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

Annexe 16
Juillet 2020

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. 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.

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 lorsqu'ils ne sont plus nécessaires, 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 d'atteinte à la protection des renseignements personnels

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.

Atteinte à la protection des renseignements personnels
Une atteinte à la protection des renseignements personnels survient lorsqu'il y a accès non autorisé à des renseignements personnels ou collecte, utilisation ou communication non autorisée de tels renseignements. Ces activités sont « non autorisées » lorsqu'elles contreviennent aux lois applicables en matière de protection des renseignements personnels, telles que la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), ou aux lois provinciales similaires en matière de protection des renseignements personnels. Certaines des atteintes les plus courantes à la protection des renseignements personnels surviennent lorsque les renseignements personnels d'un consommateur, d'un patient, d'un client, ou d'un employé sont volés, perdus ou distribués par erreur (p. ex., le vol d'un ordinateur contenant des renseignements personnels ou l'envoi par erreur d'un courriel contenant des renseignements personnels à la mauvaise personne). Une atteinte peut également être la conséquence d'une procédure déficiente ou d'une défaillance opérationnelle.

Quatre principales étapes à suivre en cas d'atteinte
Il existe quatre principales étapes à suivre en cas d'atteinte à la protection des renseignements personnels :

1) limitation de l'atteinte et évaluation préliminaire
2) évaluation des risques associés à l'atteinte

3) notification à l'intention des personnes concernées
4) prévention

Les trois premières étapes doivent être réalisées le plus tôt possible après l'atteinte. Les quatre étapes fournissent des recommandations pour des solutions à plus long terme et des stratégies de prévention.

Étape 1 : Limitation de l'atteinte et évaluation préliminaire
Le Responsable de la protection des renseignements personnels doit être avisé immédiatement après la découverte d'une brèche qui a eu lieu ou qui est en train de se produire. Il pourra ainsi agir rapidement afin de la limiter. Voici des mesures qui pourraient être nécessaires de prendre après la découverte de l'atteinte :

- Limiter immédiatement l'atteinte (mettre fin à la pratique non autorisée, récupérer les dossiers, éteindre le système concerné par l'atteinte, révoquer ou changer les codes d'accès de l'ordinateur ou corriger les lacunes des systèmes de sécurité matériels ou électroniques).
- Désigner une personne qualifiée pour mener l'enquête initiale. Cette personne devrait avoir la marge de manœuvre voulue au sein de l'organisation pour mener l'enquête initiale et formuler des recommandations. Une enquête plus minutieuse pourrait être réalisée plus tard, au besoin.
- Déterminer s'il est nécessaire de mettre sur pied une équipe qui pourrait mettre à contribution des représentants des secteurs concernés de l'entreprise.
- Déterminer qui doit être avisé de l'incident à l'interne et, éventuellement, à l'externe. Transmettre le dossier aux supérieurs, au besoin, y compris au Responsable de la protection des renseignements personnels de votre organisation.
- Aviser la police si l'atteinte implique le vol ou une autre activité criminelle.

Étape 2 : Évaluation des risques associés à l'atteinte
Le Responsable de la protection des renseignements personnels doit évaluer les risques associés à l'atteinte afin de déterminer toute autre mesure à prendre immédiatement. Les facteurs pour évaluer le niveau de risque associé à l'atteinte comprennent :

1. Renseignements personnels en cause
   - Quels éléments de données ont été touchés par l'atteinte?
   - Dans quelle mesure les renseignements sont-ils sensibles? En règle générale, plus les renseignements sont sensibles, plus le risque de préjudice pour les personnes est élevé. Certains renseignements personnels sont plus sensibles que d'autres (les renseignements médicaux, les pièces d'identité émises par le gouvernement, comme les numéros d'assurance sociale [NAS], de permis de conduire et de carte d'assurance-maladie, ainsi que les numéros de comptes financiers, comme les numéros de cartes de crédit ou de débit, lesquels peuvent servir au vol d'identité). La combinaison de renseignements personnels est généralement plus sensible qu'un renseignement personnel seul. Toutefois, la sensibilité n'est pas le seul critère dont il faut tenir compte pour évaluer le risque, les préjudices prévisibles pour la personne étant tout aussi importants. Dans quel contexte les

renseignements personnels compromis s'inscrivent-ils? Une liste de clients sur la route d'un camelot, par exemple, peut ne pas être sensible. Par contre, les mêmes renseignements au sujet de clients qui ont demandé une interruption de service pendant qu'ils sont en vacances peuvent être plus sensibles. De même, les renseignements accessibles par le public tels que ceux que l'on retrouve dans un bottin téléphonique peuvent être moins sensibles. Les renseignements personnels sont-ils convenablement encodés, dépersonnalisés ou difficiles d'accès?

