



POLITIQUE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS

CHEF DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS : MYLÈNE GAGNON

DATE DE RÉVISION : 16 NOVEMBRE 2023

TABLE DES MATIERES

1. NOTRE ENGAGEMENT	2
2. RESPONSABILITÉ.....	2
3. CONSENTEMENT.....	2
4. RENSEIGNEMENTS PERSONNELS RECUEILLIS.....	3
5. RAISONS DE LA COLLECTE / UTILISATION / CONSERVATION	4
6. LIMITE DE LA COLLECTE.....	5
7. LIMITE DE L'UTILISATION / COMMUNICATION À UN TIERS / CONSERVATION.....	5
8. EXACTITUDE DES RENSEIGNEMENTS.....	6
9. PROTECTION DE VOS RENSEIGNEMENTS PERSONNELS	6
10. ACCÈS À VOS RENSEIGNEMENTS PERSONNELS ET À VOTRE DOSSIER	7
11. MISE À JOUR DE VOS RENSEIGNEMENTS PERSONNELS	7
12. DURÉE DE CONSERVATION DE VOS RENSEIGNEMENTS PERSONNELS.....	8
13. POUR NE PLUS RECEVOIR DE RENSEIGNEMENTS SUR NOS PRODUITS.....	8
14. VOS CHOIX EN MATIÈRE DE RENSEIGNEMENTS PERSONNELS	8
15. POUR NOUS JOINDRE	8
16. RÉVISION ET MISE À JOUR DE LA POLITIQUE	9
17. VOTRE DROIT DE PORTER PLAINE.....	9
18. RÉVISION DE LA POLITIQUE.....	9
19. ENTRÉE EN VIGUEUR	9
20. RÉVISIONS	9
ANNEXE A - PROCÉDURE EN CAS DE MANQUEMENT / BRÈCHE / ATTEINTE	11
ANNEXE B - RÉFÉRENCES DE LA CHAMBRE DE LA SÉCURITÉ FINANCIÈRE	16

1. NOTRE ENGAGEMENT

Afin de vous donner accès aux produits et aux services financiers, nous recueillons certains de vos renseignements personnels et nous assurons la protection de ceux-ci. Nous respectons la Loi fédérale sur la protection des renseignements personnels et les documents électroniques (LPRPDE), ainsi que la Loi du Québec sur la protection des renseignements personnels dans le secteur privé (chapitre P-39.1) qui édicte les règles de conduite en matière d'usage et de divulgation des renseignements personnels et confidentiels des employés, usagers, clients et partenaires d'une entreprise au Québec. Nous suivons aussi les recommandations et le code déontologique de la Chambre de la sécurité financière qui est l'organisme d'autoréglementation de notre industrie. Voyez en annexe B les références au code déontologique, ainsi que les questions fréquemment posées.

Optima Services Financiers accorde une attention particulière à la sensibilisation de ses employés à la protection et la confidentialité des renseignements personnels qu'ils recueillent, utilisent et communiquent et exige d'eux la plus grande discréction quant à ces informations, dans l'exercice de leur fonction et à l'extérieur de leur travail.

La présente politique a donc été mise en place pour décrire dans quelles conditions les renseignements qui nous sont transmis sont recueillis, utilisés, divulgués et conservés, et pour préciser nos pratiques en matière de sécurité.

2. RESPONSABILITÉ

Nous sommes responsables des renseignements personnels que nous recevons de nos clients. Nous protégerons ces renseignements, quel que soit le moyen utilisé lors de la transmission.

3. CONSENTEMENT

Nous ne recueillerons, n'utiliserons et ne divulguerons vos renseignements personnels qu'avec votre consentement, sauf dans les cas prévus et exigés par la loi.

Lorsque vous présentez une demande de produit ou de service, nous vous demandons de nous fournir uniquement les renseignements qui nous permettent de traiter votre demande, de vous offrir les meilleurs produits ou services ou de vous offrir des produits ou services susceptibles de vous intéresser.

Votre consentement peut être verbal, écrit, exprès (par exemple, fournir les renseignements personnels sur une proposition et/ou une ouverture de compte) ou tacite (par exemple, ne pas retirer son consentement à l'égard de l'utilisation de vos renseignements personnels lorsque requis).

Votre conseiller autorisé peut accorder le consentement en votre nom si ce dernier est dûment autorisé à le faire, par exemple par l'emploi du formulaire d'autorisation limitée et une consigne claire de votre part.

En signant le formulaire d'autorisation, vous consentez, en votre nom ainsi qu'au nom de vos liquidateurs, administrateurs ou cessionnaires, à :

- Fournir des renseignements exacts tout au long de notre relation d'affaires et au fur et à mesure que votre situation évolue.

