Financière IGM

Politique de protection des renseignements personnels

Société financière IGM Inc.

Groupe Investors Inc.

Corporation Financière Mackenzie

Investment Planning Counsel Inc.

Table des matières

1. Objectif

L'objectif de la Politique de protection des renseignements personnels d'IGM (la « Politique ») est de veiller à ce que la Société financière IGM Inc. qui comprend le Groupe Investors Inc. (« IG »), la Corporation Financière Mackenzie (« Mackenzie »), Investment Planning Counsel Inc. (« IPC »), et leurs filiales respectives ci-dessous (collectivement appelés « les sociétés d'IGM ») exercent leurs activités conformément aux lois fédérales et provinciales sur la protection des renseignements personnels.

Société inscrite	Catégorie d'inscription (Canada)
Société de gestion d'investissement I.G. (SGIIG)	Gestionnaire de fonds d'investissement/ gestionnaire de portefeuille
Valeurs mobilières Groupe Investors Inc. (VMGI)	Courtier en valeurs mobilières / Cabinet de services financiers*
Services Financiers Groupe Investors Inc. (SFGI)	Courtier en épargne collective / Cabinet de services financiers*
Services d'Assurance I.G Inc. (SAIGI)	Société d'assurance inscrite au niveau provincial
Compagnie de Fiducie du Groupe Investors Ltée (CFGI)	Société de fiducie (BSIF)
Corporation Financière Mackenzie (CFM)*	Gestionnaire de fonds d'investissement/ gestionnaire de portefeuille/courtier dispensé sur le marché
Counsel Portfolio Services (CPS)	Gestionnaire de fonds d'investissement/ gestionnaire de portefeuille
IPC Investment Corporation (IPCIC)	Courtier en épargne collective/courtier sur le marché dispensé / Cabinet de services financiers*
IPC Securities Corporation (IPCSC)	Courtier en valeurs mobilières / Cabinet de services financiers*

* Québec seulement

**Les filiales de CFM situées à l'extérieur du Canada sont assujetties aux lois régissant la protection des renseignements personnels dans le territoire de compétence où elles se trouvent.

Les sociétés d'IGM sont tenues de se conformer à la *Loi sur la protection des renseignements personnels et les documents électroniques* (la « LPRPDE ») ainsi qu'à la *Personal Information Protection Act* de l'Alberta, à la *Personal Protection Act* de la Colombie-Britannique et à la *Loi sur la protection des renseignements personnels dans le secteur privé* du Québec (collectivement appelées « lois provinciales sur la protection des renseignements personnels »). Les lois provinciales sur la protection des renseignements personnels visent les clients qui résident dans les provinces visées.

IGM tient à protéger les renseignements personnels de ses clients, et la présente Politique fait état des exigences de la LPRPDE et des lois provinciales sur la protection des renseignements personnels.

Les termes en majuscules sont définis à la section 4 de la Politique.

2. Contexte

La LPRPDE a pris effet en 2004 en ce qui concerne les entreprises du secteur privé canadien, et régit la façon dont les organisations recueillent, utilisent ou communiquent des renseignements personnels dans le cadre d'activités commerciales. L'objectif de la LPRPDE et des lois provinciales consiste à établir les règles du traitement des renseignements personnels de manière à tenir compte du droit d'un particulier à la protection de ses renseignements personnels et de l'obligation de l'entreprise de réunir, d'utiliser et de communiquer des renseignements personnels pour des raisons professionnelles légitimes.

3. Champ d'application

Cette politique vise IGM et les sociétés d'IGM en qualité de sociétés inscrites auprès des commissions des valeurs mobilières provinciales, de l'Association canadienne des courtiers de fonds mutuels (« ACFM »), de l'Organisme canadien de réglementation du commerce des valeurs mobilières (« OCRCVM ») et du Bureau du surintendant des institutions financières (BSIF), et à tout autre titre en vertu duquel les sociétés d'IGM recueillent et utilisent les renseignements personnels relatifs aux clients.

La présente politique ne s'applique pas à ce qui suit :

- les coordonnées des contacts professionnels;
- les renseignements confidentiels;
- les renseignements personnels concernant les employés, dirigeants, administrateurs et mandataires d'IGM ou d'une des sociétés d'IGM (« personnel d'IGM »).

4. Définitions

« Client » signifie toute personne au sujet de laquelle les sociétés d'IGM recueillent et conservent des renseignements personnels concernant notamment :

- les anciens clients, et les clients actuels et potentiels;
- les anciens investisseurs, et les investisseurs actuels et potentiels;
- les personnes autorisées à agir au nom d'un client ou pour un compte;
- les bénéficiaires désignés sur des comptes de client;
- les représentants de courtier (conseillers) et autres employés de courtiers externes; et
- les personnes ayant l'intention de faire des opérations avec IGM et qui ont fourni des renseignements personnels.

