



**Chambre
de la sécurité
financière**

RÈGLES RELATIVES À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Approuvé par :

Comité sur l'accès à l'information et la protection des
renseignements personnels de la CSF

ENTRÉE EN VIGUEUR :

2023-09-22

DERNIÈRE MISE À JOUR :

DATE D'ABROGATION :

RÈGLES RELATIVES À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Introduction

Dans le cadre de sa mission, la Chambre de la sécurité financière (la « **CSF** ») recueille et utilise des renseignements personnels. La CSF est un organisme assujéti à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ c. A-2.1 (la « **Loi sur l'accès** »). En conformité avec la Loi sur l'accès, elle doit assurer la protection des renseignements personnels qu'elle détient.

Les présentes Règles relatives à la protection des renseignements personnels (les « **Règles** ») ont été approuvées et recommandées par le Comité sur l'accès à l'information et la protection des renseignements personnels de la CSF.

1. Traitement des renseignements personnels

La CSF met en place les bonnes pratiques en matière de protection des renseignements personnels.

1.1 Types de renseignements personnels pouvant être collectés

Dans le cadre de sa mission de protection du public en veillant à la formation continue obligatoire, à la déontologie et à la discipline de ses membres, la CSF recueille des renseignements personnels. Elle recueille ce qui est nécessaire à l'exercice de ses fonctions et à la mise en œuvre de programmes pour la prestation de services et la réalisation de sa mission.

La CSF prend les mesures adéquates pour s'assurer qu'elle effectue une cueillette de renseignements personnels qui est adéquate, pertinente et non excessive.

1.2 Collecte et consentement

Sous réserve de ce qui est prévu par la loi, la CSF devra obtenir le consentement à la cueillette, à l'utilisation ou à la divulgation des renseignements personnels des personnes concernées. Pour être valable, le consentement devra être manifeste, libre, éclairé, être donné à des fins spécifiques, en termes simples et clairs ainsi que pour la durée nécessaire à la réalisation des fins auxquelles il a été demandé. Dès lors, la

personne concernée aura accès à toute l'information nécessaire pour prendre une décision éclairée. À tout moment après l'obtention du consentement, il demeure possible de le retirer.

Dans certaines circonstances énumérées par la Loi sur l'accès, la CSF pourra communiquer des renseignements sans le consentement de la personne concernée.

1.3 Conservation et destruction

La CSF conserve les renseignements personnels qu'elle collecte conformément aux lois applicables et à son calendrier de conservation. Les renseignements personnels sont stockés et archivés au Canada.

Sous réserve des exigences légales ou contractuelles, vous pouvez retirer votre consentement à la collecte, l'utilisation ou la communication de renseignements personnels. Cela est notamment le cas pour les offres promotionnelles. Nous traiterons votre demande dans les meilleurs délais.

1.4 Gestion des accès

La CSF limite les accès aux renseignements personnels. Elle autorise l'accès, en tenant compte de la sensibilité des renseignements personnels, seulement aux membres de son personnel qui en ont besoin pour l'exercice de leurs fonctions.

La CSF fait également un suivi afin de réviser et révoquer les accès selon la nécessité d'avoir accès aux renseignements personnels. Elle veille également à ce que ces renseignements ne soient utilisés que pour les finalités déterminées ou comme autorisé.

1.5 Communications lors d'un contrat

Dans certaines situations, il peut être nécessaire de transmettre certains renseignements personnels, par exemple, pour l'embauche de personnels ou les enquêtes de sécurité.

Lors de la transmission de renseignements personnels, la CSF demande aux fournisseurs visés de compléter un formulaire de cybersécurité ou de transmettre une preuve de certification de type ISO27001. L'analyse de risques et de menaces afférente au formulaire doit être à l'entière satisfaction de la CSF. Les fournisseurs visés signent également une entente de confidentialité.

1.6 Évaluation des facteurs relatifs à la vie privée

Une évaluation des facteurs relatifs à la vie privée sera effectuée par la CSF pour les projets impliquant des systèmes d'information ou de prestation électronique de services tel qu'indiqué par la Loi sur l'accès.

Le Comité sur l'accès à l'information et la protection des renseignements personnels sera consulté, dès le début du projet, pour les fins de cette évaluation.

2. Rôles et responsabilités du Comité sur l'accès à l'information et la protection des renseignements personnels et des membres du personnel

La CSF a mise en place un Comité sur l'accès à l'information et la protection des renseignements personnels (le « **Comité** ») qui est responsable de la soutenir dans l'exercice de ses responsabilités et dans l'exécution de ses obligations en vertu de la Loi sur l'accès.

Plus précisément, le Comité soutient le Responsable de l'accès aux documents et de la protection des renseignements personnels dans l'exercice de ses fonctions et pour le respect de la Loi sur l'accès, notamment pour :

- définir les orientations et formuler des recommandations en matière de protection des renseignements personnels ;
- effectuer le suivi et la mise de la Déclaration de confidentialité et conditions d'utilisation et des Règles relatives à la protection des renseignements personnels ;
- être consulté lors de tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels, aux fins de l'évaluation des facteurs relatifs à la vie privée;
- effectuer le suivi du registre des incidents de confidentialité.

