Transferts transfrontaliers

Modifications à la Loi sur la protection des renseignements personnels dans le secteur privé du Québec
Article 17

Introduction

Le 22 septembre 2021, le Québec a adopté la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (2021, chapitre 25) (la « Loi ») qui met à jour les lois sur la protection des renseignements personnels dans le secteur public et dans le secteur privé. Les dispositions de la Loi entrent en vigueur sur une période de 3 ans.

Ce document a été créé par des sommités canadiennes en matière de protection des renseignements personnels, en collaboration avec des associations industrielles nationales et régionales. Nous pensons qu'il est important d'adopter une approche harmonisée des lois sur la protection des renseignements personnels dans toutes les juridictions canadiennes afin que les règles soient compréhensibles pour les particuliers et les entreprises. L'interprétation des lois sur la protection des renseignements personnels doit être pragmatique, raisonnable et axée sur les résultats pour les particuliers et la mise en œuvre pour les entreprises. Dans cet esprit, nous avons élaboré des conseils qui nous semblent appropriés pour interpréter les dispositions les plus complexes de la Loi.

Ce document peut être partagé et utilisé par les entreprises. Il ne s'agit pas d'un avis juridique, mais de recommandations, de pratiques exemplaires à l'intention des entités qui souhaitent se conformer à la Loi avant que le gouvernement ou la Commission d'accès à l'information (la « CAI ») ne fournisse des règlements ou des directives supplémentaires. Nous encourageons les entreprises à suivre les développements de la CAI et des autorités gouvernementales sur ces sujets et ceux liés à la Loi.

Transferts transfrontaliers

La Loi exige qu'une entreprise (y compris son fournisseur de services, sa filiale ou son service corporatif à l'extérieur du Québec) respecte les exigences suivantes avant de pouvoir transférer des renseignements personnels à l'extérieur du Québec :

1) Procéder à une évaluation des facteurs relatifs à la vie privée (EFVP) afin d'évaluer si les renseignements recevraient une protection adéquate conformément aux principes de protection des renseignements personnels généralement reconnus ; et
2) Conclure une entente écrite qui tient compte des résultats de l'ÉFVP et, s'il y a lieu, comprend des mesures afin d'atténuer les risques identifiés dans l'ÉFVP.

Il peut être utile de consulter les lignes directrices du Commissariat à la protection de la vie privée du Canada sur le traitement transfrontalier des renseignements personnels.

a) Facteurs relatifs à la vie privée à évaluer

Les entreprises doivent prendre en compte les facteurs suivants liés à la protection de la vie privée et s'assurer que les renseignements seront protégés conformément aux principes de protection des renseignements personnels généralement reconnus.

1) Sensibilité des renseignements : Les renseignements « intimes », y compris les renseignements médicaux, biométriques ou ceux dont le contexte ou l'utilisation ou la communication implique un niveau élevé d'attente raisonnable en matière de vie privée, sont soumis à un degré de protection plus élevé.
2) Finalité de l'utilisation des renseignements : Les renseignements transférés doivent être raisonnablement requis pour les fins identifiées.
3) Mesures de protection, y compris celles qui sont contractuelles, dont le renseignement bénéficierait à appliquer : Les mesures de protection doivent être adaptées à la sensibilité des renseignements et tenir compte du risque et des conséquences possibles d'un accès non autorisé aux renseignements, de leur utilisation ou de leur divulgation.
4) Régime juridique applicable dans l'État où ce renseignement serait communiqué : Les lois sur la protection des renseignements personnels de la juridiction étrangère devraient protéger les renseignements conformément aux principes de protection des renseignements personnels généralement reconnus. Il serait commercialement raisonnable d'évaluer le régime juridique d'un État destinataire par rapport aux principes de l'OCDE qui constituent la base de la plupart des principales lois de protection des renseignements personnels dans le monde.

b) Entente écrite pour le transfert de données

Une fois que l'entreprise a terminé l'évaluation et déterminé que les renseignements peuvent être transférés vers l'État destinataire, elle doit alors conclure une entente écrite de transfert de renseignements avec le destinataire. L'entente doit tenir compte des résultats de l'évaluation et, le cas échéant, inclure les conditions requises pour atténuer les risques identifiés dans l'évaluation.

Les dispositions contractuelles suivantes sont suggérées comme meilleures pratiques pour aider à se conformer à cette exigence :

Section 1 — Objectif et portée

Définissez clairement les objectifs et la portée pour lesquels le fournisseur de services peut traiter les données, et limitez strictement tout traitement à ces objectifs.