- Comment les renseignements personnels peuvent-ils être utilisés? Peuvent-ils servir à des fins frauduleuses ou autrement préjudiciables? La combinaison de certains types de renseignements personnels sensibles accompagnés du nom, de l'adresse et de la date de naissance de la personne concernée peut représenter un niveau de risque supérieur, compte tenu de la possibilité de vol d'identité.

Une évaluation du type de renseignements personnels en cause aidera à déterminer les mesures à prendre et la manière dont les personnes touchées, le cas échéant, ainsi que le Commissariat à la protection de la vie privée approprié devraient être informés.

2. Cause et étendue de l'atteinte
   - Dans la mesure du possible, il faut déterminer la cause de l'atteinte.
   - Y a-t-il un risque que l'atteinte se poursuive ou que les renseignements soient davantage compromis?
   - Quelle a été l'étendue de l'accès non autorisé aux renseignements personnels ou de la collecte, de l'utilisation ou de la communication non autorisée de tels renseignements, y compris le nombre et la nature des destinataires probables? Quel est le risque que cet accès, cette utilisation ou cette divulgation se poursuive, y compris dans les médias de masse ou en ligne?
   - Les renseignements ont-ils été perdus ou volés? S'ils ont été volés, peut-on déterminer s'ils étaient la cible du vol?
   - L'organisation a-t-elle récupéré les renseignements personnels?
   - Quelles sont les mesures prises pour atténuer les préjudices?
   - S'agit-il d'un problème systémique ou d'un incident isolé?

3. Personnes concernées par l'atteinte
   - Combien de personnes sont concernées par l'atteinte?
   - Qui est touché par l'atteinte (employés, entrepreneurs, public, clients, fournisseurs de services, autres organisations)?

4. Préjudices prévisibles découlant de l'atteinte
   - Au moment d'évaluer la possibilité de préjudices prévisibles découlant de l'atteinte, quelles sont les attentes raisonnables des personnes concernées? Par exemple, plusieurs personnes considéreraient que la liste des abonnés à un magazine spécialisé est plus préjudiciable que la liste des abonnés à un journal national.
   - Qui est le destinataire des renseignements? Y a-t-il un lien entre les destinataires non autorisés et le sujet des données? Par exemple, les renseignements ont-ils été communiqués à une personne inconnue ou soupçonnée d'être mêlée à des activités criminelles, ce qui laisserait présager une utilisation inappropriée des

renseignements personnels? Ou le destinataire est-il une entité ou une personne connue, digne de confiance et susceptible, selon toute vraisemblance, de rendre les renseignements sans les communiquer ou les utiliser?

- Quels préjudices l'atteinte pourrait-elle causer aux personnes concernées? Par exemple :
  - risque pour la sécurité (physique)
  - vol d'identité
  - perte financière
  - perte commerciale ou perte de possibilités d'emploi
  - humiliation, atteinte à la réputation ou détérioration des relations.
- Quels préjudices l'atteinte pourrait-elle causer aux organisations concernées? Par exemple :
  - perte de confiance en l'organisation
  - perte d'actifs
  - risque financier
  - poursuite judiciaire
- Quels préjudices l'avis concernant une brèche pourrait-il causer au public? Par exemple :
  - risque pour la santé publique
  - risque pour la sécurité publique

Étape 3 : Notification à l'intention des personnes concernées

En vertu de la LPRPDE, les organisations doivent aviser les personnes concernées si une brèche dans la protection de leurs renseignements personnels présente un risque réel de préjudice grave. Le risque réel de préjudice grave doit être déterminé en fonction de la nature délicate des renseignements personnels en cause et de la probabilité que ces renseignements aient été/soient utilisés à tort. Les préjudices graves incluent le vol d'identité, les pertes financières, l'incidence négative sur la cote ou le dossier de crédit, la perte d'occasions d'emploi, d'affaires ou de relations professionnelles, l'atteinte à la réputation ou aux relations, l'humiliation, la perte d'une propriété, les dommages à une propriété et les préjudices physiques. Après l'évaluation des risques d'une situation, le Responsable de la protection des renseignements personnels déterminera quel type d'avis pourrait être nécessaire.

<u>Quand, comment et qui devrait informer</u>

À cette étape, le Responsable de la protection des renseignements personnels doit avoir terminé l'évaluation des risques afin de déterminer si les personnes concernées doivent être avisées.

Quand informer : Les personnes concernées devraient être informées le plus rapidement possible après l'évaluation de l'atteinte. Toutefois, lorsque les autorités chargées d'appliquer la loi participent au processus, l'organisation doit vérifier avec celles-ci si elle doit reporter l'envoi de l'avis afin d'éviter de compromettre l'enquête.

Comment informer : Les organisations ne doivent utiliser la notification indirecte, soit au moyen de sites Web, d'avis publics, de médias, que si la notification directe est susceptible de causer davantage de préjudices, que les coûts afférents sont excessifs ou que les coordonnées actuelles des personnes concernées sont inconnues. Dans certains cas, il pourrait être plus approprié d'utiliser plusieurs méthodes de notifications. Il faut également déterminer si une méthode de notification pourrait augmenter le risque de préjudices (en alertant la personne qui a volé l'ordinateur portable de la valeur des renseignements contenus dans celui-ci).

