GROUPE FINANCIER

Politique et procédure pour la protection des renseignements personnels

GROUPE FINANCIER UNICO INC.(GFU), nous prenons l'engagement de protéger la confidentialité des renseignements personnels que vous nous confiez dans le cadre de nos activités. Nous agissons toujours en conformité avec les lois applicables en matière de protection de la vie privée.

Lorsque la présente Politique fait référence à GROUPE FINANCIER UNICO INC., elle fait aussi référence à nos autres sociétés affiliées. Notre Politique s'applique autant aux clients de GFU, qu'aux conseillers qui recourent à nos services.

1. Préoccupations et demandes de renseignements ou requêtes générales

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

Le directeur de la conformité fait suivi toutes les préoccupations, demandes de nature générale ou requêtes liées à la confidentialité et aux produits et services de la compagnie au président de GFU

2. Demandes de clients visant à accéder aux renseignements personnels

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

Toute demande d'accès d'un client à ses renseignements personnels consignés dans les dossiers client de GFU est envoyée au directeur de la conformité afin qu'il réponde à la demande du client. La date et les modalités de la demande sont consignées jusqu'à ce qu'elle soit exécutée. Le directeur de la conformité aidera le client à préparer sa demande d'accès, au besoin. Les renseignements sont fournis au client le plus rapidement possible et au plus tard dans les 30 jours suivant la réception de la demande, dans un format technologique couramment utilisé.

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

2.1 Décisions automatisées

Si GFU met en place une technologie de prise de décision automatisée, à la demande du client, il lui fera savoir, au plus tard au moment où il l'informe de la décision, quels renseignements personnels ont été utilisés pour prendre la décision et lui expliquera, dans un langage facile à comprendre, comment la décision a été prise. Le client conserve le droit de consulter et de corriger tout renseignement erroné.

2.2 Usage à mauvais escient des renseignements personnels

Toutes personnes contactées doivent signaler sans délai tout usage à mauvais escient de renseignements personnels ou toute atteinte possible aux mesures de sécurité quant aux produits et aux services au Directeur de la conformité de GFU.

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

Une atteinte à la vie privée survient lors de la divulgation ou de l'utilisation non autorisée de renseignements personnels, de l'accès non autorisé à de tels renseignements ou de la perte de renseignements personnels découlant d'une atteinte aux mesures de sécurité. Une atteinte à la vie privée comprend également toute autre atteinte à la protection des renseignements personnels qui n'est pas conforme à la législation relative à la protection des renseignements personnels, comme lorsque des renseignements personnels

sont conservés même s'ils ne sont plus nécessaires aux fins pour lesquelles ils ont été recueillis.

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.

Toutes les atteintes doivent faire l'objet d'une évaluation afin de déterminer le risque pour le client.

Terminologie de l'évaluation : Les 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 à la Commission d'accès à l'information (OPC) au Québec et/ou au Commissariat fédéral à la protection de la vie privée du Canada (CPVP) et aux commissaires provinciaux à la protection de la vie privée en dehors du Québec, selon le cas, tous étant désignés par le terme « le commissaire ».

2.3.1 Politique et procédure

Les atteintes présumées ou réelles, les plaintes ou toutes les préoccupations reliées à un problème de confidentialité, peu importe qu'elles touchent une personne ou un fournisseur, sont immédiatement déclarées au directeur de la conformité de GFU. Le directeur de la conformité de GFU 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.

2.3.2 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 : le directeur de la conformité
- Le directeur de la conformité communique avec l’agent de conformité de la pratique et de la conformité de l’assureur et/ou partenaire.

2.3.2.1 Perte, vol ou piratage d’appareils électroniques

- GFU effectuera un balayage des ordinateurs afin de détecter tout logiciel malveillant avant d’accéder de nouveau aux systèmes.
- Communiquera immédiatement avec l’équipe de soutien technologique de chaque compagnie concernée pour demander la modification des mots de passe.
- Communiquera avec le service de police pour déposer une plainte.
- Modifiera les mots de passe des autres systèmes (p. ex. service bancaire en ligne).