« Renseignements personnels » signifie tout renseignement sur un individu identifiable. Cela comprend notamment :

- le nom;
- l'âge;
- la date de naissance;
- le numéro de téléphone personnel;
- l'adresse du domicile;
- l'adresse de courriel personnelle;
- le numéro d'assurance sociale;
- les numéros de compte et les opérations;
- les renseignements bancaires;
- le revenu, l'actif, la profession, l'état civil et d'autres renseignements Connaître son client; et
- les adresses de protocole Internet (seulement si elles peuvent être associées à un individu identifiable).

« Renseignements confidentiels » signifie tous les renseignements non publics en rapport avec IGM ou les sociétés d'IGM. Cela comprend notamment :

- les activités commerciales, les plans et les stratégies;
- les nouveaux produits et les initiatives commerciales; et
- les contrats et conventions d'entreprise.

« Coordonnées des contacts professionnels » signifie les coordonnées relatives à une personne agissant à titre professionnel. Cela comprend notamment :

- l'adresse de courriel professionnelle;
- l'adresse du bureau;
- le numéro de téléphone au travail; et
- le titre du poste.

5. Principes relatifs à l'équité dans le traitement de l'information

La LPRPDE a énoncé dix principes fondamentaux visant la protection des renseignements personnels et IGM les a intégrés à sa Politique.

Premier principe – Responsabilité

IGM et les sociétés d'IGM sont responsables des renseignements personnels en leur possession, y compris des renseignements reçus de la part de tiers ou transférés à des fournisseurs externes aux fins de traitement.

Agents désignés de la protection des renseignements personnels

Chacune des sociétés d'IGM a désigné un agent responsable de la protection des renseignements personnels pour veiller à la mise en application de la Politique à l'échelle de l'organisation. Les agents de

la protection des renseignements personnels peuvent déléguer certaines fonctions à d'autres personnes au sein des services de conformité des sociétés d'IGM.

L'agent de la protection des renseignements personnels doit :

- se tenir au courant des changements à la LPRPDE, aux lois provinciales sur la protection des renseignements personnels et à toute autre loi sur la protection de la vie privée;
- déterminer l'incidence des modifications aux lois susmentionnées sur IGM et les sociétés d'IGM;
- tenir la haute direction et les comités de surveillance au courant des problèmes sérieux touchant les renseignements personnels; et
- veiller à la mise à jour et au respect de la Politique de protection des renseignements personnels d'IGM et des procédures connexes.

Personnel d'IGM

Le personnel d'IGM est chargé de la protection des renseignements personnels des clients et doit :

- accéder aux renseignements personnels seulement dans la mesure requise pour s'acquitter des tâches liées à ses fonctions;
- protéger les renseignements personnels recueillis et veiller à ce qu'ils soient recueillis, utilisés et divulgués conformément aux politiques et procédures applicables;
- préserver la confidentialité de tous les renseignements personnels auxquels il a accès même après avoir quitté IGM;
- demander l'autorisation du client (pour recueillir, utiliser et divulguer des renseignements personnels) de manière à ce que le client comprenne raisonnablement comment ces renseignements seront utilisés et communiqués;
- utiliser les renseignements personnels seulement dans le but prévu à l'origine tel que communiqué au client;
- conserver un relevé des communications de renseignements personnels lorsque requis; et
- signaler toute atteinte aux mesures de sécurité conformément à la Politique.

Deuxième principe – Détermination des fins de la collecte de renseignements

Les fins auxquelles des renseignements personnels sont recueillis, utilisés ou divulgués doivent être déterminées et consignées avant la collecte ou au moment de l'effectuer.

Les sociétés d'IGM peuvent recueillir des renseignements personnels dans la mesure nécessaire pour l'exécution des fins déterminées. Le type de renseignements personnels recueillis dépend de la nature de la relation avec le client.

Si une société d'IGM souhaite utiliser des renseignements personnels à d'autres fins que celles déterminées auprès du client, celles-ci doivent être établies au préalable, sauf s'il s'agit d'une exigence de la loi, et il faut obtenir le consentement du client.

En général, les sociétés d'IGM recueillent des renseignements personnels aux fins suivantes :

- fournir aux clients des services financiers, des produits de placement et des services d'administration des comptes;
- se conformer aux exigences juridiques et réglementaires visant les services en question, p. ex. établir l'identité de la personne et évaluer la convenance du produit; et
- gérer les comptes, transmettre des documents réglementaires et soumettre des relevés fiscaux.