- Nous permettre d'utiliser, de transmettre et de divulguer ces renseignements au besoin à nos fournisseurs, associés et agents généraux administrateurs, qui pourraient conserver certains renseignements dans leurs dossiers pour une utilisation et une recommandation ultérieure par nous, nos fournisseurs et tout cessionnaire.
- Nous permettre de conserver vos renseignements personnels, y compris les renseignements médicaux qui apparaissent sur vos propositions, dans nos dossiers papier et électroniques aussi longtemps que vous souhaitez faire affaires avec nous ou que nous devions satisfaire à un besoin commercial ou règlementaire en conservant les renseignements.
- Céder votre dossier, y compris vos renseignements personnels, à un autre agent et/ou AGA, pour continuer à répondre à vos besoins, advenant l'invalidité, le décès, la retraite ou tout autre événement majeur affectant votre conseiller. Vous avez cependant le droit de choisir votre propre conseiller à ce moment-là, si jamais vous n'êtes pas d'accord avec celui qui vous a été attribué.

Vous pouvez retirer le consentement que vous nous avez accordé à l'égard de la collecte, de l'utilisation et de la divulgation de vos renseignements personnels à tout moment, sous réserve des restrictions juridiques et contractuelles et d'un préavis raisonnable.

4. RENSEIGNEMENTS PERSONNELS RECUUEILLIS

Les renseignements personnels signifient les renseignements concernant un individu identifiable et peuvent se rapporter plus particulièrement, mais non limitativement aux éléments décrits à la section 4.1 et suivantes.

4.1 renseignements permettant d'établir votre identité

- le nom, l'adresse, le numéro de téléphone de la résidence, l'emploi, le numéro de téléphone au travail, l'adresse de courriel, le numéro d'assurance sociale, le numéro de sécurité sociale, la date de naissance, les numéros de comptes, etc.;
- * *Afin d'établir votre identité, nous avons besoin d'une pièce d'identité avec photo émanant d'un gouvernement, soit fédéral ou provincial (ex. : passeport, permis de conduire, carte d'assurance maladie).*

4.2 renseignements liés aux opérations

- par exemple, les renseignements sur les opérations effectuées dans le cadre de votre relation avec nous et avec d'autres institutions financières;

4.3 renseignements nécessaires à la souscription d'un de nos produits ou services

- par exemple, votre revenu annuel, votre employeur, vos placements, le solde de vos comptes, vos dettes, votre actif, votre passif, votre avoir net et l'historique de vos opérations;

4.4 renseignements sur vos habitudes financières

- comme vos antécédents de paiement et votre solvabilité;

4.5 renseignements sur votre santé

- nous pouvons vous demander de nous fournir de tels renseignements si vous souscrivez un produit ou un service d'assurance;

4.6 renseignements de nature commerciale

- si vous faites appel à nos services au nom d'une entreprise, nous pouvons vous demander de nous fournir des renseignements comme la dénomination sociale, les numéros d'inscription, l'adresse, le numéro de téléphone, l'adresse courriel, le secteur d'exploitation et la situation financière de cette entreprise, de même que les détails sur son propriétaire, ses employés et sa haute direction;

4.7 renseignements supplémentaires

- d'autres renseignements peuvent vous être demandés s'ils peuvent nous aider à déterminer votre admissibilité à un ou des produits ou services que nous offrons.

Vous êtes toujours libre de nous fournir ou non les renseignements personnels que nous vous demandons. Toutefois, si vous faites appel à nos services pour un produit d'assurance, produit financier ou tout service financier connexe et que vous refusez de nous communiquer certains renseignements, il peut être difficile, voire impossible pour nous de vous fournir les produits ou services que vous avez souscrits. Il peut être d'autant plus difficile de vous conseiller ou de vous suggérer d'autres possibilités.

Vous pouvez retirer le consentement que vous nous avez accordé à l'égard de la collecte, de l'utilisation et de la divulgation de vos renseignements personnels à tout moment, sous réserve des restrictions juridiques et contractuelles et d'un préavis raisonnable.

5. RAISONS DE LA COLLECTE / UTILISATION / CONSERVATION

Nous recueillons tous les renseignements personnels (y compris les renseignements médicaux et financiers ainsi que ceux sur la société et les renseignements qui y sont liés) avec votre consentement. Nous les utilisons et les conservons uniquement afin de fournir des conseils, d'administrer des produits ou des services que vous achetez par notre entremise et de vous conseiller de nouveaux produits ou services qui pourraient vous intéresser.

Nous utilisons ces renseignements personnels, incluant votre numéro d'assurance sociale pour :

- confirmer votre identité;
- déterminer votre admissibilité aux produits d'assurance et financiers et/ou déterminer si ces produits conviennent à votre situation;
- déterminer et vérifier votre solvabilité relativement aux produits et aux services financiers et aux produits et aux services d'assurance que vous sollicitez;
- administrer et assurer le service pour les produits d'assurance et/ou financiers que nous fournissons;
- satisfaire aux exigences légales, réglementaires et contractuelles relatives aux produits et aux services auxquels vous avez accès;

Nous pouvons également communiquer avec vous par divers moyens, notamment par téléphone, par courrier électronique ou par courrier, en utilisant les coordonnées que vous nous avez fournies.

