



Commissariat
à la protection de
la vie privée du Canada

LPRPDE

Traitement transfrontalier des données personnelles **Lignes directrices**



OBJET

Le Commissariat à la protection de la vie privée du Canada a élaboré les présentes lignes directrices afin d'expliquer comment la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) s'applique aux transferts de renseignements personnels à des tierces parties, y compris à des tierces parties exerçant des activités à l'extérieur du Canada, aux fins de traitement.

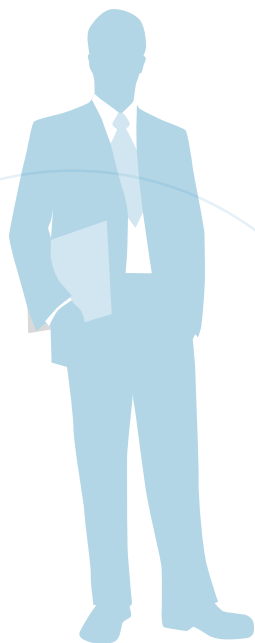
REMARQUE : Les lignes directrices ne traitent ni des transferts de renseignements personnels aux fins de traitement par des entités publiques fédérales, provinciales ou territoriales, ni des règles particulières sur les transferts aux fins de traitement contenues dans les lois provinciales relatives à la protection des renseignements personnels qui s'appliquent au secteur privé. Toutefois, les organisations dont les activités commerciales dans une province ne sont pas assujetties à la LPRPDE doivent savoir que les transferts transfrontaliers le sont.

CONTEXTE

Comme le stipule la *Loi* elle-même, la LPRPDE vise « à faciliter et à promouvoir le commerce électronique en protégeant les renseignements personnels recueillis, utilisés ou communiqués dans certaines circonstances ». Cela veut dire que la protection adéquate des renseignements personnels permet de faciliter et de promouvoir le commerce en renforçant la confiance des consommateurs.

L'actuelle économie mondiale interdépendante repose sur la circulation internationale de l'information. Les transferts transfrontaliers suscitent effectivement certaines craintes légitimes : où vont les renseignements personnels, et comment sont-ils traités en cours de transit et à leur arrivée dans un pays étranger? La confiance des consommateurs sera renforcée s'ils savent que le transfert de leurs renseignements personnels est régi par des règles claires et transparentes.

Il existe différentes approches en matière de protection des renseignements personnels transférés aux fins de traitement. Les États membres de l'Union européenne ont adopté des lois interdisant le transfert de renseignements personnels d'un pays à un autre, à moins que la Commission européenne ne juge que les mesures de protection des renseignements personnels de cet autre pays sont « suffisantes ».



En adoptant la LPRPDE, le Canada a opté pour une approche non fondée sur le concept de « protection suffisante » et il a choisi une approche adaptée à chaque organisation, plutôt qu'à chaque État. La LPRPDE n'interdit pas aux organisations du Canada de transférer des renseignements personnels à une organisation dans un pays étranger aux fins de traitement. Toutefois, en vertu de la LPRPDE, les organisations sont tenues responsables de la protection des transferts de renseignements personnels en vertu de chaque accord d'impartition individuel. Le Commissariat à la protection de la vie privée peut enquêter sur des plaintes et mener des vérifications concernant les pratiques de traitement des renseignements personnels des organisations.

Le premier, et le plus important principe du Code type sur la protection des renseignements personnels de l'Association canadienne de normalisation, figure à l'annexe 1 de la LPRPDE. Ce principe assure l'équilibre entre la protection des renseignements personnels des consommateurs et la nécessité pour les entreprises de transférer des renseignements personnels pour diverses raisons, notamment la disponibilité des fournisseurs de services, l'efficacité et l'économie.

Le premier principe précise que la responsabilité de la protection des renseignements personnels incombe à l'organisation qui en a la gestion. Le principe 4.1.3 de l'annexe 1 de la LPRPDE reconnaît expressément que des renseignements personnels peuvent être transférés à une tierce partie aux fins de traitement. Il oblige aussi les organisations à fournir, par voie contractuelle ou autre, « un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie ».

