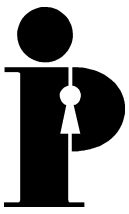
Commissaire à
l'information et à
protection de la
vie privée/Ontario

Pratiques exemplaires de protection de la vie privée dans les transactions en ligne



Ann Cavoukian, Ph.D.
Commissaire
Juin 2001

Commissaire à l'information et à la protection de la vie privée/Ontario

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
M4W 1A8

416-326-3333
1-800-387-0073
Télécopieur : 416-325-9195
ATS (Téléimprimeur) : 416-325-7539
Site Web : www.ipc.on.ca

Cette publication est disponible sur le site Web du Bureau du commissaire.

This publication is also available in English.

Table des matières

Introduction

L'inforoute ouvre aux entreprises canadiennes de nouveaux débouchés fort intéressants. Les consommateurs sont attirés par le commerce électronique non seulement en raison des produits et des services offerts, mais aussi en raison de la commodité des transactions en ligne et des économies qu'elles permettent de réaliser.

Cependant, il semble bien que la croissance du commerce électronique soit entravée par les craintes des consommateurs concernant la protection de leur vie privée dans les transactions en ligne. Une enquête menée récemment a révélé que huit consommateurs canadiens sur dix veulent que les renseignements personnels les concernant soient protégés lorsqu'ils participent à des activités en ligne et que 40 % ne croient pas que les entreprises en ligne respectent leur politique de protection de la vie privée[1].

Les craintes des consommateurs concernant la protection de leur vie privée ne sont pas dénuées de fondement, et elles sont en fait renforcées par des reportages fréquents sur les mauvaises pratiques de protection de la vie privée dans les transactions en ligne et l'accès non autorisé aux données en ligne. Une étude canadienne des sites Web commerciaux a révélé que :

- dans la moitié des sites étudiés, on ne retrouvait pas de politique de protection de la vie privée;
- 40 % des sites n'indiquaient pas s'ils échangeaient les renseignements qu'ils recueillaient avec des tiers;
- 26 % utilisaient des témoins (« cookies »), sans le dire aux utilisateurs;
- moins de la moitié fournissaient les coordonnées de personnes-ressources;
- plus de 60 % ne permettaient pas aux utilisateurs d'accéder aux renseignements qu'ils avaient soumis[2].

L'une des conclusions les plus troublantes de cette étude est que les sites canadiens protègent beaucoup moins bien la vie privée que les sites d'autres pays qui ciblent les utilisateurs canadiens[3].

De toute évidence, la nécessité de susciter et de préserver la confiance des consommateurs réels ou éventuels représente un défi de taille pour les entreprises qui font des affaires en ligne, et est garante de la réussite commerciale à long terme. La protection de la vie privée est un élément essentiel à cette fin.

---

[1] David Akin, « Canadians still not sold on Net privacy policies », *National Post Online*, 17 janvier 2001, <http://www.nationalpost.com/tech/story/html?f=/stories/20010117/439311/html>, 01/18/01.

[2] Natalie Southworth, « Canadian Web sites woeful in privacy: survey », *The Globe and Mail*, 7 décembre 2000, p. B-9.

[3] Michael Geist, « A troubling snapshot of e-privacy in Canada », *The Globe and Mail*, 7 décembre 2000, p. T-4.

Outre les pressions des consommateurs, les entreprises canadiennes doivent également composer avec l'évolution du cadre législatif régissant la protection de la vie privée dans le secteur privé. Afin de pouvoir susciter la confiance des consommateurs et de respecter les dispositions législatives, les entreprises qui souhaitent réussir dans le monde du commerce électronique s'emploient à faire de la protection de la vie privée une partie intégrante de leurs initiatives commerciales.

Les entreprises en ligne doivent s'empresser de comprendre leur obligation de respecter la vie privée de leurs clients et reconnaître qu'elles doivent :

- recueillir, utiliser ou divulguer des renseignements personnels de manière responsable;
- maximiser le contrôle qu'exercent leurs clients sur les renseignements personnels les concernant;
- s'assurer que leurs pratiques de gestion de l'information sont transparentes pour les consommateurs.

