Règles encadrant la gouvernance à l'égard des renseignements personnels

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 assujetti 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 encadrant la gouvernance à l'égard 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.

Ces Règles s'appliquent à tous les renseignements personnels détenus par la CSF et à toutes les personnes qui traitent ces renseignements personnels. La protection de ces renseignements incombe à toute personne qui traite ces renseignements dans le cadre de ses fonctions ou dans le cadre de sa relation avec la CSF.

1. Collecte, utilisation et communication de renseignements personnels

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

a. 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 notamment les renseignements personnels concernant les membres de la CSF, les employés, les administrateurs du conseil d'administration et les membres du comité de discipline.

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

Au moment de la collecte, et par la suite sur demande, la CSF informe les personnes concernées, notamment des fins pour lesquelles les renseignements personnels sont recueillis ; des catégories de personnes qui auront accès à ces renseignements personnels ; et des droits d'accès et de rectification prévus par la *Loi sur l'accès*.

b. Utilisation des renseignements personnels

L'utilisation des renseignements personnels représente le moment où ces renseignements sont utilisés par les personnes autorisées au sein de la CSF.

L'accès aux renseignements personnels sera limité aux employés qui ont la qualité de les recevoir au sein de la CSF, lorsque ces renseignements personnels sont nécessaires à l'exercice de leurs fonctions.

La CSF limite l'utilisation des renseignements personnels aux fins pour lesquels ils ont été recueillis. Pour utiliser ces renseignements à d'autres fins, la CSF obtient votre consentement, à moins d'une exception prévue par la Loi sur l'accès.

c. Communication des renseignements personnels

À cette étape, la CSF s'assure d'obtenir le consentement des personnes concernées pour communiquer leurs renseignements à un tiers, à moins d'une exception prévue par la Loi. Le consentement exprès est obtenu dans le cas où des renseignements personnels sensibles sont en cause. La CSF respecte les obligations prévues par la Loi sur l'accès lorsqu'elle communique des renseignements personnels sans le consentement de la personne concernée.

Lorsque la CSF communique des renseignements personnels à un mandataire ou un fournisseur de services dans le cadre d'un mandat ou d'un contrat de service, elle conclut avec ce dernier une entente contenant les obligations de protection des renseignements personnels. Avant que les renseignements personnels ne soient communiqués à l'extérieur du Québec, la CSF s'assure que les renseignements bénéficieront d'une protection équivalente à celle que la Loi sur l'accès procure.

d. Consentement

Sous réserve de ce qui est prévu par la Loi sur l'accès, la CSF obtient le consentement à la collecte, à l'utilisation et à la communication 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. Cela est notamment le cas pour les offres promotionnelles. Nous traiterons votre demande dans les meilleurs délais.

Dans certaines circonstances énumérées par la Loi sur l'accès, la CSF pourra utiliser et communiquer les renseignements personnels collectés sans le consentement de la personne concernée.

e. 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 conservés et archivés au Canada.

La CSF s'assure que les renseignements personnels qu'elle conserve soient à jour, exacts et complets pour servir aux fins pour lesquelles ils sont recueillis ou utilisés. Elle prend aussi toutes les mesures de sécurité propres à assurer la protection des renseignements personnels conservés.

Lorsque les fins pour lesquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, la CSF le détruit de manière sécuritaire, ou l'anonymise pour l'utiliser à des fins d'intérêt public, sous réserve des lois applicables et conformément à son calendrier de conservation.

2. Obligations, rôles et responsabilités

Les rôles et responsabilités en matière de sécurité et protection de l'information de la CSF sont définis pour chacun des niveaux de gestion au sein de la CSF, ainsi que pour chaque domaine concerné par la sécurité et la protection de l'information de la CSF.

a. Comité de direction de la CSF

i) Valide la présente Règle encadrant la gouvernance à l'égard des renseignements personnels, les Conditions d'utilisation de son site web et la Politique de sécurité de l'information ainsi que toute modification de ces documents;

ii) S'assure de l'application et du respect de ces documents par les gestionnaires de la CSF ;

iii) Valide les mesures visant à favoriser l'application de la Règle encadrant la gouvernance à l'égard des renseignements personnels, les Conditions d'utilisation de son site web et la Politique de sécurité de l'information et des obligations légales de la CSF en matière de protection et sécurité de l'information ;

iv) Valide les orientations stratégiques en matière de protection et sécurité de l'information ; et

v) Valide les plans d'action et reçoit une reddition de compte trimestrielle relativement à la protection et sécurité de l'information.

b. Présidente et chef de la direction

i) La présidente et chef de la direction en tant que plus haut responsable, définit les valeurs et les orientations en matière de protection et sécurité de l'information et assure

le respect et l'application des lois, politiques et directives relatives à la protection et sécurité de l'information ;

ii) Nomme le responsable de la protection et sécurité de l'information.

c. Responsable de la protection et sécurité de l'information de la CSF

i) Consulte le comité de direction de la CSF dans la détermination des orientations stratégiques et des priorités d'intervention ;

ii) Assure la mise en place du cadre normatif des ressources informationnelles et des mesures d'atténuation des risques ;

iii) Assure la sécurité des actifs informationnels, durant tout leur cycle de vie, en déployant les mesures de protection et sécurité appropriées et approuvées par les propriétaires de système d'information/gestionnaires ;

iv) Voit à inclure les clauses sur la sécurité et la protection de l'information de la CSF dans les contrats et les ententes auxquels la CSF intervient ;

v) Est le premier répondant de la CSF au niveau de la protection et sécurité de l'information ;

vi) S'assure que les antécédents des candidats à l'embauche ayant de hauts privilèges en matière de sécurité de l'information sont vérifiés et, au besoin, ceux des membres du personnel ou consultants impliqués dans la sécurité de l'information ;

vii) S'assure d'effectuer des tests de contrôle périodiques pour mesurer la robustesse du réseau ;

viii) S'assure de disposer d'un inventaire des systèmes ;

ix) Impose les sanctions appropriées en cas de violation des politiques, règlements, directives et code de conduite touchant la protection et sécurité de l'information ;

x) Est responsable de la reddition de compte ;

xi) Est responsable de l'application de la Règle encadrant la gouvernance à l'égard des renseignements personnels, les Conditions d'utilisation de son site web et la Politique de sécurité de l'information ;

xii) Identifie les propriétaires de système d'information/gestionnaire.

