Moins de 14 ans: consentement donné par le titulaire de l'autorité parentale;
  - 14 ans et plus: donné par le mineur ou par le titulaire de l'autorité parentale.

1. Le renforcement du consentement

- Toute collecte de renseignements personnels sensibles exige un consentement exprimé de façon expresse
  - Renseignement personnel 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 peut être retiré en tout temps

2. Précision de l'obligation de transparence pour informer l'individu, en termes «simples et clairs»

Politique de confidentialité rédigée en termes **simples et clairs** doit être publiée sur le site Internet de l'entreprise

Obligations de la personne recueillant les renseignements personnels

- Informations devant être transmises:
  - Les fins auxquelles les renseignements sont recueillis
  - Les moyens par lesquels les renseignements sont recueillis;
  - Les droits d'accès et de rectification;
  - Le droit de retrait du consentement;
  - La possibilité que les renseignements soient communiqués à l'extérieur du Québec;
  - Le nom du tiers pour qui la collecte est effectuée
- Sur demande:
  - des catégories de personnes qui ont accès à ces renseignements au sein de l'entreprise,
  - de la durée de conservation de ces renseignements,
  - des coordonnées du responsable de la protection des renseignements personnels.

Obligation de transparence – Technologies permettant l'identification, la localisation ou le profilage

- L'individu doit être informé, au préalable
  - Du recours à une technologie comprenant des fonctions permettant de l'identification, la localisation ou le profilage
  - Des moyens offerts pour désactiver ces fonctions
  - Définition de profilage:
    - Le profilage s'entend de la collecte et de l'utilisation de renseignements personnels afin d'évaluer certaines caractéristiques d'une personne physique, notamment à des fins d'analyse du rendement au travail, de la situation économique, de la santé, des préférences personnelles, des intérêts ou du comportement de cette personne.

3. La nouvelle catégorie de transparence: le recours au «traitement automatisé»

- Obligation d'informer la personne concernée lorsque ses renseignements personnels sont utilisés afin que soit rendue une décision fondée exclusivement sur un traitement automatisé de ceux-ci;
- La personne concernée doit être avisée avant ou au moment de la décision;
- Sur demande l'informer:
  1° des renseignements personnels utilisés pour rendre la décision;
  2° des raisons, ainsi que des principaux facteurs et paramètres;
  3° du droit de faire rectifier les renseignements
- L'individu peut présenter ses observations pour faire réviser la décision.

4. La création de nouveaux droits

- En plus des droits existants d'accès et de rectification, création de nouveaux droits et renforcement des droits existants
- Droit de demander qu'une entreprise cesse de diffuser un renseignement personnel ou sa désindexation, si la diffusion:
  - Contrevient à la loi
  - Contrevient à une ordonnance judiciaire

  - Droit de demander de cesser la diffusion, la désindexation ou la réindexation lorsque:
    - La publication cause un préjudice grave relatif au droit au respect de la réputation ou de la vie privée,
    - Ce préjudice est supérieur à l'intérêt public
    - La désindexation, la cessation de la diffusion ou la réindexation est proportionnelle

4. La création de nouveaux droits (suite)

- Droit d’accès aux renseignements personnels informatisés «dans un format technologique structuré et couramment utilisé»
  - Exception: si cela soulève des difficultés pratiques sérieuses

- Droit à la portabilité:
  - Communication de renseignements personnels à la demande de l’individu à tout organisme autorisé par la loi à les recueillir

5. Des mesures de gouvernance obligatoires

- Au sein de l'entreprise, la personne ayant la plus haute autorité veille à assurer le respect et la mise en œuvre de la loi.
  - La fonction peut être déléguée
  - Le titre et les coordonnées du responsable de la protection des renseignements personnels doivent être publiés sur le site Internet de l'entreprise ou rendus accessibles par tout autre moyen approprié.
  - Le responsable approuve les politiques et procédures de protection des données
- L' entreprise doit mettre en œuvre
  - Des politiques et des pratiques encadrant sa gouvernance à l'égard des renseignements personnels
  - Des échéanciers de conservation et destruction des renseignements,
  - Prévoir les divers rôles et responsabilités du personnel
  - Établir des processus de traitement des demandes d'accès, de correction, de destruction et de portabilité et de traitement des plaintes
  - Appliquer des mesures de protection des données selon leur nature
- L'entreprise doit publier ces politiques

6. La mise à niveau avec le fédéral: signalement obligatoire d'un incident de confidentialité

La nouvelle obligation au provincial – existante au fédéral :

- Si l'incident présente un risque de «préjudice sérieux» :
  - Avis à la Commission d'accès à l'information (CAI);
  - Avis à toute personne concernée.

- Sous peine de sanction administrative :
  - Maximum de $50,000 pour une personne physique;
  - Maximum de $10,000,000 ou 2% du chiffre d'affaires mondial pour une entreprise.

- Ou pénale :
  - $5,000 à $50,000 pour une personne physique;
  - $15,000 à 25,000,000 ou 4% du chiffre d'affaire mondial pour une entreprise.

