Orchestro
ASSURANCES ET
RENTES COLLECTIVES

PROGRAMME DE CONFORMITÉ VISANT LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Révisé le : 15 février 2023

Orchestro
ASSURANCES ET RENTES COLLECTIVES

Table des matières

Section 1 – Nomination d'un agent de conformité

L'agent de conformité a la responsabilité :

- De mettre en œuvre, de surveiller, de mettre à jour et d'exécuter le programme de conformité, y compris :
  - Les politiques et les procédures
  - La formation et la sensibilisation
  - L'auto révision/autoévaluation du programme
- De superviser le processus en cas d'atteinte à la vie privée, et de traiter les demandes de renseignements et les plaintes des clients
- De faire état des nouveaux risques, des risques existants, des activités de surveillance et des changements d'ordre législatif ou réglementaire qui auront une incidence sur le programme de conformité aux décideurs principaux du cabinet, et ce, sur une base régulière

L'agent de conformité devrait avoir les pouvoirs et les ressources nécessaires pour s'acquitter efficacement de ses obligations. L'agent de conformité devrait occuper un poste de direction au sein du cabinet et ainsi être en mesure d'avoir un accès direct aux décideurs principaux. L'agent de conformité peut déléguer certaines fonctions à d'autres employés. Toutefois, la mise en œuvre du programme de conformité demeure la responsabilité de l'agent de conformité.

La personne ci-dessous a été nommée à titre d'agent de conformité :

NOM : Suzanne Fortin

TITRE : Agent de conformité

Suzanne Fortin le 1er janvier 2023
Agent de conformité

Suzanne Fortin le 1er janvier 2023
Présidente, Orchestro Assurances et Rentes Collectives

Orchestro
ASSURANCES ET
RENTES COLLECTIVES

Section 2 – Politiques et procédures

1. La protection des renseignements personnels et nos affaires

Les clients fournissent des renseignements personnels qui sont essentiels aux affaires du cabinet. Il est crucial de protéger ces renseignements afin de maintenir leur confiance. La loi du Québec pertinente, la *Loi sur la protection des renseignements personnels dans le secteur privé* régit la collecte, l'utilisation et la communication des renseignements personnels. Par « renseignements personnels », on entend toute donnée se rapportant à une personne identifiable, y compris les données médicales ou financières, de même que les données d'affaires si elles n'ont pas été classées dans la catégorie des « coordonnées d'affaires ». Cette catégorie comprend le titre professionnel, le numéro de téléphone et l'adresse courriel d'affaires de la personne, de même que les données qui sont utilisées dans le cadre de son emploi, de son entreprise ou de sa profession.

Le cabinet est responsable des renseignements personnels dont il a la gestion, et il lui incombe de prendre toutes les mesures nécessaires pour assurer la sécurité des renseignements personnels et confidentiels en sa possession. Dans certaines situations, cela signifie d'adopter de nouvelles pratiques commerciales afin de protéger la confidentialité des renseignements personnels.

Politique
Le cabinet met à la disposition du public l'information relative à ses politiques et à ses procédures, et il se conforme aux normes de confidentialité des compagnies (ci-après la « compagnie ») qu'il représente.

2. Préoccupations et demandes de renseignements ou requêtes générales

Procédure
Toutes les préoccupations, demandes de nature générale ou requêtes liées à la confidentialité et au cabinet sont transmises à l'agent de conformité du cabinet. Ce dernier examinera les demandes et en accusera réception dans les 24 heures; en son absence, les demandes seront transférées à une personne appropriée aux fins de traitement. Le client sera tenu au courant du progrès que réalise l'agent de conformité à l'égard de la situation, et la documentation complète de la préoccupation signalée et toutes les activités s'y rattachant seront conservées dans le dossier du client.

L'agent de conformité du cabinet fait suivre toutes les préoccupations, demandes de nature générale ou requêtes liées à la confidentialité et aux produits et services de la compagnie au chef de la conformité de cette compagnie.

2.1 Demandes de clients visant à accéder aux renseignements personnels

En vertu des lois relatives à la protection des renseignements personnels, les clients ont le droit d'accéder à leurs renseignements personnels consignés dans des dossiers tenus par le cabinet ou la compagnie et de contester leur exactitude, le cas échéant.

Procédure
Toute demande d'accès d'un client à ses renseignements personnels consignés dans les dossiers de client du cabinet est envoyée à l'agent de conformité du cabinet afin qu'il réponde à la demande du client dès que possible, et au plus tard 30 jours après la réception de la demande.

Corrigez ou modifiez tout renseignement personnel si son exactitude ou son intégralité sont remises en question et s'il s'avère que ce renseignement est effectivement erroné ou incomplet. Consignez au dossier tous les désaccords relatifs aux renseignements et, le cas échéant, informez-en les tierces parties.

Si un client demande d'accéder à ses renseignements personnels détenus par la compagnie, suivez les processus qu'a établis cette dernière.

2.2 Usage à mauvais escient des renseignements personnels

Procédure
L'agent de conformité du cabinet doit signaler sans délai tout usage à mauvais escient de renseignements personnels ou toute atteinte possible aux mesures de sécurité quant aux produits et aux services de la compagnie au chef de la conformité de la compagnie.

2.3 Processus visant les incidents en matière de confidentialité et les atteintes à la vie privée

Une atteinte à la vie privée survient lors de la perte ou de la divulgation non autorisée de renseignements personnels, ou de l'accès non autorisé à de tels renseignements découlant d'une atteinte aux mesures de sécurité. Une atteinte à la vie privée se produit également lorsque des renseignements personnels sont conservés d'une façon non conforme à la législation relative à la protection des renseignements personnels, comme lorsque des renseignements personnels sont conservés même s'ils ne sont plus nécessaires aux fins pour lesquelles ils ont été collectés.

Exemples d'atteinte à la vie privée :

- Des copies des relevés de renseignements personnels de client sont volées d'un véhicule.
- L'ordinateur portatif d'un conseiller est perdu ou volé et il comprend des renseignements personnels de clients.
- Le disque dur de l'ordinateur du conseiller comprenant des renseignements personnels sur des clients est compromis ou a été piraté.
- Les renseignements sur le client n'ont pas été envoyés au destinataire visé par le courriel, à l'interne ou à l'externe.
- Les renseignements sur le client ont été envoyés par la poste à la mauvaise adresse (une autre personne a ouvert le courrier).
- Des renseignements personnels ont été communiqués ou utilisés sans l'autorisation appropriée.
- Des renseignements sur les clients inactifs sont conservés plus longtemps qu'ils ne le devraient selon les calendriers de conservation.

Politique
Les atteintes présumées, les plaintes ou toutes les préoccupations reliées à un problème de confidentialité, peu importe qu'elles touchent une personne ou un fournisseur, sont immédiatement déclarées à l'agent de conformité du cabinet et à la compagnie. L'agent de

conformité du cabinet évaluera la situation, empêchera la divulgation des renseignements, corrigera la situation et contribuera à l'amélioration des mesures de contrôle afin d'éviter toute atteinte semblable à l'avenir.

