Guide sur la politique de la protection des renseignements personnels et des données électroniques de Groupe Cloutier Inc.

Annexe 16
Mars 2018

Groupe Cloutier
CABINET EN SERVICES FINANCIERS

Table des matières

1. Protection des renseignements personnels

Le commissaire à la protection de la vie privée du Canada est chargé de la surveillance de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE). Ces lois protègent les renseignements personnels qui ont été confiés aux institutions fédérales et aux organisations commerciales respectivement.

La LPRPDE vise la collecte, l'utilisation ou la communication de renseignements personnels dans le cadre d'une activité commerciale.

En vertu de la LPRPDE, on entend par renseignement personnel tout renseignement factuel ou subjectif, consigné ou non, concernant une personne identifiable. Il peut s'agir de tout type de renseignement, par exemple :

- l'âge, le nom, un numéro d'identification, le revenu, l'origine ethnique ou le groupe sanguin;
- une opinion, une évaluation, un commentaire, le statut social ou une mesure disciplinaire;
- le dossier d'un employé, un dossier de crédit ou de prêt, un dossier médical, etc

Les dix principes que les entreprises doivent respecter pour se conformer à la LPRPDE :

1. la responsabilité;
2. la détermination des fins de la collecte des renseignements;
3. le consentement;
4. la limitation de la collecte;
5. la limitation de l'utilisation, de la communication et de la conservation;
6. l'exactitude;
7. les mesures de sécurité;
8. la transparence;
9. l'accès aux renseignements personnels;
10. la possibilité de porter plainte à l'égard du non-respect des principes.

Les présentes dispositions régissent les activités de Groupe Cloutier Inc. et de ses compagnies affiliées.

Chez Groupe Cloutier Inc., nous connaissons l'importance que vous accordez à la protection de votre vie privée. C'est pour cette raison que nous nous sommes engagés à conduire nos affaires dans le respect des normes les plus strictes.

Par notre politique de protection des renseignements personnels, nous affirmons notre engagement à protéger l'information que nous possédons et à nous conformer aux lois qui encadrent la protection de la vie privée.

Nous recueillons des renseignements personnels conformément aux lois applicables et d'une manière fidèle à l'éthique, afin de pouvoir exercer nos activités. Nous ne recueillons que les renseignements nécessaires, directement ou indirectement, pour remplir ces fonctions.

Seuls les employés, mandataires et fournisseurs de services autorisés de Groupe Cloutier Inc. qui ont besoin de renseignements personnels vous concernant pour s'acquitter de leurs fonctions peuvent avoir accès à ces renseignements.

Nous avons mis en place et continuons d'élaborer des dispositifs propres à assurer la protection des renseignements contre les risques de vol, de perte, de communication non autorisée. Nous appliquons des dispositifs de protection correspondants au type de document, des mesures de type organisationnel comme la limitation de l'accès aux renseignements aux personnes qui en ont besoin pour s'acquitter de leurs fonctions et des dispositifs technologiques tels les mots de passe et le chiffrement. Nous protégeons les renseignements personnels par des mécanismes de sécurité appropriés à leur nature, afin qu'aucune personne non autorisée n'y ait accès, ne les obtienne ni ne les utilise.

Nous devons vous informer, si vous en faites la demande par écrit, de l'existence de renseignements personnels qui vous concernent, de l'usage qui en est fait et s'ils ont été communiqués à des tiers, le cas échéant. Sous réserve de certaines exceptions, nous devons vous permettre de consulter ces renseignements conformément à la loi applicable.

Vous pouvez aussi contester l'exactitude et l'intégralité des renseignements et y faire apporter les corrections appropriées, s'il y a lieu.

Vous pouvez communiquer avec nous pour nous demander des renseignements ou déposer une plainte au sujet de nos politiques et pratiques en matière de protection des renseignements personnels. La demande doit être adressée par écrit au Responsable de la protection des renseignements personnels, et envoyée au 1720, rue Sidbec-Sud, Trois-Rivières (Qc), G8Z 4H1.

2. Protection des données électroniques

Le système de «back office» de Groupe Cloutier Inc. nommé MAESTRO, est un système maison accessible seulement via notre réseau local. Notre réseau local est protégé par code d'usager et mot de passe. Les mots de passe doivent être modifiés aux 90 jours. L'accès à notre système maison est géré par code d'usager et mot de passe en plus d'une gestion par type d'usager et par niveaux d'accès.

Le courtier a accès à un outil qu'on appelle La boite à outil (BAO) via lequel il vient lire les informations pertinentes à sa clientèle. Par exemple, le suivi des nouvelles affaires, la clientèle en vigueur, les fonds distincts et les commissions. Cet accès est géré par code d'usager et mot de passe. Le mot de passe pouvant être modifié par l'usager via son accès au besoin.

L'ensemble de notre réseau est protégé via des outils de routage d'où une protection accrue de nos bases de données qui ne sont pas visibles via l'internet. Seuls les ports requis sont disponibles.

Notre site est protégé par un certificat SSL. Toutes les données qui se transigent entre les différents centres financiers (CF) se font au travers de tunnels sécurisés et encryptés.

