Ligne directrice sur le traitement des atteintes à la vie privée

Ce guide contient un sommaire d'une page puis présente la marche à suivre en cas d'une atteinte à la vie privée.

Incident ou atteinte 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'utilisation ou de l'accès non autorisé à de tels renseignements découlant d'une atteinte aux mesures de sécurité ou lorsque des renseignements personnels sont conservés d'une façon non conforme à la législation applicable en matière de protection de la vie privée (p. ex. lorsque des renseignements personnels sont conservés même s'ils ne sont plus nécessaires aux fins pour lesquelles ils ont été collectés) ou toute autre violation de la protection des renseignements personnels non conforme à la législation applicable en matière de protection de la vie privée.

Terminologie de l'évaluation :

Il peut y avoir une atteinte à la vie privée même si un seul client est touché et même si les renseignements personnels dévoilés semblent anodins. Toutes les atteintes doivent faire l'objet d'une évaluation afin de déterminer le risque pour le client. Ces évaluations peuvent être qualifiées de risque réel de préjudice grave (RRPG) ou de risque de préjudice sérieux (RPS, semblable au RRPG), et seront désignées par le terme « évaluation » dans l'ensemble du présent document. Lorsque l'évaluation détermine que le risque est grave ou sérieux, l'atteinte doit être signalée au commissaire à la protection de la vie privée ou à la Commission d'accès à l'information (CAI) au Québec, selon le cas.

Pour les conseillers rattachés à la Canada Vie, le cabinet doit signaler toutes les atteintes à la Canada Vie, qui les évaluera et les signalera à la CAI, au besoin.

Marche à suivre

Maîtriser la situation :

- Déterminez ce qui se passe
- Mettez fin à l'atteinte (p. ex. récupérez le courriel, déconnectez l'appareil du serveur, changez les mots de passe, communiquez avec le Bureau des services technologiques des compagnies visées)

Enquêter :

- Déterminez les renseignements compromis
- Évaluez l'étendue de l'atteinte

Informer :

- Communiquez avec l'agent de conformité de l'entreprise, avec l'équipe Conformité des conseillers de la Canada Vie ou l'équipe Conformité des conseillers, Québec pour les clients de la Canada Vie, ou avec les autres compagnies visées
- Communiquez, le cas échéant, avec l'équipe de soutien TI ou le service de police

Évaluer et aviser :

- Effectuez une évaluation (étapes décrites ci-dessous dans la section Effectuer une évaluation) et si l'évaluation détermine que l'atteinte présente un risque important ou sérieux :
    - Informez les personnes touchées et mettez en œuvre des mesures correctives, au besoin (surveillance du crédit, ajout d'indicateurs aux comptes)
    - À l'extérieur du Québec – communiquez l'incident au Commissariat à la protection de la vie privée du Canada
    - Cabinets du Québec (p. ex. Canada Vie/conseiller constitué en société) – signalez l'atteinte à la CAI
    - Avisez les organismes de réglementation provinciaux, au besoin

Améliorer les contrôles :

- Examinez tous les processus, toutes les mises à jour du système, toutes les formations des employés
- Modifiez les processus requis pour éviter que des incidents ne se reproduisent

Consigner l'information :

- Indiquez et enregistrez toute information sur une atteinte à la vie privée
- Les cabinets du Québec doivent conserver un registre à jour des incidents liés à la protection des renseignements personnels pendant cinq ans, à compter de la date à laquelle ils ont été mis au courant de l'incident.
- Conservez les dossiers pendant 24 mois pour les pratiques des conseillers autres que les cabinets du Québec
- Utilisez la feuille Excel personnalisée pour vous aider à indiquer l'information

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

Une atteinte à la vie privée peut être voulue, accidentelle ou attribuable à des activités criminelles.

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 ont été envoyés au mauvais destinataire du 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 ou réelles sont immédiatement déclarées à l'agent de conformité de l'entreprise. L'agent de conformité de l'entreprise empêchera la divulgation des renseignements, évaluera la situation, corrigera la situation et contribuera à l'amélioration des mesures de contrôle afin d'éviter toute atteinte semblable à l'avenir.

Processus de confinement des atteintes

En cas d'atteinte à la vie privée touchant les renseignements des clients, (p. ex., cyberattaque, accès non autorisé aux données), communiquez avec :

- L'agent de conformité de l'entreprise
- Conformité des conseillers ou Conformité des conseillers, Québec pour les affaires de la Canada Vie
- Les autres compagnies visées

En plus des étapes décrites plus haut, suivez les étapes décrites ci-dessous.