Procédure

Mesures de confinement des atteintes

Perte, vol ou piratage d'appareils électroniques :

- Mobilisez l'équipe de soutien aux TI du cabinet
- Effectuez un balayage des ordinateurs afin de détecter tout logiciel malveillant avant d'accéder de nouveau aux systèmes.
- Communiquez immédiatement avec l'équipe de soutien technologique de la compagnie pour demander la modification des mots de passe.
- Communiquez avec le service de police pour déposer une plainte.
- Modifiez les mots de passe des autres systèmes (p. ex. service bancaire en ligne).

Perte ou vol de documents papier (p. ex. polices, propositions, dossiers clients) :

- Avisez l'agent de conformité du cabinet, le chef de la conformité de la compagnie, ainsi que le directeur général régional / directeur, Services aux entreprises du cabinet, s'il y en a un.
- Communiquez avec le service de police pour signaler le vol de documents.

Courriels envoyés au mauvais destinataire :

- Rappelez immédiatement le courriel.
- Si ce n'est pas possible, communiquez avec le mauvais destinataire pour lui demander de confirmer par écrit la suppression du courriel.
- Avisez l'agent de conformité du cabinet, le chef de la conformité de la compagnie, ainsi que le directeur général régional / directeur, Services aux entreprises du cabinet s'il y en a un.

Identification et évaluation des incidents en matière de confidentialité et des atteintes à la vie privée

A. Répondez aux questions suivantes :

a. Des renseignements personnels sont-ils touchés? Y a-t-il des preuves, est-il vraisemblable ou est-il impossible de déterminer que des renseignements personnels ont été touchés?
b. Les renseignements personnels ont-ils été divulgués ou transférés ailleurs sans autorisation? Toute divulgation non autorisée de renseignements personnels, qu'elle soit voulue, accidentelle ou à des fins criminelles, constitue une atteinte à la vie privée.
c. Les renseignements personnels ont-ils été collectés ou utilisés sans autorisation?

B. Si vous avez répondu « oui » aux questions ci-dessus, vous êtes en présence d'une atteinte à la vie privée.

C. **<u>Évaluez les risques en répondant aux questions suivantes :</u>**

a. Évaluation de la situation
   i. Quels sont le type, le degré de sensibilité et la quantité de renseignements personnels divulgués? (p. ex. : numéro de compte bancaire, NAS, renseignements médicaux, données sur les demandes de règlement)

ii. Qui a obtenu les données divulguées?
iii. Combien de personnes ont été touchées?
iv. L'information a-t-elle été récupérée en totalité?
v. Combien de temps s'est-il écoulé entre la découverte de l'incident et la mise en œuvre de mesures?
vi. Est-il possible de confirmer par écrit que les renseignements dupliqués n'ont pas été divulgués ni utilisés à mauvais escient?
vii. Les personnes touchées par l'incident pourraient-elles subir des préjudices par suite de l'incident (p. ex. : vol d'identité, fraude ou autre préjudice, y compris la douleur et la souffrance ou une atteinte à la réputation), ou n'y a-t-il aucun préjudice connu pour les personnes touchées?
viii. Quelle est la valeur potentielle des données sur le marché noir?
ix. L'incident découle-t-il d'une intention malicieuse? S'agissait-il d'une attaque ciblée? D'une erreur de manipulation? D'une erreur technique?
x. L'incident découle-t-il d'une situation problématique plus large? Un incident similaire s'est-il déjà produit?
xi. Les personnes touchées ont-elles été informées de l'incident?
xii. Les personnes touchées sont-elles vulnérables? (p. ex. : mineurs)
xiii. Peut-on s'attendre à ce que des plaintes ou des demandes de renseignements soient déposées auprès du commissaire à la protection de la vie privée? (Communication de l'incident au public)

b. Compte tenu du degré de sensibilité des renseignements et de la probabilité qu'ils soient utilisés à mauvais escient, déterminez si l'incident présente « un risque réel de préjudice grave » pour toute personne dont les renseignements ont été touchés (« personnes concernées »).
   i. Selon l'évaluation des risques menée à l'étape 3 a., y a-t-il un risque réel de préjudice grave?

2.4 Déclaration obligatoire des atteintes à la protection des renseignements personnels en vertu de la LPRPDE

Si le cabinet détermine que l'incident présente un risque réel de préjudice grave, elle doit en informer les personnes concernées et soumettre une déclaration au Commissariat à la protection de la vie privée du Canada (le « Commissariat ») et aux organismes de réglementation provinciaux applicables, et ce, dès que possible et même s'il n'y a qu'une seule personne concernée.

Le cabinet doit également informer de l'incident toute autre organisation ou entreprise qui pourrait atténuer le préjudice aux personnes concernées.

2.4.1 Avis aux personnes concernées

Voici l'information que doit fournir le cabinet aux personnes concernées, dans son avis sur l'atteinte aux mesures de protection des renseignements personnels :

A. une description des circonstances de l'atteinte;
B. la date à laquelle l'atteinte s'est produite ou la période sur laquelle elle s'est échelonnée, ou, si les dates précises sont inconnues, une approximation des dates;
C. une description des renseignements personnels touchés, dans la mesure où il est possible de le déterminer;

D. une description des mesures que l'entreprise a mises en place pour réduire les risques de préjudice découlant de l'atteinte;
E. une description des mesures que pourraient prendre les personnes concernées pour réduire les risques de préjudice découlant de l'atteinte ou atténuer ces préjudices; et
F. les coordonnées permettant aux personnes concernées de se renseigner davantage au sujet de l'atteinte.

2.4.2 Avis aux organismes de réglementation

- Envoyez un avis au Commissariat au moyen du formulaire *Rapport d'atteinte à la LPRPDE*.
- Colombie-Britannique – La loi recommande de faire rapport au Commissariat à la protection de la vie privée s'il y a un risque réel de préjudice grave. Pour savoir s'il vous faut produire un avis, reportez-vous au formulaire *Privacy Breach Checklist* (liste de vérification pour évaluer les atteintes à la vie privée) de la Colombie-Britannique.
- Alberta – *Office of the information and privacy commissioner of Alberta* (OIPC) (commissariat à l'information et à la protection de la vie privée de l'Alberta)
- Québec – Envoyez un avis à l'Autorité des marchés financiers (« AMF ») pour l'informer de toute atteinte à la protection des renseignements personnels qui pourrait nuire aux intérêts ou aux droits d'un consommateur ou à la réputation de l'entreprise.

2.5 Amélioration des mesures de contrôle

Passez en revue tous les processus, systèmes et programmes de formation, puis apportez-leur des améliorations au besoin afin d'éviter que les incidents ne se reproduisent.

2.6 Tenue de dossiers

Conservez des dossiers sur tous les incidents pendant 24 mois et fournissez-en une copie au Commissariat sur demande.

3. Obtenir l'autorisation valide et éclairée du client

L'autorisation est considérée comme valide uniquement s'il est raisonnable de s'attendre à ce que les personnes comprennent la nature, les fins et les conséquences de la collecte, de l'utilisation ou de la communication de leurs renseignements personnels auxquelles elles consentent.