Nos données les plus sensibles sont répliquées sur différents serveurs logés dans nos bureaux. Nous avons également une copie de sécurité prise sur une base quotidienne et gardée sous clé à l'extérieur de notre siège social.

On ne prend aucune photocopie de dossiers sauf dans certaines exceptions. Ces documents sont alors numérisés et attachés à la fiche de la police et accessibles seulement via notre application Maestro. Ces documents sont supprimés de nos serveurs à l'intérieur d'un délai de 12 mois, sauf exceptions à des fins de validation de dossiers.

Si vous avez des questions sur la protection des données électroniques, vous pouvez contactez le Service de la technologie et de l'informatique au 1-819-373-1345.

3. Procédure en cas de manquement

Pour protéger sa réputation, celle des conseillers, des compagnies, des Autorités et les intérêts du public, Groupe Cloutier Inc. prendra les mesures appropriées en cas de violation de la politique de la protection des renseignements personnels et des données électroniques. Elle pourra notamment produire un rapport aux organismes de l'industrie et/ou de réglementation et faire rapport aux compagnies concernées.

4. Processus de signalement

En cas de manquement à l'obligation de confidentialité, le formulaire de signalement suivant sera utilisé, et transmis sans délai au responsable de la protection des renseignements personnels:

Date du signalement	
Nom et coordonnées de la personne qui signale l'incident	
Emplacement et date de l'incident	
Description de l'incident	

Cause (si connue)	
Personne touchée par l'incident (client, employé, conseiller, assureur, autre, ...)	
Type d'information personnelle concernée (nom, adresse, NAS, informations financière, médicale, …)	
Description des actions prises pour circonscrire le manquement (récupération de l'information, arrêt du système informatique, remplacement de serrure, …)	
Date où le responsable de la protection des renseignements personnels a été avisé	
Commentaires additionnels	

5. Conservation et destruction des documents

La gestion des documents a pour objectif de créer et conserver des documents authentiques, fiables et utilisables, sous différents supports (papier, électronique) afin qu'ils servent aux activités commerciales de l'organisation. Les documents doivent être conservés tant qu'ils sont nécessaires pour que l'organisation s'acquitte de ses obligations sur les plans juridique, administratif, opérationnel et réglementaire.

Les documents imprimés à être conservés (tel que les ententes financières, contrats, …) doivent être entreposés sous clé, avec un accès restreint. Les documents électroniques (tels que courriels, documents numérisés, …) sont enregistrés et sauvegardés sur support informatique local sécurisé, avec des accès contrôlés. Les documents physiques à être détruits sont déposés dans des boîtes à accès contrôlés et déchiquetés sur place par une firme externe professionnelle.

6. Loi canadienne anti-pourriel

Entrée en vigueur le 1er juillet 2014, la Loi canadienne anti-pourriel dicte les exigences qui doivent être respectées dans les activités commerciales relativement à l'envoi de messages électroniques commerciaux à des gens à l'extérieur de l'organisation.

Un message électronique commercial est un courriel, message texte ou un message envoyé via un réseau social dans le but de faire de la prospection, du recrutement, du réseautage ou de la commercialisation d'un produit ou d'un service.

L'objectif de cette Loi est de diminuer le nombre de communications électroniques non-sollicitées.

Ainsi, un message électronique commercial doit être préalablement accepté par son destinataire (consentement), l'expéditeur doit être clairement identifié (identification) et une option de désabonnement doit être disponible (mécanisme d'exclusion). Il faut également tenir à jour un registre de consentement et de désabonnement.

Consentement : tacite si la relation d'affaires est existante, si un client vous remet une carte d'affaires sur laquelle figure son adresse courriel ou si son adresse courriel est disponible sur un site web. Le consentement est exprès s'il est obtenu verbalement ou par écrit (papier ou support électronique). Toutefois, le consentement ne s'applique pas au premier message électronique commercial envoyé (exemple ; premier contact avec un client recommandé).

Identification : chaque message doit clairement identifier l'expéditeur (nom, adresse postale, numéro de téléphone / adresse courriel / adresse de site web)

Mécanisme d'exclusion : option de désabonnement qui permet au destinataire de vous aviser qu'il ne désire plus recevoir vos messages électroniques commerciaux. Par exemple vous pouvez ajouter la note suivante dans votre signature courriel : « Si vous ne désirez plus recevoir ces messages, veuillez répondre au présent message en indiquant *Désabonnement* dans le champ *Objet* ». Le mécanisme d'exclusion doit apparaître sur tous vos messages, même si vous avez déjà obtenu l'accord du destinataire.

Tenir un registre : conserver un registre des consentements (tacites et verbaux) et des demandes d'exclusion.

7. FATCA – Foreign account tax compliance act

Cette législation, entrée en vigueur le 1er juillet 2014, exige que les renseignements sur les comptes financiers détenus au Canada par des personnes des États-Unis soient déclarés. À

ce sujet, Groupe Cloutier utilise les documents des assureurs, lesquels prévoient cette déclaration.