Si vous avez donné votre consentement, il se peut que nous utilisions vos renseignements pour vous faire parvenir des renseignements sur nous et sur les produits et services que nous offrons.

Si vous ne désirez pas que vos renseignements personnels soient utilisés à cette fin, vous pouvez communiquer avec nous au numéro de téléphone ou à l'adresse indiquée à la rubrique « Comment nous joindre » pour nous en informer.

Finalement, prenez note que les renseignements médicaux ne seront en aucun temps partagés ou utilisés à des fins autres que celles prévues à l'origine.

6. LIMITE DE LA COLLECTE

Nous recueillons et conservons uniquement les renseignements qui nous aident à vous conseiller, y compris les renseignements personnels, financiers et médicaux, et à répondre à nos obligations réglementaires. Nous utilisons uniquement des moyens équitables et légaux pour recueillir ces renseignements.

7. LIMITE DE L'UTILISATION / COMMUNICATION À UN TIERS / CONSERVATION

Nous utiliserons et divulguerons vos renseignements personnels afin de remplir nos fonctions, de vous conseiller et, s'il y a lieu, de respecter la loi. Les renseignements personnels contenus dans votre dossier client seront communiqués seulement :

- À nos employés et aux personnes que nous aurons autorisés, comme par exemple des professionnels afin de vous aider dans des domaines d'expertise qui dépassent notre compétence.
- Aux compagnies dont nous offrons les produits et les services et à leurs employés et mandataires pour leurs activités visant à vous fournir ou à chercher à vous fournir des produits et des services financiers, ou pour toute autre activité connexe (et en lien avec toute autre fin que vous avez autorisée);
- Aux tiers fournisseurs de services sélectionnés que nous aurons autorisés; s'ils sont situés à l'étranger, vos renseignements personnels peuvent alors être assujettis aux lois applicables, y compris les lois sur l'accès à l'information des autorités publiques, d'autres pays;
- Aux personnes ou aux entités à qui vous y avez donné accès ou qui sont autorisées à y accéder en vertu de la loi.

Nous avons l'obligation de conserver la plupart des renseignements que nous recueillons pour des raisons réglementaires, y compris l'exigence de démontrer que les recommandations que nous faisons sont appropriées et répondent à vos besoins identifiés.

Conformément aux lois applicables et à votre autorisation écrite, vous avez le droit de prendre connaissance des renseignements personnels qui sont contenus dans votre dossier. À votre demande, des copies (et non des originaux) d'autres documents personnels, comme des polices d'assurance, des testaments ou des mandats (procurations), peuvent être conservées dans votre dossier.

Si vous souhaitez que nous divulguions une information personnelle à votre sujet à un tiers qui ne fait pas partie de nos fournisseurs avec qui nous entretenons des relations contractuelles, nous exigerons de votre part une

procuration dans laquelle vous devrez identifier cette personne et nous préciser la nature des informations que vous souhaitez que nous lui divulguions et le contexte.

Nous ne vendons pas les renseignements personnels.

Par contre, en cas de transfert de clientèle, vos renseignements personnels pourraient provenir ou être transférés d'un courtier offrant le service à un autre afin de maintenir le service qui vous est dû.

8. EXACTITUDE DES RENSEIGNEMENTS

Afin de faire les recommandations appropriées, nous devons recevoir des renseignements exacts. Il nous incombe de conserver les renseignements à votre sujet aussi exacts et à jour que possible. Si la situation le permet, nous tenterons de mettre à jour vos renseignements personnels afin de déterminer si les recommandations que nous avons faites sont toujours appropriées selon l'évolution de votre situation. Cependant, nous nous fions également à vous pour nous fournir des mises à jour régulières pour la même raison. Vous pouvez passer en revue les renseignements personnels que nous conservons à votre sujet sur demande.

9. PROTECTION DE VOS RENSEIGNEMENTS PERSONNELS

Nous sommes responsables de tous les renseignements personnels que nous avons en notre possession. Nous conservons un dossier de vos renseignements personnels.

S'il y a lieu, les documents papier relatifs à votre dossier sont conservés au bureau du conseiller attitré.

Nous avons également conçu des dispositifs de protection physiques (déchiquetage), électroniques (conservation infonuagique, cryptage des appareils informatiques) et procéduraux visant à protéger vos renseignements personnels contre les pertes, le vol, la divulgation non autorisée, la reproduction, l'utilisation et les modifications non autorisées.

Les documents papiers sont conservés pour la durée de l'analyse ou en attendant de vous les remettre advenant que ce soit des documents qui doivent vous être remis. Sinon, l'information est conservée électroniquement. Les documents sont numérisés afin de faciliter la consultation. Les dossiers sont conservés chez un fournisseur de système de gestion de données sécurisé qui est soumis lui-même à des règles strictes de confidentialité.