Politique
Au début de la relation avec un client, le cabinet obtiendra son autorisation écrite pour la collecte, l'utilisation et la communication de ses renseignements personnels et l'avisera du stockage possible à l'extérieur du Canada.

Lors de la collecte de renseignements auprès de clients existants et potentiels, expliquez le but de la collecte de ces renseignements et fournissez des renseignements sur les politiques en matière de protection des renseignements personnels du cabinet.

Communiquez uniquement des renseignements personnels sur les clients à une autre personne ou société si une autorisation verbale ou écrite du client a été obtenue ou lorsque la loi vous y autorise ou vous y oblige. S'il s'agit de renseignements de nature délicate, vous devez obtenir une autorisation écrite.

Le cabinet recommandera les services d'autres professionnels ou conseillers aux clients s'ils en font la demande ou si les clients peuvent tirer avantage de tels services. Le cabinet ne fournit jamais le nom des clients ni d'autres renseignements les concernant à des tiers susceptibles d'utiliser ces renseignements en vue d'offrir leurs services, à moins que les clients en aient été informés et y aient consenti.

Procédure
Revoyez le formulaire intitulé *Engagement à l'égard de la protection des renseignements personnels et votre dossier client* avec le client et conservez la copie signée dans le dossier du client aux fins de référence future. Discutez de ce qui suit :

- Objectifs de la collecte de renseignements personnels
- Personnes ayant accès aux renseignements – accès des membres du personnel, des autres conseillers
- La discussion devrait couvrir les absences à court terme ou temporaires du cabinet, ainsi que les cas où le cabinet n'est pas en mesure d'offrir un service aux clients pendant une période prolongée et que l'aide d'un autre conseiller ou d'une nouvelle personne responsable du soutien administratif est nécessaire
- Utilisation des fournisseurs externes (p. ex. responsables du traitement de l'information, y compris les directeurs, Relations avec la clientèle et les services de stockage infonuagique)
- Probabilité que les renseignements seront stockés à l'extérieur du Canada et qu'ils seront alors assujettis aux lois applicables de ce pays, y compris les lois sur l'accès à l'information des autorités publiques
- Autorisation pour le partage de renseignements de conjoints; dossiers conjoints et accès à ces renseignements
- Possibilité que les personnes retirent leur consentement en tout temps

3.1 Nouveaux droits d'accès et nouvelles utilisations des renseignements du client

Politique
Le cabinet obtiendra l'autorisation écrite du client advenant tout changement de l'objectif ayant motivé la collecte, l'utilisation et la communication des renseignements personnels du client, ainsi que l'accès à ceux-ci.

Procédure
Passez en revue le nouvel objectif et les nouveaux droits d'accès, d'utilisation et de communication avec le client et conservez une copie de la nouvelle autorisation dans le dossier de client.

Si le client s'oppose à un transfert ou aux nouveaux droits d'accès, il peut :
Demander que ses renseignements ne soient pas communiqués
Demander de faire affaire avec un nouveau conseiller

Demander le nom d'autres conseillers qu'il peut joindre ou le nom et le numéro de téléphone du directeur général régional auquel il peut s'adresser pour demander un autre conseiller

3.1.1 Contrats avec les fournisseurs

Politique

Le cabinet exige l'autorisation du client avant de transférer les renseignements d'un client à un fournisseur et conserve le contrôle sur les renseignements lors du transfert de renseignements personnels à un fournisseur aux fins de traitement.

Les transferts de renseignements aux fournisseurs aux fins de traitement, y compris les services infonuagiques, sont effectués pour différentes raisons, notamment le stockage de données et le traitement ou la manipulation des renseignements personnels du client.

Procédure

Avant de conclure, de modifier substantiellement ou de renouveler une entente contractuelle avec un fournisseur, le cabinet évalue les mesures de protection afin de s'assurer que le fournisseur est en mesure de protéger les renseignements du client de façon appropriée.

Le cabinet effectuera une vérification auprès d'un conseiller juridique avant d'accepter les modalités du fournisseur et conservera une copie imprimée de l'entente pour ses dossiers.

Éléments à prendre en considération lors de l'évaluation :

Expérience d'affaires : Évaluer l'expérience et les compétences techniques du fournisseur pour mettre en œuvre les activités prévues et offrir un soutien à cet égard.

- Depuis combien de temps le fournisseur offre-t-il des services? Un nouveau fournisseur peut ne pas avoir un historique qui permet au cabinet de juger de ses processus et mesures en ce qui concerne la protection des renseignements.

Réputation : Évaluer depuis combien de temps le fournisseur offre des services et sa part de marché.

- Obtenir des références pour évaluer la réputation? Les références des utilisateurs actuels peuvent aider à évaluer la réputation du fournisseur.

Protection des renseignements :

- Quelle expérience le fournisseur a-t-il dans le traitement des renseignements personnels et financiers de nature délicate?
- Le fournisseur a-t-il une politique de confidentialité écrite en conformité avec la législation relative à la protection des renseignements personnels?
- Le fournisseur a-t-il une politique de sécurité matérielle ou une politique de sécurité de l'information écrite et à jour?
- Confirmez auprès du fournisseur que les données stockées ainsi que les données en transmission sont chiffrées.

Déclaration des incidents : Revoyez les programmes de déclaration et de gestion des incidents du fournisseur pour vous assurer qu'il détient des processus clairs et documentés pour l'identification, la déclaration, l'examen et la transmission aux échelons supérieurs des incidents. Assurez-vous que le processus de transmission à un échelon supérieur et de notification du fournisseur répond aux attentes du cabinet.

- Le fournisseur accepte-t-il d'aviser le cabinet dans un délai d'au plus 48 heures en cas d'atteinte à la sécurité des données pouvant toucher les renseignements des clients?
- Si une atteinte à la sécurité des données est soupçonnée, le fournisseur offre-t-il du soutien si une enquête est menée? Les registres d'accès sont-ils tenus à jour et fournis sur demande?

Planification des urgences :

- Le fournisseur possède-t-il des processus de sauvegarde et de récupération? Le cabinet pourra-t-il accéder à ses fichiers si le fournisseur connaît une interruption de service? Que se passera-t-il si le fournisseur perd les fichiers des clients? Le cabinet a-t-il une copie de sauvegarde?

Avis visant les renseignements à l'extérieur du pays :

- Le fournisseur stocke-t-il des données à l'extérieur du Canada? Des personnes de l'extérieur du Canada ont-elles accès aux données? Il est possible que des renseignements stockés dans d'autres pays ne soient pas protégés par des mesures comparables à celles du Canada et qu'ils ne soient pas conformes aux exigences en matière de protection des renseignements personnels. Tentez par tous les moyens d'avoir recours à un fournisseur qui stocke les renseignements au Canada; si ce n'est pas le cas, le cabinet avisera les clients que leurs renseignements seront stockés à l'extérieur du Canada.