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

- GFU communiquera avec le service de police pour signaler le vol de documents.

2.3.2.3 Courriels ou courrier envoyés au mauvais destinataire

- GFU rappellera immédiatement le courriel.
- Si ce n’est pas possible, communique avec le mauvais destinataire pour lui demander de confirmer par écrit qu’il a supprimé le courriel et l’a effacé de sa boîte Éléments supprimés, qu’il ne l’a pas enregistré et ne l’a pas transféré à un autre destinataire.
- Demandez au mauvais destinataire de retourner le courrier ou confirmez que le courrier a été détruit de façon sécuritaire (p. ex., déchiquetage).

2.3.2.4 Cyberattaques

- 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.
- Mobilise l'équipe de soutien aux TI de la pratique
- Communique avec le service de police

2.3.2.5 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.
- Mobilise l'équipe de soutien aux TI de la pratique
- Communique avec le service de police pour signaler l'incident et coopérer à l'enquête
- Déconnecte immédiatement du réseau les appareils visés par un rançongiciel
- Ne rien effacer sur de nos appareils (ordinateurs, serveurs, etc…)
- Examiner le rançongiciel et déterminer comment il a infecté l'appareil.
- Une fois le rançongiciel supprimé, une analyse complète du système doit être effectuée à l'aide d'un antivirus, d'un anti-maliciel et de tout autre logiciel de sécurité le plus récent disponible afin de confirmer qu'il a été supprimé de l'appareil
- Si le rançongiciel ne peut être supprimé de l'appareil (souvent le cas avec les programmes malveillants furtifs) l'appareil doit être réinitialisé au moyen des supports ou des images d'installation d'origine. Attention avant de procéder à la réinitialisation à partir de supports/images de sauvegarde, vérifier qu'ils ne sont pas infectés par des maliciels
- Si les données sont critiques et doivent être restaurées, mais ne peuvent être récupérées à partir de sauvegardes non affectées, rechercher les outils de déchiffrements disponibles sur **nomoreransom.org**
- La politique est de ne pas payer la rançon, sous réserve des enjeux en cause. Il est également fortement recommandé de faire appel aux services d'un chef de projet expert en cyberattaques (breach coach)

- Protéger les systèmes pour éviter toute nouvelle infection en mettant en œuvre des correctifs ou des routines pour empêcher toute nouvelle attaque

2.4 Processus de documentation

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

Au Québec, GFU doit tenir à jour un registre de toutes les atteintes à la vie privée pendant cinq ans à partir du moment où il a pris connaissance de l'atteinte et être prêt à fournir ce registre à la Commission d'accès à l'information (CAI) sur demande.

À l'extérieur du Québec, conservez les dossiers sur toutes les atteintes à la vie privée pendant 24 mois. La pratique devrait être en mesure de fournir les dossiers au commissaire ou à d'autres organisations sur demande.

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

- Date de l'atteinte
- Description des circonstances de l'atteinte
- Nombre de personnes visées
- Types de renseignements personnels en cause
- Sensibilité de l'information visée par l'atteinte
- Probabilité de l'utilisation à mauvais escient
- Préjudice potentiel qui pourrait découler de l'atteinte
- Un 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 commissaire pour ceux qui vivent à l'extérieur du Québec et qui sont touchés par l'atteinte
- Mesures prises pour éviter que des atteintes semblables se reproduisent – considérez les éléments suivants :

    - Quelle est la cause fondamentale de l'atteinte à la vie privée?

    - Quelles sont les mesures de contrôle qui ont échoué à empêcher l’atteinte à la vie privée?
    - De nouveaux processus ou mesures de contrôle doivent-ils être instaurés?
    - Des processus ou mesures de contrôle existants doivent-ils être améliorés ou modifiés?
    - Existe-t-il des lacunes ou des vulnérabilités dans les contrôles de sécurité qui ont besoin d’être résolues?
    - La formation doit-elle être renforcée ou une nouvelle formation doit-elle être créée et donnée?
- GFU doit aussi consigner les renseignements suivants :
- Date à laquelle GFU a été mis au courant de l’incident
- Si la description des renseignements personnels n’est pas fournie, indiquez pourquoi
- Si on détermine qu’il y a un risque grave ou sérieux – la date et la confirmation de l’avis à la CAI et aux personnes touchées et si des avis publics ont été émis et les raisons de l’avoir 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. GFU peut s’en servir comme registre pour les besoins de la CAI.