- L'entreprise doit tenir un registre de tout incident.
- Le devoir de donner accès à la CAI sur demande.

7. La mise à niveau avec l’Europe: Création de pénalités

- Administratives administrées par la CAI :
  - Maximum de $10,000,000 ou 3% du chiffre d’affaires pour une entreprise

- Pénales :
  - Personne physique : $5,000 à $50,000
  - Entreprise: $15,000 à $25,000,000 ou 4% du chiffre d’affaires
  - Pour:
    - Communication illégale;
    - Défaut de déclaration d’un incident;
    - Tentative d’identification d’un renseignement dépersonnalisé.

- Et d’un droit de poursuite en dommages intérêts

8. Deux nouveaux joueurs

1. L’évaluation des facteurs relatifs à la vie privée (EFVP)

- Lorsque l’entreprise envisage tout projet de système d’information ou de prestation électronique de services comportant le traitement de données personnelles

- Lorsque l’entreprise envisage de communiquer des renseignements hors Québec

8. Deux nouveaux joueurs (suite)

2. Les conditions de transfert hors Québec

- Sujets à :
  - Une évaluation des facteurs relatifs a la vie privée tenant compte de:
    - Sensibilité
    - Finalité
    - Mesures de protection
    - Régime juridique de l’État de destination

Similitudes et divergences avec le projet de loi fédéral C-11

Principales similitudes

- Exigences accrues en matière de consentement et de transparence
- Clarification du concept de « renseignements dépersonnalisés »
- Exceptions similaires relativement à l'interdiction de communication
- Droits individuels similaires :
  - Accès
  - Rectification
  - Portabilité / Mobilité
- Obligation de signaler un incident à la sécurité lorsqu'il existe un risque réel de préjudice grave et de tenir un registre des manquements
- Mêmes responsabilités générales
- Pénalités financières
- Protection des lanceurs d'alerte

Principales différences

Projet de loi nº 64 du Québec

- Modifie la loi existante
- Fortement inspiré du RGPD
- Conditions de transfert de renseignements personnels hors du Québec
- Obligations de procéder à des évaluations des facteurs relatifs à la vie privée (EFVP)
- Accord parental obligatoire pour les mineurs de moins de 14 ans
- Droit à la « désindexation »
- Pénalités financières administrées par l'organisme de réglementation

Projet de loi C-11 du Canada

- Remplace la loi existante
- Emprunts limités au RGPD
- Aucune condition de transfert transfrontalier – seulement une obligation d'informer
- Aucune obligation d'évaluer les facteurs relatifs à la vie privée
- Seule disposition relative aux mineurs se rapporte au représentant autorisé
- Droit de « retrait »
- Pénalités financières administrées par un tribunal sur recommandation de l'organisme de réglementation

Le contexte européen pertinent

Le resserrement des transferts transfrontaliers

- En vertu du Règlement général sur la protection des données (RGPD), les organisations traitant des données de personnes dans l'UE ou la ZEE ne peuvent transférer les données à l'extérieur sauf si
  - L'État a été reconnu comme offrant une protection «adéquate», ou
  - Le transfert est régi par des clauses contractuelles types (CCT), ou
  - Le transfert est intra-compagnie munie de Règles d'entreprises contraignantes
  - L'individu a consenti
- Ceci s'applique à toute la chaine de fournisseurs de service
- La loi fédérale sur la *Protection des renseignements personnels et documents électroniques* a reçu l'adéquation – la loi québécoise, non
- L'exigence est accrue depuis la décision Schrems II – 16 juillet 2020:
  - Même avec des CCT, l'organisation doit s'assurer que les renseignements recevront une protection adéquate

Les principaux défis et les stratégies de mise œuvre ou comment vous préparer

Défi #1 : Un risque financier sans précédent

Mesures :

1. Si ce n'est déjà fait, identifier la meilleure personne/position, selon les besoins de l'organisation, pour assurer la conformité.
2. Charger cette personne d'une analyse des écarts entre les mesures existantes et les exigences du Projet de loi 64.
3. À partir de cette analyse, développer un plan d'action pour la conformité au Projet de loi 64 :
   a) En assignant les tâches pertinentes de façon structurée;
   b) En réunissant le personnel responsable autour de ces tâches, et au besoin, en allant chercher une expertise externe;
   c) En affectant à l'exercice les ressources nécessaires.
4. Si ce n'est déjà fait, procéder à une analyse des menaces et risques à la sécurité des données – technologiques, physiques, administratives et contextuelles.
5. À partir de cette analyse, adopter les mesures de protection pertinentes.

Défi #2 : Des peines significatives en cas de mauvaise gestion d'un incident de sécurité

- Ce n'est pas d'avoir subi un incident à la sécurité qui mène aux peines maximales – c'est d'avoir contrevenu aux règles de réponse :
  - Défaut d'aviser la CAI;
  - Défaut d'aviser les personnes concernées;
  - Défaut de tenir un registre des incidents.
- Pour assurer la conformité de la réponse, il faut un Plan de réponse aux incidents qui :
  - Définit un plan d'escalade de l'alerte et de la réponse interne;
  - Informe les employés du plan d'escalade et de leur rôle;
  - Identifie l'équipe de réponse;
  - Assigne les responsabilités;
  - Encadre l'évaluation des obligations juridiques et leur exécution.