Les employés de la CSF qui ont accès à des renseignements personnels dans le cadre de leurs fonctions doivent :

- préserver la confidentialité des renseignements;
- informer immédiatement leur supérieur et le Responsable de l'accès aux documents et de la protection des renseignements personnels de toute situation où la confidentialité de renseignements personnels pourrait avoir été compromise.

3. Demande d'accès et rectification

La Loi sur l'accès vous donne le droit d'obtenir tout renseignement personnel que la CSF détient sur vous, sauf exception, notamment prévu à celle-ci. Vous pouvez aussi, sous réserve des dispositions prévues à la Loi sur l'accès, exiger qu'un renseignement inexact ou équivoque soit rectifié ou détruit.

Pour formuler ce type de demande, vous pouvez compléter le [Formulaire de demande d'accès](#) ou écrire directement au Responsable de l'accès à l'adresse suivante : responsableacces@chambresf.com.

4. Gestion des incidents de confidentialité

Pour les fins des présents et conformément à l'article 63.9 de la Loi sur l'accès, on entend par « incident de confidentialité » un accès, une utilisation ou une communication qui est non autorisé d'un renseignement personnel ou la perte d'un renseignement personnel ou l'atteinte à la protection d'un renseignement personnel.

Lorsque la CSF a des motifs de croire qu'un incident de confidentialité impliquant un renseignement personnel s'est produit, elle prendra les mesures raisonnables nécessaires pour diminuer les risques qu'un préjudice soit causé.

Plus précisément, lorsqu'il y a un bris de confidentialité, un événement de sécurité est ouvert à travers l'outil de billetterie de la CSF. Le Comité évalue les critères pour déterminer s'il s'agit d'un incident de confidentialité. S'il s'agit d'un incident de confidentialité qui implique des renseignements personnels, la CSF va effectuer le diagnostic et prendre les mesures raisonnables pour diminuer les risques. L'incident sera détaillé dans le Registre des incidents de confidentialité.

Lorsqu'il s'agit d'un incident de confidentialité qui présente un risque de préjudice sérieux, la CSF avisera la Commission d'accès à l'information, ainsi que toute personne dont un renseignement personnel est touché par l'incident. Pour déterminer s'il s'agit d'un risque de préjudice sérieux, la CSF sur consultation du Responsable de la protection des renseignements personnels prendra notamment en considération :

- la sensibilité du renseignement concerné;

- les conséquences appréhendées de son utilisation; et
- la probabilité qu'il soit utilisé à des fins préjudiciables.

Registre des incidents de confidentialité

Le Responsable de l'accès aux documents et de la protection des renseignements personnels ou la personne à qui la tâche a été confiée, maintient un Registre des incidents de confidentialité qui contient les éléments suivants :

- Date de l'événement (date ou période où l'incident a eu lieu) ;
- Date de la prise de connaissance ;
- Description des circonstances de l'incident ;
- Description des renseignements visés ;
- Nombre de personnes concernées par l'incident ;
- Description des éléments qui amène la CSF à conclure qu'il existe un risque de préjudice sérieux ;
- Date de transmission de l'avis à la Commission d'accès à l'information, s'il y a un préjudice sérieux et aux personnes concernées ;
- Mesures que la CSF a prises pour diminuer les risques qu'un préjudice soit causé.

5. Processus de traitement des plaintes

La CSF a mis en place un processus pour le traitement des plaintes des consommateurs et de ses membres.

Ainsi, toutes plaintes relatives à la protection des renseignements personnels doivent être transmises à la CSF par courriel au info@chambresf.com .

6. Activités de formation et de sensibilisation

Tous les employés de la CSF doivent obligatoirement suivre mensuellement et réussir des formations en matière de cybersécurité octroyées par un tiers-fournisseur de la CSF expert en la matière. Ces formations ont pour objectif de sensibiliser les employés à la cybersécurité.

7. Membres de la CSF

La CSF recueille des renseignements personnels sur ses membres tel que permis par la loi et dans le cadre de sa mission. La CSF prend les mesures appropriées afin de veiller à la protection de ces renseignements.

Le membre est responsable du maintien de la confidentialité de ses données d'identification et de ses mots de passe.

8. Sondages

La CSF effectue occasionnellement des sondages auprès de ses membres et des consommateurs dans le cadre de sa mission. La CSF ne recueille que les renseignements qui sont nécessaires. Lorsque la CSF retient les services de tiers-fournisseurs, elle effectue une analyse de risques et de menace via son questionnaire de cybersécurité ou valide ses certifications.

9. Entrée en vigueur

Les présentes Règles entrent en vigueur le 22 septembre 2023.