Le principe 1 précise que :

« Une organisation est responsable des renseignements personnels qu'elle a en sa possession ou sous sa garde, y compris les renseignements confiés à une tierce partie aux fins de traitement. L'organisation doit, par voie contractuelle ou autre, fournir un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie. »



QUE SIGNIFIENT LES TERMES EMPLOYÉS DANS LE PREMIER PRINCIPE?

Transfert

Le « transfert » constitue une utilisation de l'information par l'organisation, à ne pas confondre avec une communication. Lorsqu'une organisation transfère des renseignements personnels aux fins de traitement, ces renseignements ne peuvent être utilisés qu'aux fins pour lesquelles ils ont été recueillis à l'origine; par exemple, des renseignements personnels peuvent être transférés afin de traiter les paiements des clients, ou encore transférés à une tierce partie par un fournisseur de services Internet pour assurer la disponibilité d'un soutien technique 24 heures sur 24, 7 jours sur 7. Les organisations impartissent de plus en plus les processus à des tierces parties. Dans bien des cas, un transfert d'information est nécessaire pour ce faire. Dans le cadre de ce document, lorsqu'il est fait mention d'impartition, on fait référence à l'impartition qui concerne des renseignements personnels.

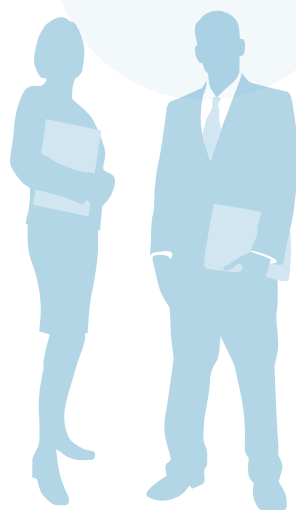
La LPRPDE ne fait pas la distinction entre les transferts nationaux et internationaux de données.

Traitement

Le « traitement » est interprété de façon à englober toute utilisation de l'information par la tierce partie traitant les renseignements afin que ceux-ci puissent être utilisés par l'organisation qui les transfère.

Degré comparable de protection

« Degré comparable de protection » signifie que la tierce partie qui traite les renseignements doit fournir une protection comparable au niveau de protection qui serait fourni si l'information n'avait pas été transférée. Cela ne veut pas dire que les mesures de protection devraient être les mêmes partout, mais qu'elles devraient généralement s'équivaloir.



QUE DOIVENT FAIRE LES ORGANISATIONS?

Le premier principe suppose que les organisations protègent principalement les renseignements personnels qu'elles envoient à des tierces parties aux fins de traitement par voie contractuelle.

Peu importe l'endroit où l'information est traitée, que ce soit au Canada ou dans un pays étranger, l'organisation doit prendre toutes les mesures raisonnables pour protéger celle-ci contre l'utilisation ou la communication non autorisées par la tierce partie. L'organisation doit avoir l'assurance que la tierce partie a mis en place des politiques et des processus, y compris de la formation à l'intention de son personnel et des mesures de sécurité efficaces, pour s'assurer que l'information qu'elle a sous sa garde est adéquatement protégée en tout temps. Elle devrait également se réserver le droit de vérifier et d'inspecter les moyens de traitement et de stockage employés par la tierce partie, et se prévaloir de son droit de vérifier et d'inspecter lorsque c'est opportun.

Le Commissariat à la protection de la vie privée du Canada est conscient que l'univers électronique est complexe et qu'il s'avère parfois impossible pour une organisation de savoir précisément où circule l'information en cours de transit. Cela dit, la loi précise clairement où réside la responsabilité, et les organisations doivent, dans leur propre intérêt et dans celui de leur clientèle, faire tout en leur pouvoir pour protéger l'information.