d. Responsable de l'accès à l'information et de la protection des renseignements personnels

i) Le responsable de l'accès à l'information et de la protection des renseignements personnels veille au respect de la Loi sur l'accès.

e. Gestionnaires de système d'information

Chaque gestionnaire de système d'information :

i) Veille à l'accessibilité, à l'utilisation adéquate, à la gestion efficiente et à la sécurité des actifs informationnels sous sa responsabilité ;

ii) Collabore à la classification de l'information sous sa responsabilité et voit à la protection de ces données.

f. Utilisateurs des systèmes

i) Se conforme à la présente Règle encadrant la gouvernance à l'égard des renseignements personnels, les Conditions d'utilisation de son site web, de la Politique de sécurité de l'information et d'utilisation et à toute directive en matière de sécurité de l'information et d'utilisation des actifs informationnels ;

ii) Respecte les mesures de sécurité en place, sans les contourner, les désactiver ou les modifier ;

iii) Les employés utilisateurs s'assurent de compléter chacun des cours de sensibilisation à la sécurité de l'information aux termes du programme de sensibilisation de la CSF.

g. Employés.

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

La CSF a mis 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 ;
- approuver les règles encadrant la gouvernance de la CSF à l'égard des renseignements personnels ;
- effectuer le suivi et la mise à jour du document relatif aux conditions d'utilisation du site internet et des présentes Règles ;
- être consulté dès le début 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.

4. Gestion des accès aux renseignements personnels

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 autorisées.

5. Communications lors d'un contrat

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

Lors de la transmission de renseignements personnels, la CSF demande aux fournisseurs visés de remplir 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.

Lorsque les renseignements personnels sont communiqués à un mandataire ou à un fournisseur de services dans le cadre d'un mandat ou d'un contrat de service ; sans le consentement de la personne concernée, la CSF inscrit cette communication dans un registre.

6. Évaluation des facteurs relatifs à la vie privée

La CSF procède à une évaluation des facteurs relatifs à la vie privée (« EFVP ») dans le cas :

- D'un projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de Renseignements personnels ;
- D'une communication d'un renseignement personnel à l'extérieur du Québec ;
- De la collecte de renseignements personnels en collaboration ;
- De la communication de renseignements personnels en vertu de l'article 68 de la Loi sur l'accès ; ou
- D'un projet d'étude, de recherche ou de production statistique.

L'EFVP tient compte de la sensibilité des renseignements personnels, des fins de leur utilisation, de leur quantité, de leur répartition, de leur support et de la proportionnalité des mesures proposées pour les protéger. Dans le cas d'une communication des renseignements personnels à l'extérieur du Québec, l'EFVP prend en compte les mesures de protection, incluant celles qui sont contractuelles et le régime juridique applicable dans la juridiction où ces renseignements seraient communiqués, notamment les principes de protection des renseignements personnels applicables.

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.

7. Procédure de traitement des plaintes

La CSF a mis en place une procédure 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 comme indiqué dans la Procédure de gestion et traitement des plaintes.

Les plaintes qui sont formulées au sujet de nos pratiques en matière de protection des renseignements personnels, y compris la manière dont nous utilisons vos renseignements personnels, sont traitées par le Responsable de l'accès aux documents et de la protection des renseignements personnels de la CSF qui doit y répondre dans un délai de 30 jours.

8. Gestion des incidents de confidentialité

Pour les fins des présentes 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.

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. Lorsque la CSF a des motifs de croire qu'un incident de confidentialité impliquant un renseignement personnel s'est produit, elle effectuera le diagnostic et prendra les mesures raisonnables nécessaires pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent. 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 l'accès aux documents et 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.

9. 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) ou, si cette dernière n'est pas connue, une approximation de cette période ;
- Date de la prise de connaissance de l'incident par la CSF ;
- Description des circonstances de l'incident ;
- Description des renseignements visés par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description ;
- Nombre de personnes concernées par l'incident ou, s'il n'est pas connu, une approximation de ce nombre ;
- Description des éléments qui amène la CSF à conclure qu'il existe ou non un risque de préjudice sérieux ;
- Date de transmission de l'avis à la Commission d'accès à l'information, si l'incident présente un risque qu'un préjudice sérieux soit causé ;
- Mesures que la CSF a prises pour diminuer les risques qu'un préjudice soit causé.

Les renseignements contenus au registre seront tenus à jour et conservés par la CSF pendant une période minimale de 5 ans après la date ou la période au cours de laquelle la CSF a pris connaissance de l'incident.

10. Activités de formation et de sensibilisation

Tous les employés de la CSF doivent obligatoirement suivre périodiquement 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 à la cybersécurité les employés.

11. 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. La CSF prend les mesures de protection adéquates à l'égard des renseignements personnels recueillis ou utilisés dans le cadre du sondage. La CSF a en outre adopté une règle interne de gouvernance qui inclue l'évaluation à entreprendre pour conclure à la nécessité de recourir au sondage, ainsi que l'évaluation de l'aspect éthique du sondage compte tenue, notamment, de la sensibilité des renseignements personnels recueillis et de la finalité de leur utilisation.