En plus de respecter la loi, la protection de la vie privée est essentielle à la compétitivité en ligne. Pour faire des affaires, il est nécessaire d'assurer efficacement la protection de la vie privée. Les entreprises qui ne protègent pas adéquatement la vie privée de leurs clients s'exposent à des risques importants et à des conséquences fâcheuses d'ordre commercial et légal.

Pour encourager les entreprises à examiner leur façon de faire des affaires en ligne et à mieux intégrer la protection de la vie privée dans ces pratiques, le Bureau du commissaire à l'information et à la protection de la vie privée/Ontario[4] (le « Bureau du commissaire ») a élaboré une série de pratiques exemplaires visant la protection de la vie privée dans les transactions en ligne. Ces pratiques soulignent les aspects à aborder pour bien protéger la vie privée des consommateurs en ligne. Elles se chevauchent et sont reliées entre elles, ce qui signifie que pour bien protéger la vie privée, les 11 aspects doivent être pris en considération. Cependant, ces pratiques n'ont pas à être adoptées intégralement; elles sont plutôt présentées sous forme de liste dans laquelle vous pouvez choisir celles qui conviennent le mieux à votre situation.

Cette série de pratiques exemplaires se veut un instrument d'éducation et n'a pas pour objet de remplacer les lois existantes ou futures, les accords internationaux, les conditions d'adhésion des associations industrielles ou d'autres dispositions obligatoires ou facultatives que les entreprises qui font des affaires en ligne doivent respecter. Cependant, elle peut servir de point de départ à l'élaboration de pratiques de protection de la vie privée dans les entreprises qui font des affaires en ligne.

[4] Pour de plus amples renseignements sur le Bureau du commissaire à l'information et à la protection de la vie privée/Ontario, consulter son site Web à <www.ipc.on.ca>.

Pratiques exemplaires

Respect de la vie privée

- Faire des affaires d'une manière qui porte le moins possible atteinte à la vie privée.

- Comprendre et respecter les lois, normes et accords régissant la protection de la vie privée.

- Comprendre que les renseignements personnels comprennent tous les renseignements concernant une personne qui peut être identifiée ou liés à cette personne, notamment le nom, l'adresse, le numéro de carte de crédit, le revenu, les préférences quant aux achats et les données transactionnelles. Les adresses électroniques et les données recueillies au moyen de méthodes de repérage automatique peuvent constituer des renseignements personnels si elles sont liées à une personne qui peut être identifiée.

- Reconnaître que les particuliers ont le droit d'exercer un contrôle raisonnable sur les données qui les concernent.

- Évaluer l'incidence sur la protection de la vie privée des pratiques, services, produits ou technologies en ligne avant leur mise en oeuvre.

- Faire preuve de prudence si les produits ou les services de l'entreprise sont destinés aux enfants. S'il est probable que des données seront recueillies auprès des enfants ou que des données concernant des enfants seront utilisées ou divulguées, suivre les pratiques appropriées concernant la protection de la vie privée (p. ex., les éléments spéciaux concernant les enfants contenus dans *Code de déontologie et Normes de pratiques* de l'Association canadienne du marketing).

Transparence

- Élaborer des politiques et des pratiques de protection de la vie privée exigeant que les renseignements personnels soient manipulés avec transparence et d'une manière responsable.

- Faire preuve de transparence concernant les politiques et pratiques de l'entreprise touchant les renseignements personnels.

- S'assurer que les politiques et les pratiques déclarées sont informatives, exactes et complètes. Ne pas représenter faussement l'identité de l'entreprise ou ses pratiques de gestion de l'information.

- Informer les particuliers, sur demande, des documents que l'entreprise possède et qui contiennent des renseignements personnels les concernant, la façon dont l'entreprise les utilise et les données qu'elle divulgue.

- Fournir aux particuliers suffisamment de renseignements pour qu'ils puissent comprendre leurs droits en matière de protection de la vie privée, et leur donner l'occasion d'exercer ces droits rapidement, efficacement et à des coûts raisonnables. Ces renseignements devraient comprendre le nom ou le titre d'une personne-ressource ou les coordonnées du service de l'entreprise responsable de ses politiques et pratiques de protection de la vie privée, ainsi que des précisions concernant la façon dont les particuliers peuvent accéder aux renseignements personnels qui les concernent et dont l'entreprise a le contrôle.