Défi #3 : Des exigences précises sur la structure de gouvernance de PRP

- En plus du plan de réponse aux incidents, il faut établir une structure de gouvernance de protection des données :
  - Inventaire des bases de données
  - Politiques et procédures internes de gestion et de protection des données;
  - Mécanismes et responsabilités pour répondre aux demandes :
    - D’accès;
    - De rectification;
    - De désindexation;
    - D’explication des mécanismes de traitement automatisé;
    - De portabilité.
  - Échéanciers de conservation des données.
- Processus d’EFVP.

Défi #4 : De nouvelles exigences dans l’interface avec les individus

- Mise à jour des modes d’obtention du consentement
- Mise à jour des politiques de confidentialité
- Développement du narratif sur le traitement automatisé

Défi #5 : L’obligation de l’évaluation des facteurs relatifs à la vie privée

- S’applique à **tout projet** de système d’information ou de prestation électronique de services qui mette en cause les renseignements personnels.
- L’obligation s’applique donc pour l’avenir.
- Mesures à prendre maintenant :
  - Établir un processus de développement et d’approbation des EFVP pour les projets visés;
  - Développer un gabarit pour les EFVP.

Défi #6 : Des conditions nouvelles au transfert des données hors Québec

- Le transfert doit être soumis à une EFVP.
- L’entreprise doit s’assurer que le renseignement bénéficierait d’une protection équivalente.
- Le transfert est assujetti à une entente écrite sur la protection des données.
- Mesures :
  - Évaluation des transferts actuels hors Québec;
  - Adoption de lignes directrices sur l’impartition à des fournisseurs de service hors Québec;
  - Formation du personnel responsable des contrats sur les lignes directrices;
  - Révision, si nécessaire, de l’impartition hors Québec.

Pour conclure

- Repensez l'équation risques – ressources à propos de la protection des renseignements personnels: un épargne en amont peut être ruineuse en aval.
- Préparez-vous dès maintenant pour assurer une mise en œuvre efficace et « en douceur ».
- Mobilisez votre personnel pour ancrer une culture de confidentialité – c'est votre première ligne de défense et…votre plus grande vulnérabilité.
- Documentez votre conformité:
  - Pour répondre aux pouvoirs accrus des régulateurs
  - Pour être prêt en cas de fusion ou acquisition
  - Pour maintenir la confiance des individus

Personnes-ressources

Chantal Bernier
Avocate-conseil, Ottawa

+1 613 783 9684
chantal.bernier@dentons.com

Alexandra Quigley
Avocate, Montréal

+1 514 878 5856
alexandra.quigley@dentons.com

Charmaine Borg
Avocate, Ottawa

+1 613 783 9643
charmaine.borg@dentons.com

Merci

Dentons Canada LLP

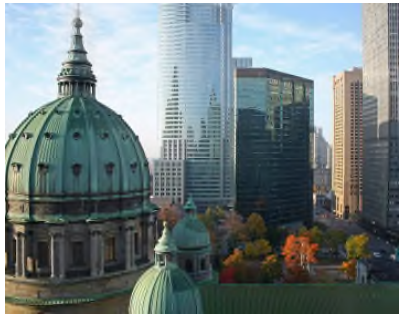
99 Bank Street, Suite 1420

Ottawa, Ontario K1P 1H4

Dentons Canada LLP

1 Place Ville Marie, Bureau 3900

Montréal, Québec H3B 4M7



Dentons fournit des solutions juridiques et commerciales d'excellence à ses clients. Plus grand cabinet du monde, il est classé parmi les meilleurs cabinets d'avocats par Acritas*, lauréat du BTI Client Service 30 Award, et reconnu par les plus grandes entreprises et annuaires juridiques pour sa capacité d'innovation, notamment grâce au lancement de Nextlaw Labs et Nextlaw Global Referral Network. Première firme mondiale polycentrique, Dentons défie le statu quo et accompagne ses clients sur tous les marchés et dans toutes les opérations.
www.dentons.com

© 2020 Dentons. Dentons est un cabinet d'avocats mondial qui fournit des services à sa clientèle par l'intermédiaire de ses cabinets membres et des membres de son groupe partout dans le monde. Le présent document n'est pas destiné à servir d'avis d'ordre juridique ou autre et vous ne devriez pas agir, ou vous abstenir d'agir, sur la foi de son contenu. Nous vous communiquons certains renseignements à la condition que vous conveniez d'en préserver le caractère confidentiel. Si vous nous communiquez des renseignements confidentiels sans toutefois retenir nos services, il se pourrait que nous représentions un autre client dans le cadre d'un mandat auquel vos renseignements confidentiels pourraient servir. Veuillez consulter les avis juridiques à l'adresse dentons.com.