Communication des motifs

Les motifs de la collecte de renseignements doivent être communiqués au client au préalable.

De façon générale, cette communication fera partie de la demande d'ouverture de compte ou de tout autre document rempli par le client au moment de recueillir les renseignements personnels, mais elle peut également faire partie d'autres documents de divulgation que le personnel d'IGM remet au client.

Les motifs de la collecte des renseignements personnels sont aussi divulgués par le truchement des avis de protection des renseignements personnels affichés sur les sites Web respectifs des sociétés d'IGM.

Troisième principe – Consentement

Pour pouvoir réunir, utiliser ou communiquer des renseignements personnels, il faut en informer le client et obtenir son consentement. Il y a deux formes de consentement :

- **Consentement exprès** – la personne a donné son consentement direct par écrit ou de vive voix.

- **Consentement tacite** – la personne n'a pas donné son consentement directement, mais plutôt de manière tacite par suite de ses actions ou des circonstances.

Le fait qu'une société d'IGM ait obtenu un consentement exprès ou tacite est en général déterminé par la nature de la relation entre les sociétés d'IGM et le client.

Le consentement de l'intéressé n'est pas requis pour la collecte, l'utilisation ou la communication de renseignements personnels à certaines fins juridiques ou de sécurité, conformément aux règles de la LPRPDE.

Obtention du consentement

En général, les sociétés d'IGM obtiennent un consentement exprès étant donné que les motifs de la collecte et d'autres renseignements pertinents sont fournis au client sur les formulaires de demande, dans les conventions ou les avis sur la protection des renseignements personnels remis au client au moment de la collecte.

Le consentement peut aussi être fourni par une personne légalement autorisée à agir au nom du client si elle détient une procuration ou est désignée à titre de tuteur.

Consentement tacite

Si une société d'IGM agit uniquement à titre de gestionnaire de fonds de placement à l'égard d'un client, et si des comptes d'investissement dans les fonds sont ouverts ou administrés directement par un courtier externe, le consentement tacite peut être présumé.

Consentement valable

Selon la LPRPDE, le consentement doit être valable, et il est considéré comme tel seulement si on peut raisonnablement s'attendre à ce que la personne visée comprenne la nature, les fins et les conséquences de la collecte, de l'utilisation ou de la communication de ses renseignements personnels.

Le consentement valable repose sur les sept principes directeurs qui suivent, selon le cas :

1. **Mettre l'accent sur les éléments clés** – Rappelez au client le type de renseignement personnel recueilli, les tiers à qui les renseignements seront communiqués. Si certains risques sont associés à la collecte, à l'utilisation et à la communication des renseignements, ces risques doivent être divulgués et expliqués.
2. **Permettre aux clients de déterminer à quel point et quand ils souhaitent obtenir de l'information détaillée** – Fournissez des avis de protection des renseignements personnels et de l'information en formats gérables et facilement accessibles, qui permettent aux clients de trouver facilement les renseignements pertinents grâce à une identification claire.
3. **Donner clairement aux individus l'option de dire « oui » ou « non »** – Offrez des options aux clients et la possibilité de retirer leur consentement s'ils le désirent.
4. **Faire preuve d'innovation et de créativité** – Proposez des options qui offrent plus de choix et de transparence aux clients.
5. **Tenir compte de la perspective du client** – Assurez au client une expérience conviviale qui correspond à sa perception de l'utilisation que nous faisons des renseignements personnels.
6. **Faire du consentement un processus dynamique et continu** – Le processus de consentement doit évoluer à mesure que les organisations innovent, prennent de l'essor et se transforment.
7. **Être responsable et se tenir prêt à démontrer sa conformité** – Effectuez des examens périodiques pour garantir la conformité des avis de protection des renseignements personnels, des formulaires de demande et des autres documents pertinents avec la LPRPDE et autres lois applicables.

Retrait du consentement

Sous réserve des restrictions légales ou contractuelles, et moyennant un préavis raisonnable, le client peut retirer son consentement en tout temps. IGM doit aviser les clients lorsque le refus ou le retrait du consentement entraîne des répercussions, par exemple, dans le cas de la fermeture d'un compte.

Quatrième principe – Limitation de la collecte

La quantité et le type de renseignements personnels recueillis sont limités à l'information nécessaire aux fins déterminées, et l'organisation doit procéder à la collecte de façon honnête et licite.

Les types de renseignements recueillis sont décrits dans les demandes d'ouverture de compte, les brochures de divulgation qui les accompagnent et/ou les avis relatifs à la protection des renseignements personnels qui sont affichés sur les sites Web des sociétés d'IGM.