Section 2 — Interprétation

Les définitions ou la terminologie utilisées dans les lois sur la protection des renseignements personnels, ou dans le langage courant, peuvent différer d'une juridiction à l'autre. Il est donc recommandé de prévoir une section « Définitions » pour garantir une interprétation précise, en s'attachant en particulier à clarifier les termes clés lorsqu'il existe une terminologie différente, par exemple pour définir ce qu'est un renseignement sensible.

Section 3 — Obligations des parties

- **Finalité limitée**. Le fournisseur de services ne peut traiter les données que conformément aux instructions et aux fins spécifiées par le client.
- **Exactitude et transparence**. Le fournisseur de services doit informer le client lorsqu'il a connaissance que des renseignements sont inexacts et collaborer avec elle pour les rectifier.
- **Coopération**. Le fournisseur de services doit coopérer avec le client et l'aider à se conformer à la législation applicable en matière de protection des renseignements personnels, y compris les demandes d'accès, la portabilité des renseignements, la suppression des renseignements, la conformité aux demandes des organismes de réglementation de la protection des renseignements personnels.
- **Incident de sécurité**. Le fournisseur de services doit informer le client lorsqu'il a connaissance d'un incident de sécurité impliquant les renseignements personnels du client, s'attaquer à l'incident et en atténuer les effets négatifs, collaborer avec le client pour évaluer l'incident et informer les personnes concernées et les organismes de réglementation, le cas échéant.
- **Remise ou destruction des renseignements personnels**. Le fournisseur de services doit détruire ou remettre les renseignements selon les instructions du client ou à l'expiration du contrat.
- **Mesures de sécurité**. Le fournisseur de services doit protéger les données à l'aide de mesures de sécurité adaptées au niveau de sensibilité des données. Par exemple
    - Restreindre l'accès au besoin de savoir, contrôler l'accès et cloisonner les renseignements ;
    - Contrôle de sécurité des employés ; et
    - Supervision et contrôle des mesures de protection des renseignements personnels.

Il est recommandé d'exiger le respect de normes détaillées. Ces normes peuvent être définies par l'entreprise dans une annexe, ou le contrat peut exiger la conformité à une ou plusieurs normes de sécurité externes reconnues.

- **Politique et procédures**. Le fournisseur de services doit avoir des politiques et des procédures relatives à la protection des renseignements personnels et à la sécurité ou se conformer à la politique et aux procédures de protection des renseignements personnels et de sécurité du client.
- **Formation et qualité**. Les fournisseurs de services doivent offrir une formation obligatoire sur la protection des renseignements personnels à leurs employés et disposer d'un mécanisme permettant de vérifier si la formation a été suivie dès l'embauche et de façon continue.
- **Notification**. Le fournisseur de services doit informer le client lorsque les lois et pratiques locales peuvent avoir un impact sur le contrat.

Section 4 — Tiers et sous-traitants.

Le fournisseur de services ne peut transférer les renseignements personnels du client à tiers (y compris un sous-traitant) ou transférer les renseignements en dehors de la ou des juridictions autorisées sans le consentement écrit du client. Il est également possible d'autoriser un transfert à une partie ou à un groupe de parties prédéfinies (après une évaluation par l'entreprise), mais d'interdire les transferts à d'autres tiers sans le consentement de l'organisation cédante/contrôlante.

Section 5 — Contrôle de la qualité

- **Audit**. Le client peut vérifier le respect par le fournisseur de services de ses obligations en matière de confidentialité et de sécurité. Le client peut effectuer cet audit lui-même ou par l'intermédiaire d'un auditeur indépendant.
- **Documentation et conformité**. Le fournisseur de services doit maintenir une documentation appropriée afin de pouvoir démontrer sa conformité avec le contrat, les lois applicables et les meilleures pratiques.

Section 6 — Demande d'accès du gouvernement et d'autres autorités publiques

Dans la mesure où la loi le permet, le fournisseur de services doit informer le client s'il reçoit une demande d'accès, une ordonnance de production, une assignation à comparaître ou une demande similaire, une demande ou un ordre d'une autorité gouvernementale ou d'une autre autorité publique et doit fournir une assistance raisonnable au client dans le cas où il demande une ordonnance de protection.

Section 7 — Droit applicable

Dans la mesure du possible, le droit applicable doit être celui de la province de Québec.

Section 8 — Responsabilité et assurance

- Le fournisseur de services est responsable et doit indemniser le client pour les pertes liées à une atteinte à la protection des renseignements personnels ou à la sécurité.
- Le fournisseur de services doit souscrire une assurance responsabilité cyber risques dont la limite ne doit pas être inférieure à [X millions par événement, montant à déterminer par l'évaluation des risques].