Tous nos employés, nos conseillers associés, nos représentants et nos fournisseurs de services autorisés doivent assurer la confidentialité de vos renseignements personnels. Tous et chacun d'entre nous sommes tenus de signer un accord de confidentialité dès le début de l'emploi et nous nous assurons de rester conscientisés sur une base régulière par des formations et contenus touchant l'importance de la protection des renseignements personnels et de la cybersécurité. De plus, seuls les employés, les représentants et les fournisseurs de services autorisés devant avoir accès à vos renseignements personnels dans l'exercice de leurs fonctions obtiennent l'autorisation d'avoir accès à vos renseignements personnels.

Ainsi, vos informations pourraient aussi être gardées à l'un des bureaux de nos agents généraux en assurances et de courtage en épargne collective et chez les assureurs, banques et compagnies de fonds dans le cadre des activités nécessaires à la gestion de vos demandes.

Cependant, nous n'assumons aucune responsabilité pour les pratiques relatives à la protection de la vie privée et les politiques des entreprises et des organismes:

- qui visent à obtenir des renseignements personnels sans que des liens soient maintenus avec nous;
- dont notre site Web fournit les liens.

Vous devez passer en revue les politiques sur la protection des renseignements personnels de ces entreprises et ces organismes avant de leur fournir vos renseignements personnels.

En annexe A, vous trouverez notre procédure en cas de manquement / brèche / atteinte à la protection de vos renseignements personnels.

10. ACCÈS À VOS RENSEIGNEMENTS PERSONNELS ET À VOTRE DOSSIER

Vous avez le droit, dans le cours normal des activités, de :

- savoir si nous conservons des renseignements personnels sur vous. Cependant, si nous avons obtenu d'un tiers des renseignements médicaux de nature pertinente à votre sujet, nous ne divulguerons ces renseignements qu'à votre médecin;
- savoir dans quel but nous avons utilisé et utilisons les renseignements personnels que nous avons recueillis sur vous;
- connaître les noms de ceux à qui nous avons divulgué des renseignements personnels vous concernant.

Vous devez communiquer avec nous (vous trouverez notre adresse dans la section Comment nous joindre) si vous désirez avoir accès aux renseignements personnels que nous possérons sur vous. Dans certains cas, il se peut que vous ayez accès à tous les renseignements. Par contre, il est possible que l'accès à ces renseignements soit restreint, selon ce que la loi permet et/ou exige. À titre d'exemple, nous ne pourrons communiquer certains renseignements liés au privilège juridique, à l'information personnelle d'un tiers ou des renseignements qui constituent des renseignements commerciaux confidentiels.

11. MISE À JOUR DE VOS RENSEIGNEMENTS PERSONNELS

Nous nous efforcerons de nous assurer que les renseignements personnels recueillis et utilisés sont exacts et, au besoin, mis à jour. Nous vous invitons à nous déclarer toutes modifications à vos renseignements personnels en communiquant avec nous.

Vous avez également le droit de demander une modification de tout renseignement inexact et incomplet vous concernant.

12. DURÉE DE CONSERVATION DE VOS RENSEIGNEMENTS PERSONNELS

Nous conserverons vos renseignements personnels tant et aussi longtemps qu'ils seront nécessaires dans le cadre de notre relation avec vous, qu'ils seront requis par la Loi ou qu'ils seront nécessaires pour protéger nos droits en cas de recours. La durée de conservation de vos renseignements personnels est liée au produit ou au service et à la nature de l'information.

Afin d'obtenir davantage d'information sur la durée exacte pendant laquelle ces renseignements seront conservés, nous vous invitons à communiquer avec le Responsable de la protection des renseignements personnels identifié plus loin dans la présente Politique.

13. POUR NE PLUS RECEVOIR DE RENSEIGNEMENTS SUR NOS PRODUITS

Vous pourrez toujours garder le contrôle de vos renseignements personnels. Si vous ne désirez pas que vos renseignements soient utilisés pour recevoir des documents promotionnels de notre part, si vous souhaitez retirer votre consentement ou vous ne voulez pas que vos renseignements personnels soient utilisés, divulgués ou partagés, vous pouvez tout simplement communiquer avec nous par écrit à l'adresse mentionnée à la page suivante. Veuillez noter que le retrait et/ou la modification de votre consentement seront effectués dans un délai raisonnable.

14. VOS CHOIX EN MATIÈRE DE RENSEIGNEMENTS PERSONNELS

Vous pouvez retirer votre consentement en tout temps (sous réserve de restrictions contractuelles ou légales de nous fournir un préavis raisonnable) en communiquant avec nous. Si vous retirez votre consentement, nous pourrions être dans l'impossibilité de vous fournir les produits ou les services demandés et nous pourrions devoir mettre fin à notre relation d'affaires.