On ne doit pas réunir des renseignements personnels à des fins non déterminées.

Cinquième principe – Limitation de l'utilisation, de la communication et de la conservation

On ne doit pas utiliser ni communiquer de renseignements personnels pour des besoins distincts de ceux pour lesquels ces renseignements ont été réunis, sauf avec le consentement du client ou pour respecter les exigences de la loi. On ne doit conserver ces renseignements que pendant la durée nécessaire pour répondre à ces besoins ou pour respecter les exigences de la loi.

Communication à des tiers

Les sociétés d'IGM peuvent communiquer des renseignements personnels à leurs sociétés affiliées et fournisseurs externes dans le but de remplir leurs obligations envers les clients.

Les sociétés d'IGM demeurent responsables des renseignements personnels confiés à des tiers et doivent protéger ces renseignements au moyen de contrats visant à assurer des niveaux comparables de protection fournis par IGM.

S'il existe un doute au sujet de la possibilité de communiquer des renseignements personnels, le personnel d'IGM devrait consulter l'agent de la protection des renseignements personnels désigné avant de communiquer des renseignements.

Conservation

Les sociétés d'IGM conservent les renseignements personnels pendant la période prescrite par la loi et conformément à la Politique de conservation des documents d'IGM. Les renseignements personnels qui ne sont plus requis en vertu de la Politique doivent être détruits, effacés ou rendus anonymes de manière sécuritaire.

Sixième principe 6 – Exactitude

Les renseignements personnels recueillis doivent être exacts, complets et aussi à jour qu'il le faut pour répondre aux besoins auxquels ils sont destinés.

Les sociétés d'IGM confirment ou demandent des mises à jour des renseignements personnels auprès des clients ou d'autres intervenants autorisés, au besoin. On peut demander aux clients de vérifier et de mettre à jour régulièrement leurs renseignements Connaître son client et les courtiers externes peuvent confirmer et/ou modifier les renseignements personnels des investisseurs dans les fonds.

Septième principe – Mesures de sécurité

Les renseignements personnels doivent être protégés par des mécanismes de sécurité qui tiennent compte du degré de confidentialité de l'information. Les mesures de sécurité doivent assurer la protection contre la perte, le vol, l'accès non autorisé, l'utilisation, la communication, la copie ou la modification des renseignements personnels, peu importe sous quelle forme ils sont contenus.

Les sociétés d'IGM utilisent diverses méthodes pour protéger les renseignements personnels, notamment :

- **Mesures physiques** – limiter l'accès aux bureaux ou aux zones dans lesquels des renseignements personnels sont accessibles et verrouiller les classeurs.

- **Mesures organisationnelles** – utiliser des autorisations d'accès, accorder l'accès aux renseignements uniquement s'ils sont requis pour des raisons professionnelles, et évaluer périodiquement si les autorisations d'accès ou l'utilisation des applications liées aux renseignements personnels sont toujours requises.

- **Mesures technologiques** – utiliser des mots de passe, le chiffrement des données et des pare-feu, et mettre en place des normes et une supervision efficaces.

- **Mesures contractuelles** – veiller à ce que les contrats avec des fournisseurs de services externes contiennent des dispositions visant la protection des renseignements personnels en leur possession et à ce que les normes soient satisfaites.

Sécurité de l'information

IGM a mis sur pied un Bureau de la sécurité informatique et a adopté à l'échelle de l'entreprise la Politique en matière de sécurité informatique et des normes connexes.

Formation

Tout le personnel d'IGM doit veiller à l'utilisation adéquate et à la protection de tous les renseignements personnels, et suivre une formation axée sur la protection des renseignements personnels et la sécurité informatique à leur entrée en service et périodiquement par la suite.

Gestion des atteintes à la vie privée

IGM a défini des directives à suivre pour signaler et gérer les atteintes à la vie privée. Veuillez consulter la **section 6** de la Politique et l'**Annexe** pour en savoir plus long.

Huitième principe – Transparence

Il faut faire savoir aux clients que les sociétés d'IGM disposent de politiques et de pratiques concernant la gestion des renseignements personnels, et ces politiques doivent être aisément accessibles et faciles à comprendre.

Les sociétés d'IGM affichent publiquement leurs avis de protection des renseignements personnels sur leurs sites Web qui incluent les renseignements suivants :

- Nom ou titre et adresse de la personne responsable des politiques et pratiques de la société d'IGM à qui les plaintes ou les demandes de renseignement peuvent être adressées;
- Façons dont les clients peuvent obtenir l'accès à leurs renseignements personnels;
- Description des types de renseignements personnels recueillis, utilisés et conservés; et
- Description des renseignements personnels qui sont communiqués à des sociétés affiliées et à des fournisseurs de services externes.

