

En quoi consiste la Loi sur la protection des renseignements personnels et les documents électroniques?

La Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) protège les renseignements personnels détenus par des entreprises du secteur privé et fournit des lignes directrices pour la collecte, l'utilisation et la divulgation de cette information dans le cadre d'activités commerciales. La Loi est chapeautée par le Commissaire à la protection de la vie privée.

Les renseignements personnels y sont définis comme « tout renseignement concernant un individu identifiable ». Il peut s'agir par exemple du nom d'une personne, de son adresse, de son numéro de téléphone, de son sexe, de ses numéros d'identification, de son revenu, de son groupe sanguin, de son dossier de crédit, de ses registres de prêts et autres renseignements. La LPRPDE couvre également tout renseignement personnel sensible comme ceux relatifs à l'état de santé d'une personne, à son dossier médical, à ses origines ethniques ou raciales, à ces opinions politiques, à ses croyances religieuses, à ses appartenances syndicales et l'information financière la concernant.

Qui est visé par cette Loi ?

Depuis le 1er janvier 2004, toutes les entreprises canadiennes ayant des activités commerciales doivent de conformer aux 10 grands principes de la Loi concernant la confidentialité. La Loi couvre les entreprises, les associations, les partenariats et les syndicats, y compris les organismes engagés dans la vente, la location ou l'échange de listes de donneurs, de membres ou autres listes servant à des campagnes de financement.

En quoi cette Loi concerne-t-elle la gestion de l'information ?

La Loi établit l'obligation de l'entreprise de protéger les renseignements qu'elle recueille. Les organisations qui négligent de protéger les renseignements personnels s'exposent à des risques importants, comprenant notamment des poursuites et des sanctions réglementaires ou liées à l'industrie. Elles risquent aussi, bien sûr, de voir leur réputation, leur marque et leurs relations d'affaires entachées.

Plus précisément, l'annexe 1, article 5 de la LPRPDE souligne 10 grands principes. Les principes 5 et 7 ont trait à la conservation et à la destruction de documents :

4.5 Cinquième principe – Limitation de l'utilisation, de la communication et de la conservation – « Les organisations qui se servent de renseignements personnels à des fins nouvelles doivent documenter ces fins » (voir article 4.2.1). Les organisations devraient élaborer des lignes directrices et appliquer des procédures pour la conservation des renseignements personnels. Ces lignes directrices devraient préciser les durées minimales et maximales de conservation.

On doit conserver les renseignements personnels servant à prendre une décision au sujet d'une personne suffisamment longtemps pour permettre à la personne concernée d'exercer son droit d'accès à l'information, après que la décision a été prise. Une organisation peut être assujettie à des exigences prévues par la Loi en ce qui concerne les périodes de conservation.

On devrait détruire, effacer ou dépersonnaliser les renseignements personnels dont on n'a plus besoin aux fins précisées. Les organisations doivent élaborer des lignes directrices et appliquer des procédures régissant la destruction des renseignements personnels.

Ce principe est en lien direct avec le principe de consentement (paragraphe 4.3), avec la détermination des fins de la collecte des renseignements (paragraphe 4.2) et avec le principe de l'accès aux renseignements personnels (paragraphe 4.9).

4.7 Septième principe – Mesures de sécurité – « Les mesures de sécurité doivent protéger les renseignements personnels contre la perte ou le vol ainsi que contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées. Les organisations doivent protéger les renseignements personnels, quelle que soit la forme sous laquelle ils sont conservés.

La nature des mesures de sécurité variera en fonction du degré de sensibilité des renseignements personnels recueillis, de la quantité, de la répartition et du format des renseignements personnels ainsi que des méthodes de conservation. Les renseignements plus sensibles devraient être mieux protégés. La notion de sensibilité est présentée à l'article 4.3.4.

Les méthodes de protection devraient comprendre :

- a) des moyens matériels, par exemple le verrouillage des classeurs et la restriction de l'accès aux bureaux;
- b) des mesures administratives, par exemple des autorisations sécuritaires et un accès sélectif;
- c) des mesures techniques, par exemple l'usage de mots de passe et du chiffrement.

Les organisations doivent sensibiliser leur personnel à l'importance de protéger le caractère confidentiel des renseignements personnels.

Au moment du retrait ou de la destruction des renseignements personnels, on doit veiller à empêcher les personnes non autorisées d'y avoir accès (article 4.5.3). »

Que doivent faire les entreprises pour se conformer à la LPRPDE?

La question de la conformité est abordée abondamment dans le texte de la Loi. De façon générale, les entreprises doivent disposer d'une politique de confidentialité, formulée à partir des dix principes de confidentialité de la LPRPDE. Cette politique doit aborder la question des pratiques en matière de gestion, de collecte, d'utilisation, de divulgation, de conservation, de sécurité et de destruction de l'information.

Assurer la conformité à la Loi est la responsabilité du Commissaire à la protection de la vie privée du Canada. La partie 1, section 2 de la Loi traite du processus de dépôt d'un avis de non-conformité et d'enquête pour non-conformité. Les plaintes reçues font l'objet d'une enquête et, comme on le précise dans cette section de la Loi, « le Commissaire peut tenter de parvenir au règlement de la plainte en ayant recours à un mode

de règlement des différends, notamment la médiation et la conciliation ». Le Commissaire peut aussi faire appel à la Cour fédérale pour une audience du tribunal. La question des audiences est abordée à la partie 1, section 2, articles 14 à 17 de la Loi. L'article 16 se penche sur les réparations possibles :

« 16. La Cour peut, en sus de toute autre réparation qu'elle accorde : (a) ordonner à l'organisation de revoir ses pratiques de façon à se conformer aux articles 5 à 10; (b) lui ordonner de publier un avis énonçant les mesures prises ou envisagées pour corriger ses pratiques, que ces dernières aient ou non fait l'objet d'une ordonnance visée à l'alinéa a); (c) accorder au plaignant des dommages-intérêts, notamment en réparation de l'humiliation subie. » Il n'y a pas de limite aux dommages-intérêts que la Cour peut accorder. De même, le neuvième principe exige que les organisations permettent à tout individu de consulter les renseignements qu'elles détiennent à leur sujet, sur demande. Les organisations sont tenues de répondre à de telles demandes dans les 30 jours.

Comment pouvons-nous vous aider ?

Securit gestion d'archives offre aux entreprises l'assurance que leurs documents sont entreposés de façon sécuritaire, tout en demeurant accessibles au besoin.

Que vous souhaitiez détruire des renseignements quotidiennement ou à la fin d'une période donnée, Securit veille à ce que les documents soient entièrement détruits sur place, par les représentants Securit. Une fois les documents détruits, Securit vous remet un certificat de destruction qui prouve que les documents en question ont été détruits comme il se doit. Pour avoir l'esprit tranquille, appelez dès aujourd'hui Securit en composant le 1 800 697 4733.

Pour en savoir plus :

Commissaire à la protection de la vie privée du Canada : www.privcom.gc.ca

Industries Canada, Protection des renseignements en affaires : <http://privacyforbusiness.ic.gc.ca/epic/internet/inpfb-cee.nsf/fr/Home>

Ce document ne constitue pas un avis juridique ni un conseil juridique. Prière de ne pas se fier à ce document sans avoir d'abord obtenu un avis juridique.

© Copyright 2005