- Afficher sur le site Web de l'entreprise sa politique de protection de la vie privée, expliquant clairement toutes ses responsabilités et pratiques en matière d'information. Cette politique devrait notamment être :

    - facile à trouver, à lire, à imprimer et à comprendre (p. ex., contenir des exemples expliquant et démontrant les pratiques de l'entreprise);

    - accessible de n'importe quelle page Web, pas seulement de la page d'accueil;

    - rédigée dans la même langue que le site Web auquel elle est annexée.

- En cas de modification des politiques et pratiques déclarées en matière de protection de la vie privée, laisser assez de temps aux personnes concernées pour qu'elles puissent prendre des décisions éclairées et les mesures appropriées.

- Informer les particuliers :

    - de tous les accords et textes législatifs applicables qui régissent la protection de la vie privée, en prévoyant des liens vers les sites Web des autorités responsables de leur administration et de leur application;

    - de tous les codes de déontologie professionnelle et programmes de délivrance de labels de qualité ou autres que l'entreprise doit respecter, en établissant des liens vers le texte complet de ces documents et vers les sites Web des organismes responsables de leur administration et de leur application;

    - des conséquences pour l'entreprise de l'inobservation de ses politiques et pratiques de protection de la vie privée et des programmes et textes législatifs pertinents (p. ex., vérification, sanctions, révocation du label de qualité, perte de l'adhésion, dépôt de plaintes à un organisme de surveillance pour enquête, publication du nom pour inobservation);

    - de leur recours s'ils croient que l'entreprise ne respecte pas ses politiques et pratiques de protection de la vie privée ou d'autres programmes ou textes législatifs pertinents.

- Expliquer l'utilisation d'instruments Web pour recueillir des renseignements personnels à l'insu de l'utilisateur : logiciels de repérage automatique, données sur le parcours (« clickstream »), témoins et images GIF invisibles.

- Expliquer les pratiques de sollicitation de l'entreprise (courrier électronique et autres moyens) ainsi que les renseignements personnels qu'elle échange avec des tiers, ou qu'elle leur loue ou vend, à des fins de marketing ou autres.

- Informer les particuliers :

    - que le traitement des données recueillies, utilisées et divulguées en ligne est différent du traitement des données hors ligne, le cas échéant, en leur indiquant d'autres moyens de communiquer avec l'entreprise (p. ex., poste, en personne, télécopieur, téléphone);

    - des politiques de sécurité ou de protection de la vie privée qui ont été violées, le cas échéant, relativement aux renseignements personnels qui les concernent, le plus rapidement possible, ainsi que des mesures qu'ils peuvent prendre pour régler le problème ou minimiser les risques.

Responsabilité

- Veiller à ce que la protection de la vie privée constitue une priorité à tous les paliers de l'entreprise. Un engagement de la haute direction envers les politiques et les pratiques de protection de la vie privée est essentiel à la réussite.

- Comprendre que la collecte de renseignements personnels signifie que l'entreprise accepte la responsabilité de les traiter conformément à ses politiques et pratiques déclarées en matière de protection de la vie privée et de rendre ces renseignements accessibles aux particuliers concernés.

- Assurer la formation du personnel et lui inculquer la responsabilité de respecter les politiques et pratiques de l'entreprise en matière de protection de la vie privée.

- Désigner un employé ou un poste responsable de la protection de la vie privée et du respect des politiques de l'entreprise en matière de protection de la vie privée. Même si, dans les grandes entreprises, il peut être nécessaire de former une équipe ou un groupe chargé d'élaborer et de mettre en oeuvre les politiques, selon différents niveaux de responsabilité, une personne devrait avoir la responsabilité finale et disposer des ressources et des pouvoirs nécessaires pour s'en acquitter efficacement et rapidement.

- Indiquer sur le site Web de l'entreprise l'identité de la personne responsable, ses coordonnées ainsi que les jours et les heures où on peut la joindre.

- Établir des procédures d'examen des politiques et pratiques de protection de la vie privée pour qu'elles soient exactes, complètes et à jour.