Les coordonnées de l'agent de la protection des renseignements personnels sont affichées pour chaque société d'IGM comme suit :

Société d'IGM	**Courriel de la personne-ressource**
Placements Mackenzie (CFM)	privacy@mackenziefinancial.com
IG Gestion de patrimoine (SFGI, VMGI, SAIGI et CFGI)	privacy-IG@ig.ca
Investment Planning Counsel (Services de portefeuille Counsel, IPCIC, IPCSC)	privacy@ipcc.ca

À leur demande, les clients doivent obtenir des renseignements sur les politiques et pratiques d'IGM concernant la protection des renseignements personnels; cette information se trouve dans les avis de protection des renseignements personnels affichés sur les sites de chacune des sociétés d'IGM.

Neuvième principe – Accès aux renseignements personnels

Les clients ont le droit de demander l'accès aux renseignements personnels qu'une société d'IGM détient à leur sujet. Ils ont aussi le droit de contester l'exactitude et l'intégralité des renseignements et d'y faire apporter les corrections appropriées.

Demandes d'accès à des renseignements personnels

Les demandes des clients concernant l'accès à leurs renseignements personnels, tels que des copies de leur dossier, doivent être faites par écrit. Sur demande, les clients doivent être informés de l'existence et de l'utilisation de leurs renseignements personnels et doivent y avoir accès dans les 30 jours suivant leur demande.

Le délai de traitement des demandes d'accès peut être prolongé pendant un maximum de 30 jours additionnels si :

- L'envoi d'une réponse dans les 30 jours civils aurait pour effet de nuire aux activités de la société d'IGM de manière déraisonnable;
- La société d'IGM a besoin d'un délai supplémentaire pour effectuer des consultations; ou

- La société d'IGM a besoin de plus de temps pour convertir les renseignements personnels du client en un autre format.

Seul l'agent désigné de la protection des renseignements personnels peut prendre la décision de prolonger un délai de traitement, et la société d'IGM doit aviser le client de la prolongation dans les 30 jours suivant la réception de la demande et l'informer de son droit de porter plainte au Commissariat à la protection de la vie privée du Canada et/ou au commissaire provincial à la protection de la vie privée.

Répondre aux demandes d'accès

À la réception d'une demande d'accès à des renseignements personnels, le personnel d'IGM suivra les directives établies à cet égard et énoncées dans l'**Annexe**.

Les renseignements demandés doivent être fournis au client dans un format compréhensible pour eux. Par exemple, des explications doivent être fournies au sujet des abréviations, codes et acronymes utilisés pour consigner les renseignements personnels.

Corriger des renseignements personnels

Si une personne démontre que les renseignements sont inexacts ou incomplets, les sociétés d'IGM corrigeront les renseignements personnels dans les meilleurs délais et, le cas échéant, les transmettront aux fournisseurs de services externes autorisés.

Dixième principe – Possibilité de porter plainte à l'égard du non-respect des principes

Il est possible pour un client de contester la conformité d'IGM aux principes relatifs à l'équité dans le traitement de l'information en s'adressant à l'agent de la protection des renseignements personnels de la société d'IGM.

IGM mènera une enquête sur toutes les plaintes concernant la protection des renseignements personnels et y répondra, conformément aux directives énoncées à ce sujet dans l'**Annexe**.

S'il s'avère qu'une plainte est fondée, IGM prendra les mesures adéquates, y compris, si nécessaire, la modification de ses politiques, procédures et pratiques.

6. Gestion des atteintes à la vie privée

Une atteinte aux mesures de sécurité visant les renseignements personnels, ou une atteinte à la vie privée, est définie comme toute forme d'accès non autorisé à des renseignements personnels ou toute communication de renseignements personnels, que le geste soit intentionnel ou non.

En voici des exemples :

- Un client a reçu le relevé de compte d'un autre client et l'a ouvert par erreur;
- Une télécopie ou un courriel contenant les renseignements personnels d'un client a été transmis à la mauvaise personne; et
- Une personne a accédé en ligne aux renseignements personnels d'un client sans autorisation.

Une société d'IGM ou un fournisseur de services externe agissant au nom de la société d'IGM peut être responsable d'une atteinte à la vie privée. Dans les deux cas, la société d'IGM est responsable de la gestion des atteintes à la vie privée.