Examinez attentivement le contrat de licence du fournisseur : Il s'agit d'un contrat; en cliquant sur « J'accepte » ou en téléchargeant tout logiciel, vous pourriez, par inadvertance, exposer les renseignements stockés dans le site à des risques excessifs si les mesures appropriées de protection des renseignements ne sont pas respectées.
Aucune autre tierce partie ne doit participer aux services, ni au partage de données, ni au groupage des données, ni avoir des droits d'accès en ce qui concerne les renseignements de nature délicate des clients, à moins que le contrat du fournisseur n'en fasse clairement mention.
Assurez-vous que le fournisseur :

- Limite l'utilisation des renseignements à l'objectif précisé pour respecter le contrat
- Limite l'accès aux données aux personnes qui en ont besoin pour respecter le contrat
- Limite la divulgation de renseignements à ce qui est autorisé par le cabinet ou à ce que la loi exige
- Transmette toute demande d'accès ou toute plainte liée aux renseignements au cabinet
- Retourne ou dispose des renseignements transférés dès la résiliation du contrat
- Effectue des déclarations quant au caractère adéquat de ses mesures de sécurité ou de contrôle des renseignements personnels et permette à votre organisation de vérifier la conformité du fournisseur relativement au contrat, si nécessaire

Comprenez :

- Comment résilier le contrat avec le fournisseur et vous assurer que les données sont éliminées ou retournées. Un fournisseur qui ne retire pas ou ne retourne pas les renseignements peut présenter un risque pour les renseignements du client et, par conséquent, pour le cabinet.
- Les limites de la responsabilité du fournisseur de service.

3.2 Exception visant les autorisations de transactions commerciales

Les transactions commerciales comprennent, par exemple, la vente d'un cabinet, une fusion de deux organisations ou plus ou toute autre entente prescrite entre deux organisations ou plus visant à mener une activité commerciale.

Politique
Lorsque nécessaire, le cabinet transfère des renseignements personnels afin de déterminer si une transaction doit être effectuée ou afin d'effectuer une transaction. Les renseignements doivent uniquement être utilisés ou communiqués aux fins relatives à la transaction, protégés de façon adéquate, retournés ou détruits lorsqu'ils ne sont plus nécessaires à cette fin, et les clients concernés doivent être avisés que leurs renseignements personnels ont été transférés à une autre organisation.

Procédure
Lors de la réception de renseignements personnels, le cabinet conclut une entente visant à utiliser ou à communiquer les renseignements uniquement dans le cadre de la transaction et à les protéger et à les retourner ou à les détruire si la transaction n'est pas effectuée. Si la transaction est effectuée, le cabinet avisera les clients concernés que leurs renseignements personnels ont été transférés à une autre organisation.

3.2.1 Conventions de rachat

Politique
Le cabinet utilisera, communiquera et protégera les renseignements du client pendant le processus d'évaluation et lors de la recherche d'un acheteur pour le bloc d'affaires ou au moment d'acheter un bloc d'affaires.

Procédure
Le cabinet limite l'identification des renseignements de client dans les documents partagés avec des tiers et communique avec des conseillers juridiques pour rédiger une entente de confidentialité appropriée qui doit être signée par les tiers visés par le processus d'évaluation du bloc d'affaires en vue d'un achat ou d'une vente possible.

3.2.2 Agent réalisateur – Changement

Politique
Dans le cas d'un changement d'agent réalisateur demandé par le client, le cabinet présume l'approbation de transfert d'accès aux renseignements et aux dossiers du client, le cas échéant, au nouveau conseiller.

4. Collecte de renseignements personnels

Politique
Lors de la collecte de renseignements personnels :

- Limitez la quantité et le type des renseignements recueillis au strict nécessaire pour la réalisation des fins visées.
- Faites tous les efforts raisonnables pour veiller à ce que les renseignements sur les clients existants et éventuels faisant partie des dossiers clients soient exacts et mis à jour ou corrigés au besoin.

- Prenez les mesures nécessaires afin de vous assurer que les renseignements recueillis sont utilisés aux fins déterminées et non à d'autres fins, et qu'ils ne sont pas communiqués à une tierce partie sans le consentement du client existant ou éventuel, sauf indication contraire dans la loi.

4.1 Enregistrement des entretiens téléphoniques avec les clients

Politique
Tout enregistrement des appels avec les clients implique la collecte de renseignements personnels. Par conséquent, l'appelant doit consentir à l'enregistrement.

Procédure
L'enregistrement ne peut avoir lieu qu'avec le consentement du client. Si l'appelant s'y refuse, fournissez-lui d'autres solutions sensées. S'il refuse toujours, cessez l'enregistrement de la conversation immédiatement et détruisez tout enregistrement existant.

- Enregistrez uniquement les appels à des fins précises.
- Le client doit être informé que la conversation est enregistrée dès le début de l'appel. Faites tout effort raisonnable pour vous assurer que le client est au courant des fins auxquelles servira l'enregistrement.
- Assurez-vous de respecter les lois sur la protection des renseignements personnels applicables.
- Si une copie du dossier du client est demandée, fournissez les enregistrements d'entretiens téléphoniques avec le client, ou leur transcription.

5. Utilisation, communication et conservation

Politique
Les renseignements personnels ne doivent pas, sans consentement, être utilisés ou communiqués à un tiers à des fins autres que celles auxquelles ils ont été recueillis, sauf si cette utilisation ou communication est requise ou permise par la loi.

Le cabinet ne conserve les renseignements personnels que pendant la période où ils sont nécessaires aux fins déterminées, ou comme requis ou permis par la loi, et est entièrement responsable de la garde en lieu sûr de ces documents et de la protection de la confidentialité de ceux-ci.

Les renseignements personnels qui ne sont plus nécessaires aux fins précisées au moment de la collecte sont détruits ou effacés de façon sécuritaire.

5.1 Destruction sécuritaire

Politique

- Les documents papier renfermant tout renseignement personnel concernant un client existant ou éventuel doivent être détruits par déchiquetage, et non recyclés.
- Les renseignements sont supprimés de tous les supports électroniques avant la destruction de ces derniers. Les dispositifs de stockage doivent être détruits afin de s'assurer que les données qu'ils contiennent ne peuvent pas être récupérées.

- Lors de l'élimination ou de la destruction des renseignements personnels, prenez les mesures appropriées pour empêcher les parties non autorisées d'accéder aux renseignements.
- Au moment de se défaire d'équipements ou d'appareils utilisés pour conserver des renseignements personnels (par exemple, des classeurs, des ordinateurs, des disquettes et des bandes sonores), prenez les mesures appropriées pour supprimer tous les renseignements consignés ou empêcher autrement des parties non autorisées d'y accéder.

5.2 Conservation des documents

Politique
Les dossiers sur les clients du cabinet doivent être conservés pendant au moins la durée minimale stipulée par la loi.

6. Mesures de protection

Politique
Les mesures de protection appropriées doivent être prises pour ce qui est du stockage et de l'élimination des renseignements sur les clients. Toutes les personnes liées au cabinet ou à son emploi sont tenues de respecter les procédures décrites dans cette section.