Toutefois, aucun contrat ni autre moyen ne peut avoir préséance sur les lois d'une administration étrangère.

Alors, comment une organisation peut-elle s'y prendre pour remplir ses obligations aux termes du principe 4.1.3 de l'annexe 1 de la LPRPDE pour ce qui est des transferts à des pays étrangers lorsque survient la question de l'accès aux renseignements personnels par des organismes d'application de la loi, des agences de sécurité nationale et des tribunaux étrangers?

Dans le cadre d'une enquête faisant suite à une plainte concernant le transfert de renseignements à une entreprise établie aux États-Unis par Visa CIBC, le Commissariat à la protection de la vie privée du Canada a conclu que la CIBC



respectait la LPRPDE. Le Commissariat à la protection de la vie privée du Canada s'est référé aux lignes directrices du Bureau du surintendant des institutions financières (BSIF) s'appliquant aux institutions financières sous réglementation fédérale. Celles-ci recommandent aux organisations de porter une attention particulière aux exigences juridiques du pays où est établie la tierce partie qui traite les renseignements, de même qu'à « la situation politique, économique et sociale étrangère et aux événements susceptibles de réduire la capacité du fournisseur de services étranger d'assurer le service, sans oublier tout autre facteur de risque pouvant nécessiter l'ajustement du programme de gestion des risques ».

Même si ces lignes directrices établissent des normes élevées pour la protection de renseignements financiers de nature délicate par des institutions financières, d'autres organisations qui procèdent au transfert de renseignements personnels de nature délicate feraient bien de s'en inspirer également.

Nous supposons que toute organisation prend en considération une série de facteurs avant de décider de transférer des renseignements à une administration étrangère, notamment les économies de coûts potentielles, la capacité à fournir un meilleur service à la clientèle, la disponibilité d'une expertise spécialisée à l'extérieur de l'entreprise et d'autres considérations pratiques.

Dans les cas d'impartition à un pays étranger, la LPRPDE *n'exige pas* une comparaison exhaustive entre les lois canadiennes et les lois étrangères. Elle *exige* par contre que les organisations prennent en considération tous les éléments entourant la transaction. L'organisation pourrait ainsi se rendre compte qu'il serait mal avisé de procéder à certains transferts en raison de la nature instable d'un régime étranger. Dans d'autres cas, les renseignements se révèlent de nature si délicate qu'ils ne devraient être envoyés à aucune administration étrangère.

Les organisations doivent faire preuve de diligence dans toutes leurs opérations avec les tiers étrangers qui traitent leurs renseignements.

Pourquoi respecter la Loi?

- Vos clients s'attendent à ce que vous fassiez preuve de transparence au sujet de vos pratiques : ils s'informeront.
- Il s'agit de pratiques exemplaires : les suivre peut vous procurer un avantage concurrentiel.
- En vertu de la *Loi*, vous devez protéger les renseignements personnels lorsqu'ils sont entre les mains d'un tiers : le non-respect de la *Loi* pourrait entraîner des plaintes et des poursuites.



À QUOI DOIVENT S'ATTENDRE LES CONSOMMATEURS?

Les consommateurs devraient s'attendre à ce que leurs renseignements personnels soient protégés, peu importe l'endroit où ils sont traités. En fin de compte, les organisations qui transfèrent des renseignements personnels à des tierces parties sont responsables de la protection de ces renseignements. Les consommateurs devraient s'attendre à ce que les organisations fassent preuve de transparence en ce qui concerne le transfert de renseignements à des pays étrangers.

Ils ont le droit d'évaluer les risques que pose pour eux l'accès potentiel des autorités étrangères à leurs renseignements personnels. Certains sont plus enclins à la prudence, tandis que d'autres sont prêts à prendre certains risques moyennant plus de commodité ou l'accès à un service particulier.