Mesures à prendre en cas d'atteinte à la vie privée

Advenant une atteinte à la vie privée, il est important de prendre des mesures rapidement pour gérer et atténuer les risques potentiels de préjudice grave à l'endroit des clients concernés, entre autres :

- **Limiter la portée de l'atteinte** – Selon les circonstances, on peut y arriver en récupérant les documents, en veillant à ce que les données soient supprimées ou détruites de façon permanente, ou en corrigeant les défaillances du système, le cas échéant.
- **Évaluer et atténuer les risques pour les clients concernés** – Mener une évaluation pour déterminer si l'atteinte pose un risque réel de préjudice grave à l'endroit des clients et atténuer ces risques par les moyens appropriés, tels que signaler les comptes touchés, changer les numéros de compte, ou offrir au client l'option de surveillance du crédit, le cas échéant.
- **Informer les clients touchés –** Les avis aux clients doivent inclure les renseignements requis en vertu de la LPRPDE.
- **Déclarer les atteintes –** S'il est établi que l'atteinte pose un risque réel de préjudice grave, il faut la déclarer au commissaire fédéral à la protection de la vie privée ou au commissaire provincial, le cas échéant.
- **Prendre des mesures préventives** – Exécuter une analyse des causes profondes et prendre les mesures requises pour empêcher que la situation ne se reproduise.

Risque réel de préjudice grave

Le « préjudice grave » comprend : les lésions corporelles; l'humiliation; le dommage à la réputation ou aux relations; la perte d'un emploi, d'occasions d'affaires ou de relations professionnelles; la perte financière ou de biens; le vol d'identité; ou l'effet négatif sur les dossiers de crédit.

Les critères permettant de déterminer s'il existe un risque réel de préjudice grave comprennent le caractère confidentiel des renseignements personnels et la probabilité d'utilisation malveillante de ces renseignements.

S'il est raisonnable dans les circonstances de croire qu'il existe un risque réel de préjudice grave pour un individu, par suite de la perte ou de la communication de ses renseignements personnels ou de l'accès non autorisé à ceux-ci, l'atteinte est visée par les exigences de notification énoncées dans la **section 7** de la Politique.

7. Exigences de notification obligatoire de l'atteinte

Notifications aux clients touchés

En cas d'atteinte à la vie privée, IGM a l'obligation d'aviser les clients touchés dans les meilleurs délais s'il est établi qu'il existe un risque réel de préjudice grave pour la personne. Les notifications au client doivent comporter ce qui suit :

- une description des circonstances entourant l'atteinte;
- la date de l'atteinte ou la période de temps, précise ou approximative, pendant laquelle l'atteinte s'est produite;
- une description des renseignements personnels qui ont été communiqués;
- une description des mesures prises par IGM pour atténuer le risque de préjudice;
- une description des mesures que le client pourrait prendre pour atténuer le risque de préjudice; et
- les coordonnées des personnes-ressources pouvant fournir des renseignements au client à propos de l'atteinte.

Si une notification directe est susceptible d'aggraver le préjudice pour la personne concernée ou de causer une contrainte excessive à IGM, ou si IGM ne possède pas les coordonnées des personnes touchées, IGM peut choisir de transmettre un avis indirect au moyen d'une communication publique ou par un moyen semblable s'il est raisonnable de croire que l'avis pourra être reçu par les personnes touchées.

Notification au(x) commissaire(s) à la protection de la vie privée

IGM doit aviser le commissaire fédéral à la protection de la vie privée et/ou le commissaire provincial, le cas échéant, dans un délai raisonnable, s'il est établi qu'une violation des renseignements personnels pose un risque réel de préjudice grave pour les clients touchés.

L'avis au(x) commissaire(s) à la protection de la vie privée doit être fait par écrit et contenir les renseignements requis, et les formulaires prescrits doivent être utilisés au besoin.

L'avis au(x) commissaire(s) à la protection de la vie privée, le cas échéant, sera traité par l'agent désigné de la protection des renseignements personnels en collaboration avec le chef de la conformité de la société touchée.

Registre des atteintes à la vie privée

IGM doit tenir un registre de toutes les atteintes à la vie privée pendant au moins deux ans après la date de détection de l'atteinte, y compris les atteintes qui ne posent pas de risque réel de préjudice grave. Les registres doivent inclure la date ou la date estimée de l'atteinte, une description des circonstances

de l'atteinte, la nature des renseignements personnels communiqués, et une note selon laquelle les personnes touchées et le(s) commissaire(s) ont été avisés ou non.

Les registres doivent contenir des précisions suffisantes pour que le(s) commissaire(s) à la protection de la vie privée puisse(nt) déterminer si les normes adéquates d'évaluation du risque réel de préjudice grave ont été satisfaites.