Procédure
Le cabinet utilise une combinaison de mesures de protection technologiques, physiques et organisationnelles pour protéger les renseignements personnels des clients contre le vol et la mauvaise utilisation, ainsi que contre l'accès, la communication, la reproduction, l'utilisation ou les modifications non autorisées.

6.1 Mesures de protection technologiques

Les outils technologiques nécessitant des mesures de protection comprennent entre autres :

- Les ordinateurs : ordinateurs de bureau, portables, serveurs et assistants personnels (tablettes et téléphones intelligents)
- Le matériel informatique et les logiciels
- Les appareils mobiles
- Les médias portables – clés USB, CD, DVD
- Les imprimantes, numériseurs, télécopieurs et photocopieurs avec options d'impression sécurisées
- Le courrier électronique et les services Internet (p. ex. l'infonuagique)

6.1.1 Chiffrement, antivirus et coupe-feu

Politique

- Les logiciels de chiffrement, les antivirus et les coupe-feux sont installés et tenus à jour sur tous les outils technologiques utilisés en contexte professionnel afin d'assurer la sécurité des données des clients. Cela comprend le chiffrement des données de nature délicate lorsqu'elles sont stockées ou transmises, y compris lors de leur transmission vers les serveurs de sauvegarde.

- Les mesures de protection de ces outils technologiques sont revues sur une base annuelle et mises à niveau lorsque nécessaire.
- Lorsque ces outils technologiques sont sans surveillance ou en cours de transport, tous les appareils doivent être fermés (éteints). Si vous ne faites que fermer votre session, verrouiller l'appareil ou le laisser en mode veille, les mesures de sécurité supplémentaires peuvent être inefficaces.

Précisions sur les programmes de sécurité

Mesures de protection	**Produit**	**Dernière mise à jour**
Chiffrement		
Antivirus ou protection contre les logiciels malveillants		
Coupe-feu		

6.1.2 Écrans de veille, nom d'utilisateur et mots de passe

Le chiffrement n'élimine pas la nécessité de créer un mot de passe difficile à décoder.

- Protégez les noms d'utilisateur et les mots de passe et ne les partagez pas.
- Choisissez des mots de passe difficiles à décoder (utilisez des majuscules, des minuscules, des chiffres et des symboles et un minimum de huit caractères).
    - Évitez les noms propres ou les mots communs répertoriés dans les dictionnaires (p. ex. assurance, mot de passe) et des renseignements personnels comme les noms de membres de la famille ou d'animaux, les dates d'anniversaire, les numéros d'identité émis par le gouvernement ou des mots ayant trait à des passe-temps et à des intérêts personnels.
- Protégez votre écran de veille à l'aide d'un mot de passe afin d'empêcher l'accès non autorisé à votre ordinateur.
- Lorsque vous vous absentez temporairement, utilisez la fonction « Verrouiller cet ordinateur ».

6.1.3 Courriel sécurisé

Protection à l'aide d'un mot de passe
Lorsque vous traitez des renseignements de nature délicate, les courriels comprenant ces renseignements doivent être sécurisés à l'aide d'un mot de passe de dossier/document ou, si possible, être chiffrés. Les mots de passe du dossier doivent être communiqués par téléphone.

Options de chiffrement pour l'envoi sécurisé de courriels ou de pièces jointes :

A. WinZip
B. Microsoft Office 2007 (Word, Excel et PowerPoint)
C. Microsoft Office Outlook 2007, avec l'utilisation de certificats numériques
D. Microsoft Office 2016 / Office 365

6.2 Mesures de protection physiques

Vous devez tenir compte des mesures de sécurité suivantes :

6.2.1 Aménagement du bureau

- Les bureaux ou les espaces de travail sont aménagés de manière qu'ils soient en retrait des aires de circulation du bureau.
- Les télécopieurs, les photocopieurs et les imprimantes sont placés dans les aires dont l'accès est plutôt restreint.
- Les associés ou les membres du personnel qui traitent les renseignements de nature délicate sont situés dans une aire de travail où les conversations ne peuvent pas être facilement entendues.
- Les dossiers de renseignements personnels des clients sont conservés à l'écart des aires de circulation.
- Les dossiers comprenant des renseignements personnels sont conservés dans des classeurs verrouillés.

6.2.2 Ordinateurs et appareils électroniques grand public

Peu importe où vous vous trouvez, que ce soit au bureau, à la maison, dans une chambre d'hôtel ou dans une salle de réunion, prenez toujours les dispositions nécessaires pour protéger votre ordinateur portable et vos appareils mobiles contre le vol en utilisant un dispositif antivol (p. ex. un câble de verrouillage).

- Gardez vos appareils sous clé en lieu sûr lorsque vous ne les utilisez pas.
- Pour prévenir le vol, évitez de laisser votre ordinateur portable dans votre véhicule. Si vous n'avez pas d'autre choix, placez-le dans le coffre ou dans un endroit à l'abri des regards.
- Fermez votre ordinateur portable et mettez-le hors tension – de cette façon, toutes les applications seront adéquatement fermées.
- Fermez toute session ouverte dans un site Web ou un programme quand vous n'avez plus à vous en servir. De plus, souvenez-vous de ne pas « enregistrer » vos renseignements de manière que la session s'ouvre automatiquement la fois suivante : si votre appareil mobile est perdu ou volé, une autre personne pourrait accéder à vos comptes ou dossiers.
- Rangez les ordinateurs et appareils électroniques grand public (et, le cas échéant, les ordinateurs des associés ou membres du personnel) en lieu sûr pendant toute période d'absence (soirées, fins de semaine, congé de maladie ou vacances) de sorte à éviter tout accès non autorisé aux données.

Protection des ordinateurs portatifs

Au bureau, pendant la journée – Les ordinateurs portatifs sont verrouillés à l'aide d'un câble de verrouillage et attachés solidement à un meuble fixe ou à un port d'attache sécurisé. La clé est conservée dans un lieu sûr éloigné de l'ordinateur portatif.

Au départ du bureau, à la fin de la journée de travail – Les ordinateurs portatifs sont rangés sous clé dans un classeur ou dans un tiroir; la clé est conservée dans un lieu sûr éloigné de l'ordinateur portatif.

Les règles relatives à la protection des ordinateurs portatifs s'appliquent également lorsque la porte du bureau est verrouillée.

