Conseil de gestion de l'assurance parentale
Québec

Politique

Accès aux documents et protection des renseignements personnels

Adoptée par le conseil d'administration le 14 septembre 2023

** Dans la présente politique, le masculin englobe les deux genres et est utilisé pour alléger le texte.*

Table des matières

1. Objet

La présente politique est adoptée en application de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ c. A-2.1), telle qu'elle a été modifiée par la *Loi modernisant des dispositions législatives en matière des renseignements personnels* (2021, c. 25).

En conformité avec l'article 63.3 de cette Loi, elle présente les règles encadrant la gouvernance des renseignements personnels détenus par le Conseil de gestion.

2. Définitions

- *Caviardage :* le caviardage consiste à masquer un renseignement personnel ou confidentiel permettant d'identifier une personne physique ou tout autre renseignement confidentiel dont l'accès peut être refusé par la loi.

- *Incident de confidentialité :* l'accès, l'utilisation, la communication ou la perte non autorisés par la loi d'un renseignement personnel ou confidentiel ou toute autre atteinte à la protection d'un tel renseignement.

- *Renseignement personnel :* un renseignement qui concerne une personne physique et permet de l'identifier. Le nom d'une personne physique, seule n'est pas un renseignement personnel, sauf s'il est mentionné avec un autre renseignement la concernant, ou lorsque sa mention dans un contexte donné révèle un renseignement personnel la concernant.

- *Renseignement confidentiel* : un renseignement dont l'accès peut ou doit être refusé en vertu de la loi.

3. Cadre juridique et administratif

Cette politique s'appuie principalement sur les lois et les règlements suivants :

- Charte des droits et libertés de la personne (RLRQ, c. C-12);
- Code civil du Québec (1991, c. 64);
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, c. A-2.1);
- Loi sur les archives (RLRQ, c. A-21.1);
- Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (RLRQ, c. A-2.1, r. 2);
- Règlement sur les incidents de confidentialité (RLRQ, c. A-2.1, r. 3)
- Règlement excluant certains organismes publics de former un comité sur l'accès à l'information et la protection des renseignements personnels (Décret 744-2023 du 3 mai 2023);
- Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques (RLRQ, c. A-21.1, r.2).

Elle est également complétée par les documents internes suivants :

- Politique de la sécurité de l'information;
- Calendrier de conservation;
- Lignes internes de conduite concernant la gestion des contrats.

4. Objectifs

La présente politique vise principalement à :

a) confirmer l'importance accordée par le Conseil de gestion à la confidentialité des renseignements personnels;

b) assurer le respect des lois et des règlements en matière de protection des renseignements personnels;

c) définir le partage des responsabilités des différentes personnes concernées dans la mise en œuvre de la présente politique.

5. Champ d'application

La politique s'applique aux membres du conseil d'administration et du personnel du Conseil de gestion ainsi qu'à toute personne liée au Conseil de gestion par un contrat de travail.

6. Principes généraux

Confidentialité

6.1. Les renseignements personnels, incluant ceux des membres du conseil d'administration et du personnel du Conseil de gestion, sont confidentiels.

6.2. Des mesures de sécurité propres à assurer la protection des renseignements personnels et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support, sont mises en place.

Collecte

6.3. Seuls les renseignements personnels nécessaires à la réalisation de la mission du Conseil de gestion et à l'exercice de ses attributions sont recueillis.

6.4. Le Conseil de gestion ne recueille aucun renseignement personnel au nom d'un autre organisme public au sens de l'article 64 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*.

6.5. Le Conseil de gestion n'effectue pas de collecte de renseignements personnels par des moyens technologiques. Il ne s'est donc pas doté d'une politique de confidentialité à cet effet.

Conservation

6.6. Les documents du Conseil de gestion sont classés selon un plan de classification qui en permet le repérage, conformément au *Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques*.

Communication et utilisation

6.7. Les renseignements personnels ne peuvent être consultés, communiqués à des tiers ou utilisés à d'autres fins que celles pour lesquelles ils ont été obtenus sans le consentement de la personne concernée, sous réserve des exceptions prévues à la loi.