15. POUR NOUS JOINDRE

Veuillez envoyer PAR ÉCRIT vos demandes d'accès à vos renseignements personnels, vos questions, vos plaintes et vos commentaires sur notre politique de protection des renseignements personnels, vos demandes de mises à jour et de corrections de vos renseignements personnels à :

Optima Services Financiers
594 Bruno, Drummondville, QC J2C 4M5
819 313-2287

Voici aussi l'adresse des agents généraux avec qui nous sommes partenaires et inscrits :

Groupe Cloutier Investissements et Groupe Cloutier inc.
Att. Agent du service de la protection des renseignements personnels
1720, rue de la Sidbec Sud, Trois-Rivières, QC G8Z 4H1
866 477-2272

16. RÉVISION ET MISE À JOUR DE LA POLITIQUE

Optima Services Financiers peut passer en revue et modifier sans préavis la présente politique sur la protection des renseignements personnels. Veuillez reparcourir régulièrement la présente politique pour vous assurer de connaître les pratiques actuelles de gestion de l'information. Si vous nous fournissez des renseignements personnels après que nous ayons modifié la présente politique sur la protection des renseignements personnels, nous tiendrons pour acquis que vous avez accepté ces modifications.

17. VOTRE DROIT DE PORTER PLAINE

Si vous avez des préoccupations concernant la collecte, l'utilisation ou la divulgation de vos renseignements personnels, ou si vous avez une plainte à formuler, vous pouvez le faire auprès de nous ou du Commissariat à la protection de la vie privée :

Chef de la protection des renseignements personnels
Mylène Gagnon
594 Bruno, Drummondville, Qc J2C 4M5
mgagnon@optimasf.ca | cell. : 819 313-2287

Commissariat à la protection de la vie privée du Canada
30, rue Victoria
Gatineau (Québec) K1A 1H3
Sans frais : 1-800-282-1376

18. RÉVISION DE LA POLITIQUE

Mme Mylène Gagnon, à titre de Chef de la protection des renseignements personnels au sein du Optima Services Financiers est responsable de la révision de la présente politique, en précisant la date de chaque révision.

19. ENTRÉE EN VIGUEUR

La présente politique est entrée en vigueur le 1^{er} janvier 2021.

20. RÉVISIONS

Date de révision	Modifications apportées	Responsable
16 novembre 2023	Révision du texte seulement	Mylène Gagnon

ANNEXE A

PROCÉDURE EN CAS DE MANQUEMENT / BRÈCHE / ATTEINTE

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.

Tel que déterminé par la Commission d'accès à l'information du Québec (www.cai.gouv.qc.ca), nous suivrons les six (6) étapes suivantes en cas d'atteinte à la protection de vos renseignements personnels :

- ÉTAPE 1 : ÉVALUATION PRÉLIMINAIRE DE LA SITUATION
- ÉTAPE 2 : LIMITÉ DE L'ATTEINTE À LA VIE PRIVÉE
- ÉTAPE 3 : ÉVALUATION DES RISQUES ASSOCIÉS À L'ATTEINTE
- ÉTAPE 4 : NOTIFICATION À L'INTENTION DES PERSONNES CONCERNÉES
- ÉTAPE 5 : PRÉVENTION
- ÉTAPE 6 : SUIVI

ÉTAPE 1 : ÉVALUATION PRÉLIMINAIRE DE LA SITUATION

- a) Définir sommairement le contexte de la perte ou du vol de renseignements personnels :
 - Identifier les renseignements personnels touchés ainsi que leur support;
 - Identifier les personnes, leur nombre ainsi que le groupe de personnes (clients, employés, etc.) touchées;
 - Etablir le contexte des événements (date, heure, lieu, etc.);
 - Identifier, si possible, les circonstances entourant la perte (cause, personnes susceptibles d'être impliquées dans l'incident, etc.);
 - Répertorier les mesures de sécurité physiques et informatiques en place lors de l'incident.
- b) Informer les autorités externes concernées qui doivent être avisés de l'incident immédiatement : (avant l'évaluation des risques)
 - Service de police (si les circonstances laissent croire à la possibilité d'un crime);
 - Commission d'accès à l'information
- c) Désigner une personne ou une équipe responsable de la gestion de la situation.

- d) Informer les intervenants concernés à l'interne :
- Dirigeants de l'organisme ou de l'entreprise;
 - Responsable de l'unité administrative concernée;
 - Responsable de la protection des renseignements personnels;
 - Conseiller juridique;
 - Direction des communications (gestion des médias et des appels de la clientèle).

ÉTAPE 2 : LIMITÉ DE L'ATTEINTE À LA VIE PRIVÉE

Prendre sans tarder des mesures adéquates pour limiter les conséquences pour les personnes concernées d'une possibilité d'utilisation malveillante de leurs renseignements personnels, de l'usurpation ou du vol de leur identité :

- a) Prendre des mesures afin de limiter immédiatement les conséquences d'une perte ou d'un vol de renseignements personnels en s'assurant de mettre fin à la pratique non conforme le cas échéant;
- b) Récupérer les dossiers physiques ou numériques, selon le cas;
- c) Révoquer ou modifier les mots de passe ou les codes d'accès informatiques;
- d) Contrôler les lacunes dans les systèmes de sécurité.