Lors des déplacements :

- Faites preuve de prudence lorsque vous utilisez un point d'accès sans fil public puisque la connexion pourrait être interceptée. Évitez d'effectuer des transactions bancaires, de faire des achats en ligne ou d'accéder à des ressources du cabinet à partir de telles connexions. Il vaut mieux attendre d'avoir accès à un réseau auquel vous faites confiance avant d'effectuer des transactions délicates. Soyez sur vos gardes si vous utilisez votre appareil dans un pays étranger. L'interception des communications et l'analyse de trafic pourraient être plus répandues dans un réseau étranger. Lorsque vous travaillez, placez l'ordinateur portatif de façon à ce que l'utilisateur soit le seul à pouvoir voire les renseignements personnels qui paraissent à l'écran.
- Prenez note des numéros de série et de modèle de l'ordinateur portatif et conservez-les en lieu sûr.
- Transportez l'ordinateur portatif dans un sac discret. Utilisez un sac matelassé, comme un sac à dos, au lieu de la mallette ou du sac de transport réservé à cet effet, afin de transporter en toute sécurité l'ordinateur portatif sans attirer l'attention.
- Ne laissez pas d'ordinateur portatif à la vue dans une voiture; rangez-le dans le compartiment verrouillé de la voiture lorsque vous voyagez pour éviter les vols.
- Ne laissez jamais d'ordinateur portatif dans le coffre arrière de taxis ou de limousines étant donné que ceux-ci sont rarement verrouillés.
- N'enregistrez jamais d'ordinateur portatif dans les hôtels ou auprès des transporteurs aériens.
- À l'aéroport, après avoir placé un ordinateur portatif sur le transporteur à courroie du système de détection par rayons X, surveillez bien le sac et ne laissez personne vous dépasser.
- À la maison ou à l'hôtel, verrouillez l'ordinateur portatif comme il est d'usage de le faire au travail. Utilisez un câble de verrouillage et rangez l'ordinateur portatif hors de la vue.
- Les chambres d'hôtel qu'on ouvre avec une carte-clé permettent un bon suivi des personnes qui sont entrées dans la chambre et de l'heure de la visite. Les clés ordinaires peuvent être égarées ou reproduites. Si l'hôtel n'utilise pas de cartes d'accès, envisagez de ne pas laisser l'ordinateur portatif dans la chambre.

6.2.3 Bureaux et dossiers

- Les renseignements personnels de nature délicate ou d'autres documents confidentiels ne doivent jamais être laissés sans surveillance. Lorsque des renseignements personnels doivent être imprimés pour être traités activement, tous les dossiers et leur contenu devraient être disposés de manière à ne pas être à la vue de personnes qui n'ont pas l'autorisation de les lire.
- Tous les renseignements personnels de nature délicate doivent être conservés dans des pièces, des classeurs ou des tiroirs verrouillés et à accès restreint lorsqu'ils ne sont pas utilisés.

Garde des documents à l'extérieur des lieux de travail

Il faut assurer la protection des renseignements des clients, qu'ils se trouvent dans un bureau personnel, dans une voiture ou dans tout autre lieu. Les dossiers papier qui renferment des renseignements personnels doivent être retirés du lieu de travail uniquement lorsque cela s'avère absolument nécessaire ou pour assurer un service approprié aux clients.

Aux fins de suivi et pour faciliter les démarches en cas de perte ou de vol, il faut prendre note de tous les dossiers ou documents avant qu'ils ne soient retirés du lieu de travail. Tous les associés et les membres du personnel doivent prendre connaissance de ces exigences et s'y conformer.

6.3 Communication de renseignements confidentiels

- Ne discutez jamais des clients dans des endroits publics, comme les ascenseurs, les cafétérias ou les restaurants.
- Lors d'un échange ayant trait aux renseignements personnels sur un client ou un employé au moyen d'un téléphone cellulaire, prenez toutes les précautions possibles afin que la conversation ne soit pas entendue par des tiers.
- Lors de la consultation du dossier d'un client dans un moyen de transport en commun, comme le train, l'avion ou l'autobus, placez le document de sorte à empêcher qu'il puisse être lu par des tiers.

6.3.1 Boîte vocale

Les messages laissés aux clients ne doivent comporter aucun renseignement personnel à moins que le client en ait déjà été avisé. Le client doit aussi confirmer qu'il désire que ces renseignements lui soient laissés dans sa boîte vocale.

6.3.2 Identification de l'appelant

Si une demande est effectuée par téléphone, il est nécessaire d'identifier la personne avant de fournir quelque renseignement personnel que ce soit.

Pour identifier l'appelant, la personne doit répondre à trois des questions suivantes. Posez toujours les questions dans cet ordre.

- Nom complet du ou des propriétaires
- Si l'appelant téléphone au nom de la succession, il doit fournir le nom complet du propriétaire décédé.
- Si l'appelant est le propriétaire du contrat en fiducie, il faut s'assurer que son nom correspond au nom du fiduciaire qui a été entré dans le système.
- Si l'appelant est le mandataire, il doit fournir le nom du mandataire figurant au dossier ainsi que celui du propriétaire de la police
- Numéro de police
- Numéro d'appartement, numéro et rue, ville
- Date de naissance de la personne assurée / du rentier
- Nom complet de la personne assurée / du rentier

Si les réponses ne sont pas exactes, indiquez à l'appelant que le cabinet est responsable de la protection de la vie privée et de la confidentialité des renseignements personnels du client et qu'il ne peut, par conséquent, divulguer des renseignements sans d'abord confirmer que l'appelant a bien droit de les obtenir. Demandez-lui de présenter sa demande par écrit.

6.3.3 Courrier électronique

Les messages envoyés aux clients ne doivent comporter aucun renseignement personnel, à moins que le client en ait été avisé à l'avance et qu'il ait consenti à ce que ces renseignements lui soient transmis par courriel.

La mise en garde suivante doit être ajoutée à tout courriel renfermant des renseignements personnels sur le client :

« Le contenu de la présente communication, y compris tout fichier joint, est confidentiel et peut être privilégié. Si vous n'êtes pas le destinataire visé (ou si vous ne recevez pas la présente communication au nom du destinataire visé), veuillez en aviser immédiatement l'expéditeur et supprimer ou détruire la présente communication sans la lire, en tirer des copies, la retransmettre ou en enregistrer le contenu. Merci. À noter : Nous avons pris des mesures de protection contre les virus, mais nous n'assumons aucune responsabilité pour ce qui est de la perte ou des dommages causés par la présence d'un virus. »

Authentification de courriels

Les renseignements de nature délicate ne devraient pas être communiqués par courriel, sauf si le client en a fait la demande. Si une demande est effectuée par courriel, il est nécessaire d'identifier la personne avant de fournir des renseignements personnels par courriel.

- Confirmez par téléphone que votre client a demandé ces renseignements.
- Assurez-vous que le courriel est envoyé au destinataire approprié puisque les noms des listes d'adresses peuvent être semblables.
- Identifiez le client et obtenez et documentez son consentement aux communications par courriel.
- Chiffrez ou protégez les fichiers avec des mots de passe lorsque la communication de renseignements permettant d'identifier le client est demandée par courriel.

6.3.4 Télécopies

Les télécopies ne doivent pas comporter de renseignements personnels, à moins que le client en ait déjà été avisé et qu'il ait consenti à recevoir ces renseignements par télécopieur.