Gestion contractuelle

6.8. En matière contractuelle :

a) Les contrats de service impliquant des renseignements personnels comportent des clauses de protection de renseignements personnels. Un engagement à la confidentialité signé par chaque membre du personnel du contractant qui a accès aux renseignements personnels est exigé. Ces contrats prévoient aussi la destruction des renseignements personnels lorsque les contrats arrivent à leurs termes.

b) Le Conseil de gestion ne peut pas divulguer :

- Un renseignement permettant de connaître le nombre ou l'identité des entreprises qui ont demandé une copie des documents d'appel d'offres public ainsi que le nombre ou l'identité des entreprises qui ont déposé une soumission, et ce, jusqu'à l'ouverture des soumissions.

- Un renseignement permettant d'identifier une personne comme étant un membre d'un comité de sélection constitué conformément au cadre normatif.

6.9. Le Conseil de gestion :

a) Ne peut pas communiquer le secret industriel d'un tiers ou un renseignement industriel, financier, commercial, scientifique, technique ou syndical de nature confidentielle fourni par un tiers et habituellement traité par un tiers de façon confidentielle, sans son consentement.

b) Ne peut pas communiquer un renseignement fourni par un tiers lorsque sa divulgation risquerait vraisemblablement d'entraver une négociation en vue de la conclusion d'un contrat, de causer une perte à ce tiers, de procurer un avantage appréciable à une autre personne ou de nuire de façon substantielle à la compétitivité de ce tiers, sans son consentement, sauf s'il est autorisé par la loi.

c) Doit, avant de communiquer un renseignement industriel, financier, commercial, scientifique, technique ou syndical fourni par un tiers, lui en donner avis, conformément à la loi, afin de lui permettre de présenter ses observations, sauf dans les cas où le renseignement a été fourni en application d'une loi qui prévoit que le renseignement peut être communiqué et dans les cas où le tiers a renoncé à l'avis en consentant à la communication du renseignement ou autrement.

Système d'information ou électronique

6.10. Une évaluation des facteurs relatifs à la vie privée est réalisée de tout projet d'acquisition, de développement et de refonte de système d'information ou électronique impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels. Cette évaluation tient compte notamment de la sensibilité des renseignements personnels, de la finalité de leur utilisation, de leur quantité et de leur support.

Destruction

6.11. Le Conseil de gestion veille à la destruction sécuritaire des renseignements lorsque les fins pour lesquelles ceux-ci ont été recueillis sont accomplies, et ce, en conformité avec le calendrier de conservation.

7. Études, recherches et productions de statistiques

7.1. Le Conseil de gestion peut communiquer des renseignements personnels sans le consentement des personnes concernées à une personne ou à un organisme qui souhaite utiliser ces renseignements à des fins d'étude, de recherche ou de production de statistiques.

7.2. Cette communication peut s'effectuer si une évaluation des facteurs relatifs à la vie privée conclut que :

a) l'objectif de l'étude, de la recherche ou de la production de statistiques ne peut être atteint que si les renseignements sont communiqués sous une forme permettant d'identifier les personnes concernées;

b) il est déraisonnable d'exiger que la personne ou l'organisme obtienne le consentement des personnes concernées;

c) l'objectif de l'étude, de la recherche ou de la production de statistiques l'emporte, eu égard à l'intérêt public, sur l'impact de la communication et de l'utilisation des renseignements sur la vie privée des personnes concernées;

d) les renseignements personnels sont utilisés de manière à en assurer la confidentialité;

e) seuls les renseignements nécessaires sont communiqués.

7.3 La personne ou l'organisme qui souhaite utiliser des renseignements personnels à des fins d'étude, de recherche ou de production de statistiques doit :

a) faire sa demande par écrit;

b) joindre à sa demande une présentation détaillée des activités d'étude, de recherche ou de production de statistique;

c) exposer les motifs pouvant soutenir que les critères mentionnés aux paragraphes a) à e) du précédent article sont remplis;

d) mentionner toutes les personnes et tous les organismes à qui il fait une demande similaire aux fins de la même étude, recherche ou production de statistiques;

e) le cas échéant, décrire les différentes technologies qui seront utilisées pour effectuer le traitement des renseignements;

f) le cas échéant, transmettre la décision documentée d'un comité d'éthique de la recherche relative à cette étude, recherche ou production de statistiques.