ÉTAPE 3 : ÉVALUATION DES RISQUES ASSOCIÉS À L'ATTEINTE

- a) Compléter une évaluation préliminaire des risques, en considérant la sensibilité des renseignements personnels en cause, tenant compte de leur nature, leur quantité, la possibilité de les combiner avec d'autres renseignements, les personnes concernées, etc.;
- b) Déterminer le contexte de l'incident incluant :
 - la cause (ex. le caractère délibéré ou non de la perte ou du vol de renseignements personnels, l'erreur humaine, une faille informatique, etc.);
 - les auteurs connus ou probables des renseignements personnels perdus ou subtilisés (ex. organisation criminelle, public en général, etc.);
 - l'étendue de la situation (nombre de personnes touchées et secteurs touchés);
 - le caractère systémique ou non de la disparition des renseignements personnels (particulièrement lorsque la perte n'est pas générée directement par une intervention humaine);
 - une évaluation de la probabilité qu'un événement similaire se reproduise.
- c) Évaluer la possibilité que les renseignements personnels concernés fassent l'objet d'une utilisation préjudiciable pour les personnes concernées en tenant compte, notamment, des mesures de sécurité prises pour les protéger, de leur difficulté d'accès et de leur intelligibilité (mot de passe, encodage, etc.);
- d) Évaluer le caractère réversible ou non de la situation, dont la possibilité de récupérer les renseignements personnels;

- e) Évaluer si les mesures immédiates prises étaient adéquates pour limiter l'atteinte et les compléter si nécessaire;
- f) Déterminer les préjudices potentiels, notamment en évaluant les possibilités d'utilisation future des renseignements personnels par des personnes malveillantes, notamment pour le vol d'identité;
- g) Déterminer les priorités et identifier les actions à prendre à partir des résultats de l'évaluation de ces risques.

ÉTAPE 4 : NOTIFICATION À L'INTENTION DES PERSONNES CONCERNÉES

- a) Déterminer qui doit être mis au courant de la perte ou du vol de renseignements personnels en fonction de l'évaluation des risques :
 - Service de police : Dans les cas où la disparition peut résulter de la commission d'un crime, le service de police concerné doit être avisé des éléments entourant cette disparition tout d'abord et, ensuite, de toutes les démarches subséquentes. Il est nécessaire de porter une attention particulière afin de ne pas nuire à l'enquête et de préserver les éléments de preuve pouvant être pertinents;
 - Personnes concernées : Si la perte ou le vol de renseignements personnels présente un risque de préjudice pour les personnes concernées, celles-ci devraient en être avisées sans tarder. Il ne s'agit pas d'alarmer mais de prévenir afin de leur permettre de prendre les mesures pertinentes pour protéger leurs renseignements personnels;
 - Commission d'accès à l'information: Si les personnes concernées par les renseignements personnels proviennent du Québec, la Commission pourrait amorcer une inspection ou une enquête et jouer un rôle de conseiller dans la recherche de solution;
 - Autres : Il peut également être nécessaire d'aviser d'autres intervenants, tels que les agences de crédit, un mandataire, un cocontractant, une instance gouvernementale, un syndicat, un ordre professionnel, etc.

Toutefois, dans la diffusion des informations concernant la perte de renseignements personnels, une attention particulière doit être portée afin de ne pas aggraver le préjudice que pourraient subir les personnes concernées (ex. limiter au minimum les renseignements personnels dans les avis).

- b) Désigner les personnes responsables d'aviser les intervenants externes identifiés précédemment ainsi que le moment et le moyen (lettre, courriel, téléphone);
- c) Le cas échéant, identifier et consigner les motifs à l'origine de la décision de ne pas aviser les personnes concernées et les autres intervenants.

AVIS AUX PERSONNES CONCERNÉES PAR UNE PERTE OU UN VOL DE LEURS RENSEIGNEMENTS PERSONNELS :

Selon les circonstances, il pourrait s'avérer nécessaire d'aviser les personnes victimes de la perte ou du vol de leurs renseignements personnels. Cet avis pourrait inclure certains des éléments suivants:

- Le contexte de l'incident et le moment où il s'est produit ainsi qu'une description de la nature des renseignements personnels touchés ou potentiellement touchés, sans dévoiler de renseignements personnels spécifiques;

- Une description sommaire des mesures prises afin de limiter ou de prévenir tout préjudice, ainsi que la liste des personnes qui ont été informées de la situation (Service de police, Commission d'accès à l'information, etc.);
- Les actions prises par les organismes et les entreprises pour aider les personnes concernées (Service d'aide et d'information, Abonnement alerte crédit, etc.);
- Les mesures que les personnes concernées peuvent prendre afin de réduire les risques de préjudice ou pour mieux se protéger (référence au document « Le vol d'identité » disponible à la Commission d'accès à l'information);
- Les autres documents d'information générale conçus pour aider les personnes à se prémunir contre le vol d'identité;
- Les coordonnées d'un interlocuteur de l'organisation qui peut répondre aux questions et à qui il est possible d'effectuer tout signalement;
- Les principales mesures qui seront prises pour éviter que la situation ne se reproduise (changement de pratique ou de processus, la formation du personnel, la révision ou l'élaboration de politiques, une vérification, un suivi périodique, etc.).