La mise en garde suivante doit être ajoutée au bordereau de toutes les télécopies comportant des renseignements personnels :

« Le contenu de la présente télécopie, y compris toute pièce jointe, est confidentiel et peut être privilégié. Si vous n'êtes pas le destinataire visé (ou si vous ne recevez pas la présente télécopie au nom du destinataire visé), veuillez en aviser immédiatement l'expéditeur et supprimer ou détruire la présente télécopie sans la lire, en tirer des copies, la retransmettre ou en enregistrer le contenu. Merci. »

Vérifiez le numéro de télécopieur avant d'envoyer des renseignements personnels :

- Veuillez porter une attention particulière aux divers indicatifs téléphoniques (1 866, 1 888, 1 800, etc.) et prenez le temps de vérifier l'exactitude du numéro de télécopieur avant d'appuyer sur Envoyer. Des renseignements personnels ou confidentiels peuvent aisément se retrouver dans les mauvaises mains si l'indicatif téléphonique est erroné.

- Afin de prévenir des erreurs, envisagez de programmer les numéros fréquemment utilisés dans le télécopieur.
- Confirmez de nouveau le numéro de télécopieur avant d'appuyer sur Envoyer.
- Une fois la télécopie envoyée, communiquez avec le destinataire pour qu'il confirme la réception du document.

6.4 Mesures de protection organisationnelles

6.4.1 Autorisation et limite d'accès uniquement en cas de nécessité

- L'accès aux renseignements personnels est accordé uniquement en cas de nécessité (c.-à-d. aux renseignements nécessaires pour accomplir certaines tâches). L'accès aux dossiers (papier, système ou électroniques) est revu lors de l'embauche d'associés ou de membres du personnel ou de leur transfert à un poste différent.
- Lorsqu'il est prévu qu'un associé ou membre du personnel quitte son emploi, il faut révoquer son accès aux renseignements sur les clients, y compris les données électroniques accessibles au moyen des ordinateurs et les renseignements consignés dans les documents se trouvant dans les aires de travail.

6.4.2 Ententes de confidentialité

Les employés sont avisés de l'importance de protéger la sécurité et la confidentialité des renseignements personnels. Lorsque des renseignements personnels sont de nature délicate ou que les conséquences possibles d'une communication non appropriée sont importantes, le cabinet :

- Utilise les ententes de confidentialité avec les employés
- Prend des mesures appropriées pour protéger les renseignements de client contre des tiers qui peuvent avoir accès aux bureaux, notamment les agents de sécurité, les préposés à l'entretien ménager et les fournisseurs
- Obtient, le cas échéant, une entente de non-divulgation de la personne ou de l'entreprise chargée de la réparation de l'appareil si les renseignements confidentiels ne peuvent pas être retirés d'un appareil avant sa réparation

7. Adoption des politiques et des procédures

Politiques et procédures adoptées et révisées le 1er janvier 2023 par *Suzanne Fortin*
Présidente, Orchestro assurances et rentes collectives

Section 3 – Programme de formation

Tous les conseillers et membres du personnel, permanents et temporaires, reçoivent une formation comme indiqué ci-après.

- La formation doit obligatoirement être suivie avant qu'un accès aux renseignements personnels soit accordé.
- La formation est un processus continu et des formations d'appoint doivent être suivies chaque année, ou plus fréquemment si nécessaire, relativement aux changements visant les lois, la technologie, les fournisseurs de service, les nouveaux accès aux renseignements personnels ou leurs nouvelles utilisations, etc.
- L'agent de conformité anime toutes les séances de formation et en fait le suivi dans le tableau ci-joint. La formation est effectuée par la diffusion et l'examen de la section des politiques et procédures du présent programme de conformité, qui sont revues dans le cadre du programme d'autorévision pour s'assurer que le matériel est exact et à jour.
- Un suivi est effectué afin de savoir si la formation a été effectuée et chaque conseiller et membre du personnel doit signer pour confirmer qu'il a bien suivi la formation. Les notes sur les formations terminées sont conservées dans cette section du programme de conformité.
- Une formation facultative ou supplémentaire peut comprendre des modules fournis par des assureurs, la diffusion de communications sur la confidentialité des assureurs et des mises à jour, des articles, des communications de l'industrie et des modules de formation, etc.
- Les employés qui ne sont pas en mesure de suivre une formation d'appoint aux dates prévues devront prendre d'autres arrangements afin de respecter cette exigence.

Suivi des formations terminées

Nom	**Type de formation et contenu (formation initiale, examen continu des politiques et procédures et des renseignements généraux, module fourni par l'assureur, etc.)**	**Date**	**Signature de l'employé**
Suzanne Fortin	*Formation initiale, examen continu des politiques et procédures et des renseignements généraux*	*12 janvier 2023*	

Section 4 – Autorévision

Date de la révision : le 1er janvier 2023

Révision effectuée par : Suzanne Fortin

Signature de la Présidente, Orchestro assurances et rentes collectives : *Suzanne Fortin*

Responsabilité	Oui	Non	Commentaires
Le cabinet a-t-il désigné une personne chargée de veiller à la conformité à la législation sur la protection des renseignements personnels et le nom de cette personne désignée est-il fourni au client à sa demande?	Oui		
Le cabinet a-t-il mis en œuvre des procédures pour protéger les renseignements personnels?	Oui		
Le cabinet a-t-il informé et formé le personnel au sujet des politiques et des pratiques relatives à la protection des renseignements personnels?	Oui		
Le cabinet comprend-il que la collecte de renseignements personnels doit se limiter aux renseignements personnels nécessaires aux fins déterminées?	Oui		
Le cabinet comprend-il que lorsqu'un tiers (par ex. un expert-conseil en informatique, un membre du personnel d'entretien, un comptable, etc.) a accès aux renseignements personnels, il doit recourir à des moyens contractuels ou autres pour assurer un niveau comparable de protection des renseignements personnels?	Oui		
Est-ce que le cabinet connaît et respecte les normes de confidentialité et les bonnes pratiques commerciales de la compagnie?	Oui		
Est-ce que le cabinet connaît et respecte les lignes directrices en matière de confidentialité et les pratiques commerciales solides des autres compagnies d'assurance qu'il représente?	Oui		
Le cabinet comprend-il le processus de plaintes et de requêtes de l'assureur relativement à la protection des renseignements personnels?	Oui		
Consentement	**Oui**	**Non**	**Commentaires**
Le cabinet comprend-il qu'il est responsable d'obtenir le consentement des clients pour la	Oui		

collecte, l'utilisation et la communication de leurs renseignements personnels?			
Le cabinet a-t-il instauré un processus régissant l'obtention du consentement des clients pour la collecte, l'utilisation et la communication de leurs renseignements personnels?	Oui		
Le cabinet fait-il en sorte que des mesures raisonnables sont prises pour dire aux clients comment leurs renseignements seront utilisés ou communiqués?	Oui		
Consentement	**Oui**	**Non**	**Commentaires**
Le client ou un représentant dûment autorisé (un tuteur légal ou le détenteur d'une procuration générale, p. ex.) a-t-il donné son consentement à la collecte de renseignements?	Oui		
Le cabinet a-t-il instauré un processus pour gérer le retrait du consentement (pour assurer le suivi et le respect des volontés des clients qui n'ont pas donné leur consentement, par exemple)?	Oui		
Limitation de la collecte	**Oui**	**Non**	**Commentaires**
Le cabinet limite la collecte aux renseignements nécessaires aux fins expliquées au client.	Oui		
La collecte des renseignements est effectuée par des moyens équitables et licites.	Oui		
Limitation de l'utilisation, de la communication et de la conservation	**Oui**	**Non**	**Commentaires**
Le cabinet comprend-il que si des renseignements personnels doivent servir à une fin autre que celle pour laquelle ils avaient été collectés, il faudra informer le client de cette nouvelle fin et obtenir son consentement?	Oui		
Le cabinet a-t-il des lignes directrices et des procédures relatives à la conservation des renseignements personnels?	Oui		
Le cabinet a-t-il pris des mesures pour s'assurer que des parties non autorisées n'aient pas accès aux renseignements personnels lors de leur disposition ou de leur destruction.	Oui		
Exactitude	**Oui**	**Non**	**Commentaires**