- Élaborer un processus permettant de vérifier et de démontrer la mesure dans laquelle l'entreprise respecte ses politiques et pratiques de protection de la vie privée.

- Définir l'obligation de l'entreprise de prendre toutes les mesures nécessaires pour corriger les problèmes qui découlent de l'inobservation de ses propres politiques et pratiques ou de dispositions législatives.

- Inclure des exigences en matière de protection de la vie privée, comparables aux politiques et pratiques de l'entreprise, dans les contrats avec des partenaires d'affaires ou des tiers qui auront accès à des renseignements personnels que l'entreprise aura recueillis ou dont elle a le contrôle. Cela est particulièrement important si l'entreprise envoie des renseignements personnels dans des territoires où il n'existe pas de règlement comparable de protection de la vie privée. Prendre toutes les mesures nécessaires pour faire en sorte que la partie au contrat suive les mesures de protection de la vie privée précisées dans le contrat (p. ex., visites sur place, vérifications).

Précision des fins

- Définir les fins auxquelles servira chaque renseignement personnel (p. ex., nom, adresse, adresse électronique, données sur le parcours, âge, sexe, revenu, etc.), c'est-à-dire les raisons pour lesquelles ils sont nécessaires, afin de conclure une transaction d'affaires légitime. Pour déterminer les fins possibles, vérifier :

    - s'il est possible d'utiliser des renseignements non identificateurs (p. ex., données codées, anonymes ou regroupées, pseudonymes);

    - comment les renseignements personnels doivent être recueillis (p. ex., directement du particulier, par l'entremise d'un abonnement, collecte automatique des données sur le parcours, collecte auprès d'un tiers) et pour quelles raisons;

    - qui devra utiliser les renseignements (à l'intérieur et à l'extérieur de l'entreprise) et pour quelles raisons;

    - à qui les renseignements devront être divulgués et pour quelles raisons.

- Préciser les raisons pour lesquelles il faut recueillir, utiliser ou divulguer des renseignements personnels qui ne se rapportent pas directement à la transaction (p. ex., programmes de primes, ciblage des services de marketing par courrier électronique, exploration de données, etc.).

- Comprendre que les fins visées doivent raisonnablement se rapporter à l'entreprise.

- Ne pas définir les fins de manière si vague qu'elles n'ont pas de sens pour la personne auprès de qui l'entreprise veut recueillir des renseignements personnels.

- Documenter les fins de façon que le personnel et les particuliers concernés par les renseignements personnels sachent ce qu'elles sont.

- Préciser les nouvelles fins auxquelles serviront des renseignements personnels déjà recueillis avant leur utilisation.

Connaissance[5] et consentement[6] des particuliers

- Obtenir le consentement du particulier avant de recueillir des renseignements personnels à son sujet, dans la mesure du possible. Veiller à ce que les particuliers comprennent les fins auxquelles les renseignements personnels les concernant sont recueillis, utilisés et divulgués avant d'obtenir leur consentement.

- Utiliser des dispositions expresses de consentement dans la mesure du possible. Établir les options implicites concernant le consentement de manière à protéger le plus possible la vie privée (c'est-à-dire ne pas utiliser une option négative telle que des cases préalablement cochées qui exigent que les particuliers posent un geste pour indiquer ce à quoi ils consentent et ne consentent pas).

- Tenir compte du caractère délicat des renseignements personnels en cause au moment de déterminer le genre de consentement approprié. En règle générale, les données plus délicates (p. ex., renseignements médicaux ou financiers) devraient être assorties d'un consentement exprès plutôt qu'implicite.

- Définir de manière restreinte les circonstances exceptionnelles dans lesquelles le consentement n'est pas possible ou serait inapproprié. Dans des circonstances très limitées, il faudra peut-être recueillir, utiliser ou divulguer des renseignements personnels sans que la personne concernée ne donne son consentement (p. ex., à des fins d'exécution de la loi ou lorsque la personne est mineure, gravement malade ou frappée d'incapacité mentale).