Perte, vol ou piratage d'appareils électroniques

- Mobilisez l'équipe de soutien aux TI de l'entreprise
    - 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 chaque 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)

- Communiquez avec le service de police pour signaler le vol de documents.

Courriels ou courrier envoyés au mauvais destinataire

Courriel :

- Rappelez immédiatement le courriel.
    - Si ce n'est pas possible, communiquez avec le mauvais destinataire pour lui demander de confirmer par écrit qu'il a supprimé le courriel, qu'il ne l'a pas enregistré et ne l'a pas transféré à un autre destinataire.

Courrier :

- Demandez au mauvais destinataire de retourner le courrier ou confirmez que le courrier a été détruit de façon sécuritaire.

Cyberattaque

Une cyberattaque vise des ordinateurs ou des réseaux informatiques qui tentent d'exposer, de modifier, de désactiver, de détruire, de voler ou d'obtenir des informations au moyen d'un accès non autorisé à un actif ou d'utiliser cet actif sans autorisation.

- Mobilisez l’équipe de soutien aux TI de l’entreprise
- Communiquez avec le service de police

Rançongiciel

Un rançongiciel est un type de logiciel malveillant (maliciel) qui empêche les utilisateurs d’utiliser leurs systèmes ou en limite l’utilisation en verrouillant l’écran du système ou en verrouillant les dossiers d’un utilisateur jusqu’à ce qu’un montant (une rançon) soit payé.

- Mobilisez l’équipe de soutien aux TI de l’entreprise
- Communiquez avec le service de police

Processus de documentation

Commencez le processus de documentation de toute atteinte à la vie privée dès que cette atteinte a été décelée. Tous les dossiers d'atteinte à la vie privée doivent être conservés de façon sûre.

Au Québec, les conseillers rattachés à la Canada Vie (le cabinet) doivent aviser l'équipe Conformité des conseillers, Québec pour les affaires de la Canada Vie, immédiatement lorsqu'ils prennent connaissance de l'atteinte. Les cabinets du Québec doivent tenir à jour un registre des atteintes à la vie privée pendant cinq ans à partir du moment où ils ont pris connaissance de l'atteinte, puis fournir ce registre à la CAI sur demande.

Le ou les dossiers doivent être gardés dans un endroit sûr et comprendre ce qui suit :

- La date de l'atteinte
- La description des circonstances de l'atteinte
- Le nombre de personnes visées
- Les types de renseignements personnels en cause
- La sensibilité de l'information visée par l'atteinte
- La probabilité de l'utilisation à mauvais escient
- Les préjudices potentiels qui pourraient découler de l'atteinteUn indicateur pour confirmer :
  - Si l'atteinte a entraîné un risque grave ou sérieux pour la personne, et une explication quant à cette conclusion
  - Que la ou les personnes visées ont été avisées
  - La date de confirmation et d'avis visant le Commissariat à la protection de la vie privée pour ceux qui vivent à l'extérieur du Québec et qui sont touchés par l'atteinte
- Les mesures prises pour éviter que des atteintes semblables ne se reproduisent

- La date à laquelle le cabinet a été mis au courant de l'incident
- Si la description des renseignements personnels n'est pas fournie, indiquez pourquoi
- S'il existe un risque important ou sérieux - la date et la confirmation de l'avis à la CAI, les personnes visées et si des avis publics ont été publiés, ainsi que les raisons pour lesquelles cela a été fait

Un registre de suivi comprenant une liste de toutes les atteintes à la vie privée par région consignée à un seul endroit peut aussi être conservé. Les cabinets du Québec peuvent l'utiliser comme registre pour la CAI.

Effectuer une évaluation

Tous les incidents d'atteinte à la vie privée doivent être évalués pour déterminer s'ils ont posé un risque grave ou sérieux.