Le cabinet a-t-il mis en place des mesures pour s'assurer que les renseignements personnels qu'il collecte et utilise sont exacts, complets et à jour, dans la mesure de leur utilisation prévue?	Oui		
Mesures de protection	**Oui**	**Non**	**Commentaires**
Le cabinet a-t-il instauré des mesures de protection pour prévenir la perte ou le vol, de même que la consultation, la communication, la reproduction, l'utilisation ou la modification non autorisée des renseignements personnels?	Oui		
Le cabinet a-t-il recours à un niveau de protection accru pour les renseignements de nature délicate? Exemples : Mesures physiques (verrouiller les classeurs, limiter l'accès aux lieux, etc.) Mesures organisationnelles (autoriser l'accès seulement lorsque c'est nécessaire, par exemple) Mesures technologiques (utilisation de mots de passe et cryptage, par exemple)	Oui		
Le cabinet a informé les conseillers et le personnel de l'importance de préserver le caractère confidentiel des renseignements personnels.	Oui		

Transparence	**Oui**	**Non**	**Commentaires**
Les clients peuvent facilement obtenir des renseignements au sujet des politiques et pratiques du cabinet en matière de protection des renseignements confidentiels.	Oui		
Accès aux renseignements personnels	**Oui**	**Non**	**Commentaires**
Le cabinet comprend que les clients ont le droit de présenter une demande pour consulter les renseignements les concernant figurant dans ses dossiers.	Oui		
Le cabinet a instauré un processus à suivre lorsqu'un client souhaite consulter ses renseignements.	Oui		
Le cabinet comprend que les clients ont le droit de présenter une demande pour consulter les renseignements les concernant figurant dans les dossiers conservés par la compagnie.	Oui		
Le cabinet connaît le processus lorsqu'un client souhaite consulter les renseignements	Oui		

personnels le concernant figurant dans les dossiers de la compagnie.			

Mesures à prendre :
Aucune mesure à prendre

Section 5 – Révisions et modifications du programme de conformité en matière de protection des renseignements personnels

Ce programme a été adopté le 1er janvier 2017

Ce programme a été revu et modifié les, 1er juin 2017, 1er mars 2018, 1er août 2019, 1er février 2021, 1er janvier 2023, 15 février 2023

Voici un résumé de ces modifications : mises à jour
Historique de la révision du document

Date	Ce qui a changé	Raison du changement
1er février 2021	Changement de nom du Cabinet	Changement de nom du Cabinet
1er janvier 2023	Mise à jour	
15 fév. 2023		Loi 25 – chef de la protection des renseignements personnels

Orchestro
ASSURANCES ET RENTES COLLECTIVES

Section 6 – Procédure en cas d'atteinte à la protection des renseignements personnels

Chef de la protection des renseignements personnels : Suzanne Fortin

Le 15 février 2023

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 autorisé de tels renseignements. Ces activités sont « non autorisés » 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* (LDRPDE), 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 distribuées 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 défaillante 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 chef 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 (p. ex., 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 électronique).
- 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 chef de la protection des renseignements personnels de votre organisation.
- Aviser la police si l'atteinte implique le vol ou une autre activité criminelle.
- Ne pas nuire à la capaciter d'enquêter sur l'incident. Prendre garde de ne pas détruire des éléments de preuve qui pourraient servir à déterminer la cause de l'incident ou permettre de prendre les mesures correctives qui s'imposent.

Étape 2 : Évaluation des risques associés à l'atteinte

Le chef 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 associés 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 générales, plus les renseignements sont sensibles, plus le risque de préjudice pour les personnes est élevé. Certains renseignements personnels sont plus sensibles que d'autres (p. ex., les renseignements médicaux, les pièces d'identité émises par le gouvernement, comme les numéros d'assurance sociale (NAS), de permis de conduire et carte d'assurance maladie, ainsi que les numéros de comptes financiers, comme les numéros de cartes de crédit ou débit, lesquels peuvent servir de 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 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. Cependant, 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 tel 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 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 (p. ex., 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 LPRDPE, les organisations doivent aviser les personnes concernées si une brèche dans la protection de leurs renseignements personnels présente un risque 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 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 au 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 de propriété, les dommages à une propriété et les préjudices physiques. Après l'évaluation des risques d'une situation, le chef de la protection des renseignements personnels déterminera quel type d'avis pourrait être nécessaire.

Quand, comment et qui devrait informer

À cette étape, le chef de la protection des renseignements personnels doit avoir déterminé l'évaluation des risques afin de déterminer si les personnes 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 cause davantage de préjudices, que les coûts afférents sont excessifs ou que les coordonnées actuelles des personnes concernées sont inconnues. Dans certain 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 (p. ex., en alertant la personne qui a volé l'ordinateur portable de la valeur des renseignements contenu dans celui-ci).
- Qui devrait informer : Généralement, la personne de 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 rappelé à aviser la personne concernée puisque le marchand pourrait ne pas avoir les coordonnées.
- Contenu de 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 limité 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 réglementation, les compagnies de cartes de crédit, les institutions financières, les agence 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 chef 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 »* (copie en annexe) 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 chef 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 de tout changement nécessaire afin d'intégrer les leçons tirées de l'enquête (p. ex., 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 (p. ex., 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 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 commissariat à la vie privée de votre province, s'il y en a un dans la province dans laquelle vous détenez un permis, pour le Québec : www.cai.gouv.qc.ca

Registre des incidents de confidentialité

Tenir un registre des incidents de confidentialité

Toute organisation doit tenir un registre colligeant l'ensemble des incidents de confidentialité impliquant un renseignement personnel qu'elle détient, même ceux ne présentant pas de risque de préjudice sérieux. L'organisation doit transmettre une copie du registre à la Commission lorsqu'elle le demande.

Le registre des incidents de confidentialité devrait notamment décrire les renseignements personnels visés par l'incident et contenir des informations sur les circonstances de l'incident, le nombre de personnes visées, l'évaluation de la gravité du risque de préjudice et les mesures prises en réaction à l'incident. Les dates pertinentes devraient aussi y figurer : survenance de l'incident, détection par l'organisation, transmission des avis (s'il y a lieu), etc.