- Fournir aux particuliers des renseignements clairs et adéquats qui leur permettront de donner ou non leur consentement de manière éclairée, notamment les conséquences du refus ou du retrait du consentement, le cas échéant. Les personnes devraient pouvoir retirer leur consentement en tout temps, sous réserve de restrictions juridiques ou contractuelles et moyennant un préavis raisonnable.

- Fournir aux particuliers un mécanisme en ligne simple, clair et sûr leur permettant de donner, de refuser ou de retirer leur consentement concernant :

    - la collecte, l'utilisation et la divulgation des renseignements personnels les concernant;
    - le stockage, la modification ou la copie de renseignements contenus dans leur ordinateur;
    - l'utilisation de logiciels de repérage automatique, par l'entreprise ou un tiers, notamment la divulgation automatique de données sur le parcours à des tiers;
    - la réception en ligne ou hors ligne de documents de marketing ou de promotion de l'entreprise ou de tiers.

[5] La connaissance désigne le fait, pour une personne, de connaître et de comprendre une chose et ses répercussions.

[6] Le consentement désigne le fait, pour une personne, de donner sa permission ou de convenir d'une chose. Il y a consentement exprès lorsque le consentement est donné explicitement et sans ambiguïté (p. ex., « Oui, je consens à ce que vous vendiez mon adresse postale à une tierce partie. ») Il y a consentement implicite lorsqu'il est raisonnable de conclure ou de sous-entendre qu'il y a consentement selon l'activité ou l'inactivité d'une personne (p. ex., si une personne achète un livre en ligne, il est raisonnable de conclure que la personne consent à ce que le vendeur de livres donne son adresse postale à la compagnie de livraison).

- Ne pas tromper les particuliers, ni exercer de pressions, pour obtenir leur consentement.

- Ne pas rendre le produit ou le service disponible à condition que les particuliers consentent à des fins qui ne sont pas compatibles avec le produit ou le service en question.

- Ne pas retirer des produits ou des services déjà disponibles si les particuliers ne consentent pas à l'utilisation ou à la divulgation de renseignements personnels les concernant à de nouvelles fins ou à des fins incompatibles.

- Informer les particuliers de ce que couvrent exactement les dispositions de l'entreprise sur le consentement, et de ce qu'elles ne couvrent pas (p. ex., collecte par l'entremise du site Web seulement ou par l'entremise d'une tierce partie également), et de la durée de leur consentement, le cas échéant.

- Veiller à ce que les particuliers comprennent pourquoi on ne demande pas leur consentement, le cas échéant (p. ex., après qu'une personne a donné son consentement initial et sauf avis contraire de sa part, l'entreprise ne lui demande pas la permission d'utiliser des témoins permanents chaque fois qu'elle visite le site).

- Prendre des mesures raisonnables pour vérifier que la personne qui donne le consentement est autorisée à le faire (p. ex., il s'agit du particulier concerné par les renseignements personnels ou de son représentant autorisé).

- Lorsque le produit ou le service de l'entreprise est destiné aux enfants, prendre des mesures raisonnables pour s'assurer que la personne a l'âge légal pour donner son consentement. Au besoin, obtenir le consentement explicite et vérifiable du père, de la mère, de la tutrice ou du tuteur autorisé de l'enfant avant la collecte, l'utilisation ou la divulgation de renseignements personnels concernant cet enfant.

- Obtenir le consentement du particulier concerné par les renseignements personnels avant d'utiliser ces données à de nouvelles fins ou à des fins incompatibles, sauf lorsque ces fins sont exigées par une loi.

- Ne pas supposer que parce qu'une personne a visité le site de l'entreprise ou même acheté un produit, elle consent à la sollicitation.

- Ne pas exiger des particuliers qu'ils appellent ou écrivent pour indiquer qu'ils ne consentent pas à l'utilisation des renseignements personnels les concernant qui ont été recueillis en ligne. En demandant le consentement, demander aux particuliers l'autorisation de faire un suivi auprès d'eux et comment communiquer avec eux, le cas échéant. Tenir un registre des consentements et le rendre accessible aux particuliers qui veulent l'examiner.

- Ne pas révoquer les options de refus ni modifier les délais sans en avoir informé au préalable les particuliers.