7.4 Le Conseil de gestion, lorsqu'il communique des renseignements personnels doit préalablement conclure avec la personne ou l'organisme à qui il les transmet une entente stipulant notamment que ces renseignements :

a) ne sont accessibles qu'aux personnes à qui leur connaissance est nécessaire dans l'exercice de leurs fonctions et ayant signé un engagement à la confidentialité;

b) ne peuvent être utilisés à d'autres fins;

c) ne peuvent être appariés avec tout autre fichier non prévu initialement à la présentation détaillée des activités de recherche;

d) ne peuvent être communiqués ni diffusés sous une forme permettant d'identifier les personnes concernées;

e) prévoir toutes les autres mesures et exigences prévues à la loi.

7.5 L'entente est transmise à la Commission d'accès à l'information, entre en vigueur 30 jours après son dépôt et est inscrite au registre de communication de renseignements personnels du Conseil de gestion.

8. Sondage

8.1. Le caractère nécessaire est évalué pour tout projet de sondage à réaliser par le Conseil de gestion ou pour son compte et impliquant des renseignements personnels.

8.2. L'aspect éthique du projet de sondage est également pris en considération dans cette évaluation, notamment de la sensibilité des renseignements personnels recueillis et de la finalité de leur utilisation.

8.3. Les renseignements personnels recueillis dans le cadre d'un sondage sont confidentiels. Seul le personnel autorisé peut y avoir accès et peut les utiliser uniquement aux fins du sondage. Ces renseignements sont détruits de manière sécuritaire une fois le projet terminé, en conformité avec le calendrier de conservation.

9. Enregistrement des visioconférences

9.1. Les plateformes de visioconférence sont celles qui sont autorisées par le Conseil de gestion et qui correspondent aux standards gouvernementaux en matière de cybersécurité et de sécurité de l'information.

9.2. L'enregistrement est un document détenu par le Conseil de gestion au sens de la loi. Il est susceptible de faire l'objet d'une demande d'accès.

9.3. La voix et l'image d'une personne se trouvant sur un enregistrement constituent des renseignements personnels puisqu'ils permettent de l'identifier.

9.4. Le Conseil de gestion doit justifier la nécessité de procéder à un enregistrement. Le besoin doit être raisonnablement lié à l'objectif visé et les avantages doivent être supérieurs aux préjudices potentiels qui pourraient être vécus par les participants.

9.5. Les fins de tout projet d'enregistrement doivent être autorisées par le responsable de l'accès aux documents et de la protection des renseignements personnels.

Dans son évaluation de la pertinence de l'enregistrement à la lumière de la finalité visée par la rencontre, le responsable de l'accès aux documents et de la protection des renseignements personnels doit tenir compte de l'utilité de l'enregistrement, des objectifs poursuivis, de la sensibilité des renseignements, des avantages et les bénéfices escomptés, des inconvénients à le faire ou à ne pas le faire, si l'enregistrement doit être global ou partiel.

9.6. Les finalités et les usages visés par l'enregistrement doivent être clairement signalés aux personnes concernées lors de la collecte de ces renseignements, notamment tout juste avant le début de l'enregistrement.

9.7. La réutilisation de l'enregistrement pour des usages non prévus nécessite l'obtention d'un consentement valide des personnes concernées.

9.8. L'organisateur de la rencontre doit proposer des accommodements aux participants pour éviter d'être enregistré, comme la possibilité d'éteindre leur caméra, de se créer un pseudonyme et d'avoir recours à des filtres d'image pour l'arrière-plan.

9.9. Le Conseil de gestion est tenu de détruire l'enregistrement et les renseignements personnels qui s'y trouvent lorsque les fins pour lesquelles ils ont été collectés ou utilisés sont accomplies, sous réserve de la Loi sur les archives.

10. Demande d’accès

10.1. Une demande d’accès peut être écrite ou verbale. Si elle est écrite, elle peut se faire dans un format technologique.

10.2. Si la demande d’accès est adressée au président-directeur général du Conseil de gestion, celui-ci doit la transmettre avec diligence au responsable à qui la fonction de responsable de l’accès aux documents et sur la protection des renseignements personnels a été déléguée.