ÉTAPE 5 : PRÉVENTION

- a) Approfondir l'analyse des circonstances de la perte ou du vol des renseignements personnels et effectuer une description chronologique des événements et des actions prises face à cet incident, incluant les dates et les intervenants concernés;
- b) Répertorier et examiner les normes, politiques ou directives internes en place au moment de l'incident, autant au niveau de la sécurité informatique, lorsque l'information est en cause, que de la protection des renseignements personnels en général;
- c) Vérifier si ces normes, politiques ou directives internes ont été suivies par les personnes impliquées, identifier les raisons pour lesquelles elles n'ont pas été suivies, le cas échéant;
- d) S'il s'agit d'une erreur de procédure ou d'une défaillance opérationnelle, les consigner au dossier de sécurité et adapter les processus pour éviter qu'un tel incident ne survienne à nouveau;
- e) Évaluer la nécessité d'élaborer une politique en matière de traitement d'une perte ou d'un vol de renseignements personnels au sein de l'organisme ou de l'entreprise;
- f) Formuler les recommandations relatives aux solutions à moyen et long termes et aux stratégies de prévention;
- g) S'assurer de la réelle nécessité, pour l'organisme ou l'entreprise, de la collecte des renseignements personnels concernés;
- h) Prévoir le suivi devant être accordé.

ÉTAPE 6 : SUIVI

Il est important d'effectuer le suivi :

- a) du processus de traitement qui doit être appliqué lors d'une perte ou d'un vol de renseignements personnels et des résultats obtenus afin de l'améliorer, s'il y a lieu;
- b) des mesures de sécurité requises à la suite de l'incident et de leur performance afin d'améliorer les processus et place et de mettre à jour la Politique en matière de protection des renseignements personnels;
- c) de la communication de l'information pertinente à la Commission d'accès à l'information et au service de police impliqué, le cas échéant.

TENUE DE DOSSIER

Il est également obligatoire de tenir un registre de tous les événements d'atteinte à la protection des renseignements personnels, même si certains n'avaient aucun risque de préjudice grave. Tout événement doit être conservé 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.

ANNEXE B

RÉFÉRENCES DE LA CHAMBRE DE LA SÉCURITÉ FINANCIÈRE

Code de déontologie

Un représentant doit s'assurer que les renseignements qu'il détient sur ses clients demeurent confidentiels, à moins que certaines dispositions légales ou qu'une ordonnance d'un tribunal permettent de les divulguer. Il est également tenu d'utiliser les renseignements qu'il recueille seulement aux fins pour lesquelles il les a obtenus et de ne jamais les utiliser au préjudice de son client.

Ce sont les articles 26 et 27 du Code de déontologie de la Chambre de la sécurité financière qui prévoient ces obligations.

Art. 26 – Le représentant doit respecter le secret de tous renseignements personnels qu'il obtient sur un client et les utiliser aux fins pour lesquelles il les obtient, à moins qu'une disposition d'une loi ou d'une ordonnance d'un tribunal compétent ne le relève de cette obligation.

Art. 27 – Le représentant ne doit pas divulguer les renseignements personnels ou de nature confidentielle qu'il a obtenus autrement que conformément aux dispositions de la loi, ni les utiliser au préjudice de son client ou en vue d'obtenir un avantage pour lui-même ou pour une autre personne.

Il est aussi important de souligner l'exigence de l'article 23 de la Loi sur la distribution de produits et services financiers qui prévoit qu'un représentant doit transmettre à l'établissement auquel il est rattaché tous les renseignements qu'il recueille relativement à ses clients. Il ne peut les communiquer qu'à une personne autorisée par la loi à les recevoir.

Questions fréquemment posées

Q : Les dossiers et registres tenus doivent-ils être conservés dans un classeur verrouillé ainsi que dans une pièce fermée à clé ?

R : La règle générale veut que les dossiers soient conservés dans un lieu sûr et sécuritaire. Ce lieu ne doit donc pas être accessible facilement, autrement que par les personnes autorisées. Évidemment, il faut également s'assurer que ces dossiers seront facilement repérables, dans un délai raisonnable, lorsqu'une personne dûment autorisée souhaite y avoir accès. Ainsi, conserver les dossiers dans des classeurs fermés à clé dans une pièce verrouillée constitue une bonne façon de remplir ces obligations. Toutefois, toute autre méthode sûre et sécuritaire permettant d'atteindre le même objectif serait tout aussi acceptable.