8. Lois sur la protection des renseignements personnels pour les non-résidents

IGM et les sociétés d'IGM ont leurs sièges sociaux au Canada et y exercent leurs activités, à l'exception de :

- Mackenzie Investments Europe Limited (« MIEL ») située à Dublin, en Irlande;
- Mackenzie Investments Asia Limited (« MIAL ») située à Hong Kong;
- Mackenzie Investment Corporation (« MIC ») située à Boston, aux États-Unis.

Ces sociétés d'IGM exercent des activités de gestion d'actifs institutionnels et n'offrent pas de produits ni de services aux investisseurs individuels.

Même si les sociétés d'IGM à l'étranger nommées ci-haut ne traitent pas avec les investisseurs individuels, certaines des sociétés canadiennes d'IGM peuvent avoir des clients à l'extérieur du Canada.

Règlement général sur la protection des données (RGPD)

En 2018, l'Union européenne (UE) a adopté le RGPD, un règlement portant sur la protection de la vie privée qui régit le traitement des renseignements personnels des résidents de l'UE. Les principes du RGPD correspondent dans l'ensemble aux principes et exigences de la LPRPDE. Comme la LPRPDE, le RGPD définit les données personnelles, énonce des principes concernant les données fondamentales, régit les droits des particuliers, et exige une formation au moment de l'embauche et annuellement par la suite.

Si IGM constate une atteinte à la vie privée qui touche des clients de l'UE, les procédures en cas d'atteinte à la vie privée énoncées dans l'**Annexe** seront suivies, et une évaluation sera effectuée pour déterminer si l'atteinte pose un risque probable et grave pour les droits et libertés de clients résidents de l'UE. S'il est établi que l'atteinte pose effectivement un tel risque, IGM avisera les autorités responsables appropriées de l'UE conformément au RGPD.

États-Unis

Les États-Unis (É.-U.) disposent de diverses lois fédérales et d'état régissant la protection de la vie privée, qui exigent que les sociétés adoptent et mettent en place des politiques et procédures raisonnablement conçues pour protéger la vie privée et la confidentialité des renseignements personnels.

Si une société d'IGM constate une atteinte à la vie privée touchant des clients résidents des É.-U., les procédures en cas d'atteinte à la vie privée énoncées dans l'**Annexe** seront suivies.

9. Examen de la Politique et compte rendu de la Conformité

Le Service de la conformité d'IGM doit coordonner, chaque année civile, l'examen de la Politique, et les services de conformité des sociétés d'IGM doivent soumettre la Politique à l'approbation de leur conseil d'administration respectif.

Le Service de la conformité de chaque société d'IGM doit faire rapport de toute dérogation à la Politique à son comité de surveillance de la conformité et à son conseil d'administration, au moins une fois par trimestre.

10. Politiques secondaires connexes

Voici des politiques secondaires connexes.

- Politique anti-pourriel d'IGM
- Politique de conservation des documents d'IGM

11. Agents de la protection des renseignements personnels d'IGM

Pour plus de renseignements sur la Politique, le personnel d'IGM devrait communiquer avec son agent désigné de la protection des renseignements personnels à l'adresse courriel indiquée plus bas.

Société d'IGM	**Courriel de la personne-ressource**
Placements Mackenzie (CFM)	privacy@mackenziefinancial.com
IG Gestion de patrimoine (SFGI, VMGI, SGIIG, SAIGI et CFGI)	privacy-IG@ig.ca
Investment Planning Counsel (IPCIC, IPCSC et Services de portefeuille Counsel)	privacy@ipcc.ca

Annexe

A. Procédures en cas d'atteinte à la vie privée

Une atteinte à la vie privée implique l'accès à des renseignements personnels ou la communication de renseignements personnels sans autorisation, que ce soit par erreur ou volontairement. Si une atteinte à la vie privée est considérée comme posant un risque réel de préjudice grave aux clients touchés, il est obligatoire d'en aviser les clients concernés et de la signaler au(x) commissaire(s) à la protection de la vie privée concerné(s). L'agent de la protection des renseignements personnels effectuera une évaluation pour déterminer si l'atteinte doit être déclarée au(x) commissaire(s) à la protection de la vie privée.

Voici quelques exemples d'atteinte à la vie privée :

- Vol ou perte d'ordinateur portatif contenant des renseignements personnels sur les clients;
- Vol ou perte de documents concernant les clients tels que des dossiers clients;
- Envoi d'un courriel contenant des renseignements personnels à la mauvaise personne;
- Envoi de documents sur un client au mauvais destinataire.

En cas d'atteinte à la vie privée, il importe d'agir dans les meilleurs délais et de manière responsable pour prendre des mesures visant à atténuer les risques et les incidences pour les personnes concernées.