Qui devrait informer : Généralement, la personne dans l'organisation qui a un lien direct avec le consommateur, le client ou l'employé devrait informer les personnes concernées, y compris lorsqu'un tiers fournisseur chargé de conserver et de traiter les renseignements personnels est à l'origine de l'atteinte. Cependant, dans certains cas, il pourrait être plus approprié que le tiers informe les personnes concernées. Par exemple, si un marchand est responsable d'une brèche concernant les renseignements d'une carte de crédit, l'émetteur de la carte pourrait être appelé à aviser la personne concernée puisque le marchand pourrait ne pas avoir ses coordonnées.

Contenu de la notification : Le contenu des notifications varie selon l'atteinte et la méthode de notification choisie. La notification doit contenir les renseignements nécessaires pour que la personne comprenne quels sont les risques qu'une brèche pourrait présenter et les mesures à prendre pour limiter l'incidence de préjudice. Elle doit comprendre les renseignements suivants :

- la date ou la durée de l'atteinte
- une description de l'atteinte
- une description des renseignements personnels ayant fait l'objet de l'atteinte
- une description des mesures prises pour réduire le risque de préjudice que cette brèche pourrait causer
- une description des mesures que les personnes concernées peuvent prendre afin d'éviter ou diminuer les risques de préjudice causés par l'atteinte ou limiter l'incidence de préjudice
- les coordonnées d'un représentant de l'organisation avec qui les personnes concernées peuvent communiquer afin d'obtenir des réponses à leurs questions et plus de renseignements
- le fait que les personnes concernées par l'atteinte ont le droit de porter plainte auprès du Commissariat à la protection de la vie privée ainsi que les coordonnées du Commissariat à la protection de la vie privée

Informer les tiers

Selon la nature de l'atteinte, il pourrait être nécessaire d'informer des personnes autres que celles dont les renseignements personnels ont été compromis pourraient avoir à être informées, notamment la police, les assureurs, les fournisseurs de technologie, les professionnels, les organismes de règlementation, les compagnies de carte de crédit, les institutions financières, les agences d'évaluation de crédit ou le Commissariat à la protection de la vie privée. Il pourrait également être prudent d'aviser les organisations ou les institutions

gouvernementales qui pourraient être en mesure de limiter l'incidence de préjudice causée par l'atteinte.

Le Responsable de la protection des renseignements personnels doit informer le Commissariat à la protection de la vie privée en utilisant le *Formulaire : Rapport d'atteinte à la LPRPDE* si l'atteinte présente un risque réel de préjudice grave.

Étape 4 : Prévention
Lorsque les mesures immédiates ont été prises pour réduire le risque associé à l'atteinte, le Responsable de la protection des renseignements personnels doit enquêter sur les causes de celle-ci et déterminer si la création d'un plan de prévention est nécessaire.

Le niveau d'effort doit refléter l'importance de l'atteinte et le fait qu'il s'agit d'un problème systémique ou d'un cas isolé. Ce plan doit comprendre les éléments suivants :

- une vérification de la sécurité physique et de la sécurité technique
- un examen des politiques et des procédures ainsi que tout changement nécessaire afin d'intégrer les leçons tirées de l'enquête (politiques de sécurité, de conservation des dossiers, de collecte, etc.), les politiques et les procédures devant également être revues régulièrement par la suite
- un examen des pratiques de formation de l'employé
- un examen des partenaires de distribution (courtiers, détaillants, etc.)

Le plan devrait prévoir une vérification à la fin du processus pour déterminer si le plan de prévention a été mis en œuvre avec succès.

Tenue de dossiers
Les organisations doivent conserver toutes les atteintes à la protection des renseignements personnels en dossier, même si elles ont déterminé qu'il n'y avait aucun risque de préjudice grave. Elles doivent les conserver au moins deux ans afin que le Commissariat à la protection de la vie privée puisse les examiner, sur demande.

Les dossiers doivent inclure, au minimum, les éléments suivants :

- la date ou durée estimée de l'atteinte
- une description des circonstances de l'atteinte
- la nature des renseignements en cause dans l'atteinte
- l'existence d'un rapport au Commissariat à la protection de la vie privée ou le nom des autres organisations avisées, s'il y a lieu
- une courte explication des raisons pour lesquelles l'organisation a déterminé qu'il n'y avait aucun risque de préjudice grave si l'atteinte n'a pas fait l'objet d'un rapport au Commissariat à la protection de la vie privée

Ressources
Vous trouverez des renseignements détaillés sur toutes vos obligations ayant trait à la protection des renseignements personnels au www.priv.gc.ca.

Vous devriez également vous familiariser avec le site Web du commissariat à la protection de la vie privée de votre province, s'il y en a un dans la province dans laquelle vous détenez un permis.

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.