Limites quant à la collecte

- Dans la mesure du possible, ne pas recueillir de renseignements identificateurs (p. ex., permettre aux personnes de visiter le site Web de l'entreprise sans saisir de données sur le parcours ou de faire leurs transactions de manière anonyme ou en utilisant un pseudonyme).

- Ne recueillir que la quantité et le genre de renseignements personnels nécessaires et pertinents aux fins identifiées ou exigées par la loi.

- Recueillir des renseignements personnels en utilisant des moyens équitables et légaux et à partir de sources fiables.

- Ne pas recueillir de renseignements personnels par des moyens détournés, par coercition ou par des pratiques trompeuses.

- Informer les particuliers, au moment de la collecte ou avant, du genre de renseignements personnels qui seront recueillis, y compris les données recueillies par voie électronique.

- Informer les particuliers, au moment de la collecte ou avant, que tous les renseignements personnels sont recueillis en vertu de la loi, le cas échéant, et expliquer en détail les dispositions législatives en question.

- Recueillir les renseignements personnels directement auprès de la personne concernée, sauf dans des circonstances particulières et bien délimitées.

- Informer les particuliers du genre de renseignements personnels qui sont recueillis indirectement (p. ex., auprès de tiers) pour offrir les produits et les services de l'entreprise, ainsi que la source, en expliquant pourquoi la collecte directe est impossible ou ne convient pas.

- Ne pas permettre à des tiers de recueillir des renseignements personnels ou des témoins par l'entremise du site Web de l'entreprise à moins qu'ils ne soient liés par des normes semblables en matière de protection de la vie privée.

- Éviter de recueillir des renseignements identificateurs uniques (p. ex., NAS ou numéro de permis de conduire), sauf si leur utilisation est exigée par la loi ou si la personne a donné son consentement exprès. S'il est nécessaire de recueillir des renseignements identificateurs uniques (p. ex., à des fins fiscales), expliquer les raisons à la personne au moment de la collecte ou avant.

- Respecter les restrictions législatives touchant la collecte de renseignements personnels (p. ex., la législation sur les droits de la personne peut limiter le genre de renseignements qui peuvent être recueillis dans une demande d'emploi).

Limites quant à l'utilisation et à la divulgation

- Utiliser les renseignements personnels uniquement de la manière et aux fins indiquées au particulier au moment de la collecte, sauf si le particulier concerné par les renseignements personnels consent à ce qu'ils soient utilisés autrement ou à d'autres fins, ou encore si la loi l'exige.

- Ne pas divulguer ou distribuer les renseignements personnels, ni les rendre disponibles de quelque manière que ce soit, sauf aux fins et aux sources indiquées au particulier concerné au moment de la collecte, sauf si ce dernier y consent ou si la loi l'exige.

- Prendre toutes les mesures nécessaires pour faire en sorte que les renseignements personnels que l'entreprise utilise et divulgue soient nécessaires et pertinents aux fins identifiées ou à l'exécution de la loi.

- Utiliser les politiques et les restrictions techniques nécessaires pour contrôler les utilisations et les divulgations non autorisées et non pertinentes.

- Limiter l'utilisation des témoins permanents aux aspects où ils sont requis à des fins continues. La date d'expiration d'un témoin devrait correspondre à la fin prévue.

- Informer les particuliers de l'obligation législative qu'a l'entreprise de divulguer des renseignements personnels, le cas échéant, et à qui elle doit les divulguer. Inclure ce renseignement dans les politiques de l'entreprise en matière de protection de la vie privée.

- Informer les personnes des circonstances dans lesquelles la divulgation peut se faire à leur insu ou sans leur consentement (p. ex., en cas de menace grave et imminente à la santé et à la sécurité publiques). Inclure ces raisons dans les politiques de l'entreprise en matière de protection de la vie privée.

- Ne pas sciemment divulguer ou transmettre des renseignements personnels à des tiers sans mesures appropriées de protection de la vie privée.

- Établir des mécanismes de contrôle appropriés et efficaces et des échéanciers de conservation et de destruction des renseignements personnels. Veiller à ce que toutes les pratiques soient bien documentées.