Pour déterminer s'il existe un risque grave ou sérieux, posez les questions suivantes :

- Les renseignements personnels visés par l'incident sont-ils de nature délicate?
    - Exemples de niveaux de la nature délicate des renseignements personnels : Élevé – NAS, renseignements bancaires et renseignements médicaux; faible – nom, adresse courriel, sexe, état matrimonial
- Les renseignements personnels ont-ils été obtenus de façon malveillante?
    - Les renseignements personnels obtenus au moyen d'un vol, d'une fraude ou du piratage d'un système sont plus susceptibles d'être utilisés à des fins malveillantes et représentent un risque élevé.
- Est-ce que cinq personnes ou plus sont visées?
    - Plus le nombre de personnes concernées est élevé, plus la probabilité d'une utilisation à mauvais escient est grande.
- Les renseignements n'ont-ils toujours pas été récupérés?
    - Si les renseignements personnels ne peuvent pas être récupérés rapidement, cela peut vouloir dire qu'ils ont été, qu'ils sont ou qu'ils seront utilisés à mauvais escient.
- Êtes-vous toujours en attente d'une confirmation indiquant que les renseignements personnels ont été détruits?
    - Si les renseignements personnels ne sont pas détruits par un mauvais destinataire, cela peut vouloir dire qu'ils ont été, qu'ils sont ou qu'ils seront utilisés à mauvais escient.
- L'incident découle-t-il d'un problème systémique?
    - Les problèmes systémiques peuvent entraîner d'autres incidents et augmenter les probabilités que les renseignements personnels soient utilisés à mauvais escient.
- S'est-il écoulé plus de 10 jours ouvrables entre la date de l'incident et la date de découverte de l'incident?
    - Un long délai avant la découverte de l'incident peut indiquer que le mauvais destinataire a eu le temps d'utiliser les renseignements personnels à mauvais escient.

Si vous avez répondu « non » à une des questions ci-dessus, la réponse à la question sur la détermination de l'existence d'un risque grave ou sérieux sera « non », et les niveaux de la nature délicate et la probabilité seront « faibles ». Allez à la section Amélioration des mesures de contrôle.

Si vous avez répondu « Oui » à l'une des questions ci-dessus, vous devrez déterminer le niveau de la nature délicate des renseignements personnels (faible ou élevé) et la probabilité de l'utilisation à mauvais escient. Tenez compte 1) de la sensibilité des renseignements personnels atteints; 2) des conséquences envisagées pour les personnes touchées en cas d'utilisation inappropriée de leurs renseignements personnels atteints; et 3) de la probabilité que les renseignements personnels soient utilisés de façon inappropriée.

Si vous considérez que les renseignements personnels qui ont fait l'objet de l'atteinte sont de nature « très délicate » et que la probabilité que ces renseignements personnels soient utilisés à mauvais escient est aussi « élevée », il existe un risque grave ou sérieux pour les personnes touchées; passez à la section suivante.

- Pour les affaires de la Canada Vie, vous pouvez communiquer avec l'équipe Conformité des conseillers ou avec l'équipe Conformité des conseillers, Québec pour obtenir un soutien additionnel au besoin.

Déclaration obligatoire des atteintes à la vie privée en vertu des lois provinciales en matière de protection des renseignements personnels ou de la LPRPDE

- S'il est déterminé que l'incident présente un risque grave ou sérieux, les personnes visées doivent être avisées et selon l'emplacement des personnes concernées, il faut faire une déclaration au Commissariat à la protection de la vie privée du Canada (le « Commissariat ») et aux autres organismes de réglementation provinciaux applicables, et ce, dès que possible et même s'il n'y a qu'une seule personne visée.
- L'entreprise doit également informer de l'incident toute autre organisation ou entreprise qui pourrait atténuer le préjudice aux personnes concernées (p. ex., ajouter un indicateur aux comptes des clients). Pour les clients de la Canada Vie, communiquez avec l'équipe Conformité des conseillers ou avec l'équipe Conformité des conseillers, Québec.

Avis aux personnes concernées

Un avis doit être fourni aux personnes concernées relativement à une atteinte aux mesures de protection des renseignements personnels. Au Québec, le cabinet doit s'assurer qu'un avis a été fourni.
L'avis doit contenir les informations suivantes :

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 (p. ex., suivi du crédit, ajout d'indicateurs aux comptes)
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
f. Les coordonnées permettant aux personnes concernées de se renseigner davantage au sujet de l'atteinte

Avis aux organismes de réglementation

- Cabinets du Québec – Envoyez un avis à la CAI en téléchargeant le Formulaire de déclaration d'un incident de sécurité portant atteinte à des renseignements personnels du site Web de la CAI.

Amélioration des mesures de contrôle

Passez en revue tous les processus, toutes les mises à jour du système, toutes les formations des employés, puis apportez des améliorations au besoin afin d’éviter que les incidents ne se reproduisent.