Les organisations doivent **aviser leurs consommateurs de façon claire et compréhensible** que leurs renseignements personnels pourraient être traités dans un pays étranger, et que les organismes d'application de la loi et de sécurité nationale de ce pays pourraient y accéder. Idéalement, cela devrait être fait **au moment de la collecte des renseignements**. Une fois que des consommateurs avertis décident de faire affaire avec une entreprise, ils ne peuvent s'opposer à ce que leurs renseignements personnels soient transférés.

Conseils aux particuliers

- Exigez que les organismes fassent preuve de transparence : en cas de doute, renseignez-vous.
- Soyez conscient que la circulation transfrontière des renseignements est une réalité et est très répandue.
- Soyez un consommateur averti en matière de protection de la vie privée : ne tenez pas pour acquis que parce que vous n'avez « rien à cacher », vous ne devriez pas prendre tous les moyens pour exercer un contrôle sur les renseignements qui vous concernent.
- Si vous n'êtes pas à l'aise, vous pouvez vérifier quelles sont les pratiques de protection de la vie privée d'autres organisations. Vous pouvez également discuter de vos préoccupations avec des représentants du Commissariat.

RÉSUMÉ DES PRINCIPALES CONCLUSIONS

Le Commissariat à la protection de la vie privée du Canada a formulé un certain nombre de conclusions concernant les transferts transfrontaliers de renseignements personnels dans le cadre des enquêtes sur les plaintes réalisées au cours des dernières années :

- La LPRPDE n'interdit pas aux organisations du Canada de transférer des renseignements personnels à une organisation dans un pays étranger aux fins de traitement.
- La LPRPDE établit cependant des règles concernant les transferts aux fins de traitement.
- Un transfert aux fins de traitement est une « utilisation » de l'information; il ne s'agit pas d'une communication. Si les renseignements sont utilisés aux fins auxquelles ils ont été recueillis, aucun consentement supplémentaire n'est requis pour procéder au transfert.
- L'organisation qui procède au transfert est responsable des renseignements qui sont remis à l'organisation qui les reçoit.
- Les organisations sont tenues de protéger les renseignements personnels qui se trouvent entre les mains des tiers qui les traitent. Le moyen principal d'assurer cette protection est par voie contractuelle.
- Aucun contrat ne peut avoir préséance sur les lois en matière de criminalité, de sécurité nationale et autres du pays vers lequel les renseignements ont été transférés.
- Il est important que les organisations évaluent les risques que l'intégrité, la sécurité et la confidentialité des renseignements personnels de leurs clients soient compromises au moment ou à la suite du transfert à un tiers fournisseur de services exerçant des activités à l'extérieur du Canada.
- Les organisations doivent faire preuve de transparence au sujet de leurs pratiques de traitement des renseignements personnels. Elles doivent notamment informer les consommateurs que leurs renseignements personnels pourraient être envoyés dans un autre pays aux fins de traitement, et que les tribunaux, organismes d'application de la loi et agences de sécurité nationale de ce pays pourraient y accéder.





Commissariat
à la protection de
la vie privée du Canada

POUR PLUS DE RENSEIGNEMENTS

Le Commissariat à la protection de la vie privée du Canada a publié un certain nombre de conclusions d'enquêtes liées aux transferts transfrontaliers de renseignements personnels. Dans tous ces cas, nous avons conclu que le transfert ne contrevenait pas à la LPRPDE. Consultez ces quelques résumés de conclusions d'enquête en vertu de la LPRPDE, sur le site Web du Commissariat, à www.privcom.gc.ca :

- n° 394 : L'impartition des services de courriel de canada.com à une entreprise établie aux États-Unis suscite des questions parmi les abonnés
- n° 365 : Responsabilité d'institutions financières canadiennes dans la communication de renseignements personnels par SWIFT aux autorités des États-Unis
- n° 313 : Un avis expédié aux clients d'une banque suscite des inquiétudes à propos de la *USA PATRIOT Act*

Industrie Canada présente de la documentation supplémentaire sur son site Web. Consultez l'adresse suivante : <http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/fra/gv00508.html>