Advenant une atteinte à la vie privée, les mesures suivantes doivent être adoptées :

Étapes	Mesures
1	• Limitez immédiatement l'atteinte à la vie privée pour prévenir l'aggravation du risque et les préjudices, par exemple en récupérant des documents, en supprimant une application ou en mettant fin à l'envoi ou à la distribution de documents; et • Informez votre directeur ou gestionnaire.
2	• Transmettez un sommaire de l'atteinte à la vie privée par courriel à la boîte de votre responsable de protection des renseignements personnels (voir les coordonnées de contact ci-dessous). • Si vous croyez que l'atteinte peut attirer l'attention des médias ou des poursuites judiciaires, communiquez avec votre agent de la protection des renseignements personnels sans délai.
3	• Suivez les directives de l'agent de la protection des renseignements personnels pour limiter les conséquences de l'incident (c.-à-d. aviser les clients touchés, communiquer avec les destinataires pour faire supprimer les renseignements personnels transmis par erreur).

B. Procédure de gestion des plaintes concernant les renseignements personnels

Le client qui estime que ses renseignements personnels ont reçu un traitement inadéquat peut déposer une plainte. Le client peut porter plainte dans les cas suivants :

- s'il pense que ses renseignements personnels ont été indûment recueillis, utilisés ou communiqués;
- si on lui a refusé l'accès à ses renseignements personnels; ou
- s'il juge que le délai pour lui donner accès à ses renseignements personnels a été déraisonnable.

Advenant une plainte concernant les renseignements personnels, il faut prendre les mesures qui suivent :

Étapes	Mesures
1	• À la réception d'une plainte, avisez immédiatement votre directeur/gestionnaire.
2	• Examinez la plainte pour déterminer si elle est reliée à la vie privée et/ou aux renseignements personnels. • Avisez l'agent de la protection des renseignements personnels si la plainte concerne la vie privée et les renseignements personnels. • Si la plainte n'est pas reliée à la vie privée ou aux renseignements personnels, transmettez la plainte à l'équipe responsable des plaintes et/ou des enquêtes.
3	• Faites enquête sur la plainte et réglez la question avec l'aide de votre directeur et d'autres intervenants clés internes dans un délai de 30 jours suivant la réception.
4	• Répondez par écrit à la personne ayant porté plainte dans un délai de 30 jours, en lui donnant une réponse à ses questions. • Dans votre réponse, précisez-lui que si elle n'est pas satisfaite, sa plainte peut être transmise à l'agent de la protection des renseignements personnels.
5	• Si la plainte est transmise à l'agent de la protection des renseignements personnels, ce dernier effectuera une enquête rigoureuse et communiquera directement avec la personne concernée. Tous les efforts seront mis en œuvre pour corriger la situation. • Si la personne ayant porté plainte n'est pas satisfaite de la réponse de l'agent de la protection des renseignements personnels, elle peut déposer une plainte officielle auprès du Commissariat à la protection de la vie privée du Canada et/ou auprès du commissariat à la vie privée de sa province. • L'agent de la protection des renseignements personnels continuera de gérer le dossier de plainte jusqu'à la résolution.

C. Procédure de demande d'accès aux renseignements

En vertu de la loi, les clients peuvent demander à voir les renseignements personnels contenus dans leurs dossiers, notamment les détails sur les comptes et les données clients. Toutes les demandes d'accès aux renseignements doivent être soumises par écrit par le client ou par son représentant légal. IGM doit y répondre dans un délai de 30 jours civils après la réception.

Voici la marche à suivre à la réception d'une demande d'accès aux renseignements :

Étapes	**Mesures**
1	• Accusez réception de la demande en précisant qu'une réponse écrite sera fournie dans les 30 jours. • Avisez votre agent de la protection des renseignements personnels. • Réunissez les renseignements auxquels vous avez accès.
2	• Faites appel aux autres services internes, au besoin, pour obtenir les renseignements auxquels ils ont accès.
3	• Supprimez les renseignements sans rapport avec l'auteur de la demande, par exemple : o les renseignements protégés par le secret professionnel; o les renseignements non publics au sujet d'IGM; ou o les renseignements produits par suite d'un processus de résolution de litige.
4	• Fournissez à l'auteur de la demande des renseignements dans un format facilement accessible et compréhensible.
5	• Si vous pensez ne pas être en mesure de répondre à la demande d'accès dans un délai de 30 jours, communiquez avec votre agent de la protection des renseignements personnels le plus tôt possible. • Si vous avez des questions au sujet d'une demande d'accès, communiquez avec votre agent de la protection des renseignements personnels.