- Conserver les renseignements personnels contenant des identificateurs uniquement tant qu'ils sont nécessaires et compatibles avec les fins pour lesquelles ils ont été recueillis, en vertu de loi ou pour permettre aux particuliers que les renseignements personnels concernent d'accéder à ces renseignements et de les corriger au besoin.

- Détruire, effacer ou dépersonnaliser de manière permanente les renseignements personnels devenus inutiles.

- Tenir un registre de divulgation de manière à mettre à jour les tiers qui ont déjà reçu des renseignements personnels de l'entreprise, au besoin (p. ex., dans les cas où des renseignements divulgués sont rectifiés en raison d'inexactitudes).

Exactitude

- Ne pas recueillir, utiliser ou divulguer des renseignements personnels inexacts.

- Prendre des dispositions raisonnables pour que les renseignements personnels soient exacts, complets et à jour, compte tenu de la nature des données, des fins auxquelles ils sont recueillis, utilisés et divulgués ainsi que des intérêts du particulier concerné par les renseignements.

- Mettre en oeuvre des mesures raisonnables afin de minimiser les risques que des données inexactes soient utilisées pour prendre une décision concernant un particulier. Pour déterminer quelles mesures il convient de mettre en oeuvre, tenir compte du degré de préjudice qui peut être causé au particulier si des données inexactes sont utilisées ou divulguées.

Sécurité

- Protéger tous les renseignements personnels dont l'entreprise a le contrôle contre la perte et le vol, et contre l'utilisation, la modification, la copie, la divulgation, la destruction et l'accès non autorisés (tant de l'intérieur que de l'extérieur de l'entreprise).

- Établir des mécanismes de sécurité appropriés, compte tenu du caractère délicat des renseignements personnels et de la nature des risques éventuels. Pour déterminer le caractère délicat des renseignements personnels, il faut tenir compte des préjudices possibles (p. ex., pertes financières, pertes d'avantages ou d'occasions, discrimination ou stigmatisation, embarras public) pour le particulier si les renseignements sont utilisés ou divulgués à mauvais escient.

- Mettre en oeuvre des procédures matérielles et techniques visant à protéger les renseignements personnels contenus dans le site Web de l'entreprise et les systèmes informatiques connexes.

- Élaborer des politiques et des pratiques qui limitent l'accès des employés (y compris du personnel informatique) aux renseignements personnels pour des raisons non compatibles avec les affaires de l'entreprise. Prévoir des sanctions disciplinaires appropriées en cas d'inobservation.

- Informer les particuliers des mesures de sécurité qui seront prises pour protéger les renseignements personnels les concernant. Inclure un plan de ces mesures dans les politiques de l'entreprise en matière de protection de la vie privée.

- Informer les particuliers des dispositions qu'ils devraient prendre pour faire des transactions en ligne en toute sécurité.

- Établir les procédures d'accès et de contrôle, les pistes de vérification et les contrôles de l'intégrité des documents appropriés.

- Prendre toutes les mesures nécessaires pour que les communications ou les transactions faites par l'entremise du site Web de l'entreprise ne donnent pas lieu à un accès non autorisé aux ordinateurs des particuliers ou aux renseignements personnels les concernant ni à une modification ou une destruction non autorisées de leurs données.

- Établir des procédures d'élimination pour faire en sorte que les renseignements personnels ne puissent pas être reconstitués après avoir été détruits et que le particulier ne puisse être identifié et lié à ces données d'aucune façon.

- Tenir un registre de destruction documentant comment et quand les renseignements personnels ont été détruits et les autorisations obtenues à cette fin.

- Prendre toutes les mesures raisonnables pour faire en sorte que les tiers engagés dans une transaction (p. ex., des entités qui louent des données ou celles à qui l'entreprise sous-traite le traitement ou l'exploration des données) disposent de mesures de sécurité.

Droit d'accès et de rectification

- Concevoir les systèmes et les pratiques de gestion des renseignements de manière à permettre aux particuliers d'exercer facilement leur droit d'accéder aux renseignements personnels les concernant dont l'entreprise a le contrôle et de contester l'exactitude et l'exhaustivité de ces renseignements.

- Informer les particuliers qu'ils ont le droit d'accéder aux renseignements personnels les concernant et de les rectifier, et expliquer la marche à suivre à cette fin.