2.5 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 5 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 le 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 une des questions ci-dessus, vous devrez déterminer le niveau (faible ou élevé) de la nature délicate des renseignements personnels et la probabilité qu'ils soient utilisés à mauvais escient en tenant compte 1) de la nature délicate des renseignements personnels qui ont fait l'objet de l'atteinte; 2) des conséquences envisagées

pour les personnes touchées en cas d'utilisation à mauvais escient de leurs renseignements personnels qui ont fait l'objet de l'atteinte; et 3) de la probabilité que les renseignements personnels soient utilisés à mauvais escient.

2.6 Déclaration obligatoire des atteintes à la vie privée en vertu des lois provinciales en matière de protection des renseignements personnels ou de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)

- Si GFU détermine que l'incident présente un risque grave ou sérieux, les personnes visées doivent être avisées, si cela n'interfère pas avec une enquête officielle, et selon l'emplacement des personnes concernées, il faut faire une déclaration au CAI (au Québec) et au commissaire, et ce, dès que possible et même s'il n'y a qu'une seule personne visée.
- GFU doit également informer de l'incident toute autre organisation ou entreprise qui pourrait atténuer le préjudice aux personnes.

2.6.1 Avis aux personnes concernées

Le cas échéant, un avis sur l'atteinte aux mesures de protection des renseignements personnels sera fourni par GFU aux personnes concernées et il doit renfermer les éléments suivants :

1. une description des circonstances de l'atteinte;
2. 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;
3. une description des renseignements personnels touchés, dans la mesure où il est possible de le déterminer;
4. une description des mesures que la pratique a mises en place pour réduire les risques de préjudice découlant de l'atteinte;
5. une description des mesures que pourraient prendre les personnes concernées pour réduire les risques de préjudice découlant de l'atteinte ou atténuer ces préjudices; et
6. les coordonnées permettant aux personnes concernées de se renseigner davantage au sujet de l'atteinte.
7. **2.6.2 Avis aux organismes de réglementation dans le cas des atteintes considérées comme des RRPG/RPS par GFU**

-

- Envoie un avis au Commissariat à la protection de la vie privée du Canada (fédéral) au moyen du formulaire Rapport d'atteinte à la LPRPDE.
- Envoie un avis à la Commission d'accès à l'information (CAI) en téléchargeant le Formulaire de déclaration d'un incident de sécurité portant atteinte à des renseignements personnels du site Web de la CAI.
- Colombie-Britannique – La loi recommande de faire rapport au Commissariat à la protection de la vie privée s'il y a un risque réel de préjudice grave. Pour savoir s'il vous faut produire un avis, reportez-vous au formulaire Privacy Breach Checklist (Rapport préliminaire pour évaluer les atteintes à la vie privée) de la Colombie-Britannique.
- Envoie un avis au Office of the Information and Privacy Commissioner of Alberta (commissariat à l'information et à la protection de la vie privée de l'Alberta) au moyen de son formulaire de déclaration d'atteinte à la vie privée.
- https://oipc.ab.ca/
-
- **2.7 Amélioration des mesures de contrôle**
- GFU passera 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. Comme cela est décrit à la section 2.4 « Processus de documentation », évaluez les mesures de contrôle qui peuvent être améliorées pour réduire au minimum les risques futurs et instaurez les nouvelles mesures de contrôle nécessaires pour faire face aux risques.
- Pour toute question ou préoccupation concernant notre politique de traitement des renseignements personnels ou la façon dont nous utilisons vos renseignements personnels, veuillez nous écrire au Directeur de conformité.
- *Vous pouvez consulter en tout temps la politique applicable sur le présent site. La date de la dernière mise à jour de la présente politique de confidentialité est le 1er Août 2025.*
-
-