Q : Qu'en est-il de la conservation des dossiers électroniques ?

R : En matière de dossiers électroniques, la même règle que celle des dossiers physiques s'applique, dans la mesure où il faut s'assurer que leur mode de conservation est sûr et sécuritaire. Cela suppose que les renseignements soient conservés de façon à ce que personne, autre qu'une personne dûment autorisée, n'y ait accès. De plus, il faut s'assurer que ces renseignements ne peuvent pas être falsifiés ou détruits involontairement.

L'utilisation d'un code d'accès, d'un logiciel antivirus et la protection de l'accès au réseau constituent des exemples permettant l'atteinte de ces objectifs.

Q : Doit-on posséder un classeur pour chaque type de registre ou de dossier tenu ?

R: Un principe essentiel en matière de conservation de dossiers veut que ceux-ci soient conservés de façon à ce qu'ils puissent être facilement retrouvés dans un délai raisonnable. Cela implique l'utilisation d'une méthode de classement efficace permettant de retracer chaque type de dossier ou de registre. Le recours à l'utilisation d'un classeur distinct pour chaque type de dossier, jumelé à une codification adéquate, pourrait donc s'avérer efficace même si rien ne l'oblige.

Q: Dans un dossier client, doit-on détailler le contrat vendu, même lorsque l'on joint au dossier une copie de la proposition et l'illustration des produits vendus ?

R: L'important, en matière de tenue de dossiers, est que tous les renseignements nécessaires prévus au Règlement sur la tenue et la conservation des livres et registres se trouvent dans vos dossiers. D'ailleurs, ne perdez pas de vue que ces dossiers vous permettront également d'assurer un service professionnel à vos clients. L'objectif de ces dossiers devrait donc être l'accès facile à tous les renseignements qui vous seront utiles pour bien conseiller vos clients. Vos dossiers clients devraient notamment contenir les renseignements suivants : les coordonnées du client (nom, date de naissance, adresse, numéro de téléphone, numéro de télécopieur et adresse électronique), l'objet, la nature et le coût du produit vendu ou du service rendu, le numéro de la police, les dates de l'émission du contrat et de la signature de la proposition ou de la demande de service, le nom du représentant impliqué dans la transaction, son mode de rémunération, et ce, à l'égard de chaque produit vendu ou service rendu, la date et le mode de paiement du produit vendu ou du service rendu, une copie de l'analyse de besoins financiers (ABF) du client, une copie du formulaire requis lors du remplacement d'une police ainsi que tout autre renseignement recueilli auprès du client, et tout document afférent. Ainsi, lorsque la copie de la proposition et l'illustration des produits vendus contiennent tous ces renseignements, rien n'exige de détailler le contrat vendu. Par contre, vous pouvez très bien décider d'en ajouter plus que nécessaire, pourvu que cela soit pertinent. De plus, assurez-vous de respecter les normes de tenue de dossiers imposées par l'établissement auquel vous êtes rattaché.

Q: Si un individu est le seul représentant en assurance de personnes de son cabinet, à quelles règles doit-il se conformer ?

R: Selon les obligations prévues dans la Loi sur la distribution de produits et services financiers, le Règlement sur la tenue et la conservation des livres et registres et le Règlement sur le cabinet, le représentant autonome et la société autonome, vous devez appliquer les règles en fonction du mode d'exercice sous lequel vous exercez. Dans les faits, pour qu'un représentant obtienne un droit de pratique, il doit détenir un certificat délivré par l'AMF de même qu'une assurance professionnelle, et doit être autorisé à exercer sous un mode d'exercice en particulier, conformément à l'article 14 de la Loi sur la distribution de produits et services financiers. C'est donc à ce mode d'exercice que vous devez vous référer. Ainsi, si vous êtes un représentant autonome et que vous n'êtes donc pas rattaché à un cabinet ou à une société autonome, vous devez appliquer les règles qui encadrent les représentants autonomes. Si vous exercez plutôt vos activités pour un cabinet ou pour une société autonome, ceux-ci doivent mettre en application les règles qui leur sont imposées.

Q: Un conseiller en sécurité financière peut-il conserver une copie de toutes les propositions d'assurance soumises durant l'étude d'un dossier ?

R: Rien dans la loi ou dans les règlements n'interdit au représentant de conserver les propositions d'assurance dans le dossier client s'il s'agit de renseignements pertinents. D'ailleurs, le Règlement sur la tenue et la conservation des livres et registres prévoit que tout autre renseignement utile et nécessaire recueilli auprès du client ainsi que tout document afférent doivent être conservés au registre. De plus, vos obligations déontologiques mentionnent que vous devez avoir une connaissance complète des faits. Il serait donc logique de conserver ces renseignements dans vos dossiers.