- Établir un mécanisme en ligne simple, clair et sûr permettant aux particuliers de voir :

    - quels renseignements personnels les concernant l'entreprise a en sa possession, en ligne et hors ligne;

    - à quelles fins ces renseignements personnels sont recueillis, utilisés et divulgués;

- à qui ces renseignements personnels ont été divulgués;
- le coût total d'accès (les coûts devraient être raisonnables et justifiables);
- les sources des renseignements personnels (dans la mesure du possible);
- les coordonnées de la personne responsable de ces renseignements.

• Fournir aux particuliers un mécanisme en ligne simple, clair et sûr leur permettant :

- d'accéder aux renseignements personnels les concernant, sur demande;
- d'examiner et de rectifier ces renseignements, au besoin.

• S'assurer que l'accès est accordé aux particuliers d'une manière compréhensible et sans retard indu ou coût exorbitant (p. ex., sans frais ou à un coût minimal), dans toute la mesure du possible.

• Établir des critères clairs et circonscrits pour refuser l'accès aux renseignements personnels ou leur rectification, et les inclure dans les politiques de l'entreprise en matière de protection de la vie privée.

• Vérifier l'identité des particuliers avant de leur accorder l'accès aux renseignements personnels ou la rectification de ceux-ci.

• Rectifier ou détruire dès que possible les renseignements personnels inexacts, incomplets, non pertinents ou inappropriés.

• Si leur demande d'accès aux renseignements personnels les concernant ou de rectification de ces renseignements est refusée, fournir aux particuliers :

- les motifs de cette décision, en temps opportun et d'une manière compréhensible;
- l'occasion de préparer une « déclaration de désaccord » à annexer ou lier, avec les motifs du refus, aux données en question si leur contestation n'est pas réglée;
- la possibilité de clarifier leur demande;
- une occasion équitable de contester la décision.

• Prendre toutes les mesures nécessaires pour informer les tiers qui ont eu accès à des renseignements personnels au cours de l'année écoulée, ou qui les ont utilisés, des rectifications apportées ou des contestations non réglées. Si possible, leur remettre un double des renseignements rectifiés ou du dossier de contestation non réglé.

Plaintes et résolution des différends

- Élaborer des procédures de gestion des plaintes, d'enquête et de réponse aux questions concernant tous les aspects de l'observation des politiques et pratiques de l'entreprise en matière de protection de la vie privée. Permettre le plus possible d'interactions sécurisées en ligne.

- Veiller à ce que les processus de gestion des plaintes et de règlement des différends soient efficaces, justes, impartiaux, confidentiels, compréhensibles, faciles à utiliser et opportuns. Ces processus devraient être économiques pour toutes les parties en cause dans toute la mesure du possible.

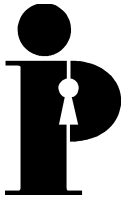
- Donner suite aux plaintes et apporter les correctifs qui s'imposent dans les plus brefs délais.

- Veiller à ce que le processus de gestion des demandes de renseignements et des plaintes de l'entreprise, y compris leur réception et les procédures de réponse, ainsi que les recours mis à la disposition des particuliers, soient très bien décrits et faciles à trouver dans le site Web.

- Ne pas imposer de frais aux particuliers qui veulent exercer leur droit de contester un refus d'accorder l'accès.

- Informer les particuliers des procédures d'enquête et de règlement des différends de tierces parties dont ils peuvent se prévaloir.

- Diriger les particuliers vers les autorités compétentes (p. ex., commissaire à la protection de la vie privée ou des données, association de l'industrie, programme de délivrance de labels de qualité) s'il est impossible de régler la plainte à la satisfaction du particulier. De même, recourir à titre facultatif à des mécanismes de règlement des différends par tierce partie. Ces processus doivent être accessibles, abordables, équitables et impartiaux pour toutes les parties.



Commissaire à l'information et à la protection de la vie privée/Ontario

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
M4W 1A8

416-326-3333
1-800-387-0073
Télécopieur : 416-325-9195
ATS (Téléimprimeur) : 416-325-7539
Site Web : www.ipc.on.ca