10.3. Les renseignements personnels obtenus par le Conseil de gestion dans le cadre d’une demande d’accès sont conservés au dossier de la demande d’accès.

10.4. Toute demande d’accès est traitée dans les vingt (20) jours de sa réception. Le demandeur est informé sur ses recours et sur la possibilité de recevoir de l’assistance pour l’aider à formuler sa demande d’accès et comprendre la décision.

10.5. Le personnel du Conseil de gestion doit collaborer, dans les délais impartis, avec le responsable de l’accès aux documents et de la protection des renseignements personnels dans la recherche de documents et de l'information faisant l'objet de la demande d'accès et dans le traitement d'une telle demande.

10.6. Le responsable de l’accès aux documents et de la protection des renseignements personnels doit motiver tout refus de donner suite à une demande d’accès et indiquer la disposition de la loi sur laquelle ce refus s’appuie.

10.7. Le Conseil de gestion ne peut refuser l'accès à un document pour le seul motif qu’il comporte des renseignements personnels ou confidentiels, sauf si ces renseignements en forment la substance. Avant de donner accès à ce document, le Conseil de gestion doit s’assurer du respect de la confidentialité des renseignements, notamment en caviardant les renseignements personnels et confidentiels.

10.8. Les décisions relatives aux demandes d’accès publiées sur le site Internet du Conseil de gestion sont anonymisées.

11. Demande de rectification

11.1. Toute personne peut demander de rectifier les renseignements personnels que le Conseil de gestion détient. Il en est de même pour l’ajout de renseignements personnels.

11.2. La demande de rectification doit se faire par écrit et être adressée au responsable de l’accès aux documents et de la protection des renseignements personnels du Conseil de gestion.

11.3. Si la demande de rectification est adressée au président-directeur général du Conseil de gestion, celui-ci doit la transmettre avec diligence au responsable de l’accès aux documents et de la protection des renseignements personnels à qui cette fonction a été déléguée.

11.4. Le responsable de l'accès aux documents et de la protection des renseignements personnels doit donner suite à la demande de rectification avec diligence et au plus tard dans les vingt (20) jours qui suivent la date de sa réception. Le cas échéant, il doit motiver tout refus de donner suite à sa demande et indiquer la disposition de la loi sur laquelle ce refus s'appuie.

11.5. Le personnel du Conseil de gestion doit collaborer, dans les délais impartis, avec le responsable de l'accès aux documents et de la protection des renseignements personnels dans la recherche de documents et de l'information faisant l'objet d'une demande de rectification et dans le traitement d'une telle demande.

12. Traitement des plaintes

12.1. Le Conseil de gestion traite les plaintes relatives à la protection des renseignements personnels en fonction du processus établi par cette politique.

12.2. La plainte doit être transmise au président-directeur général ou au responsable de l'accès aux documents et de la protection des renseignements personnels.

12.3. Un avis de réception est transmis au plaignant.

12.4. La plainte est analysée en conformité avec la loi.

12.5. La décision et les motifs à son soutien sont communiqués au plaignant dans les trente (30) jours suivant la réception de la plainte. Ce dernier est également informé de ses recours possibles à la Commission d'accès à l'information.

13. Incidents de confidentialité

13.1. Le Conseil de gestion, s'il a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'il détient, doit prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent.

13.2. Lorsqu'il évalue le risque qu'un préjudice soit causé à une personne dont un renseignement personnel est concerné par un incident de confidentialité (Annexe 1), le Conseil de gestion doit considérer notamment la sensibilité du renseignement concerné, les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables.

13.3. Si l'incident présente un risque qu'un préjudice sérieux soit causé, le Conseil de gestion doit, avec diligence, aviser la Commission d'accès à l'information. Il doit également aviser toute personne dont un renseignement personnel est concerné par l'incident, à défaut de quoi la Commission d'accès à l'information peut lui ordonner de le faire.

13.4. Le Conseil de gestion peut également aviser toutes les personnes et organismes susceptibles de diminuer ce risque, en ne lui communiquant que les renseignements

personnels nécessaires à cette fin sans le consentement de la personne concernée. Dans ce dernier cas, le responsable de l'accès aux documents et de la protection des renseignements personnels doit enregistrer la communication.

13.5. Une personne dont un renseignement personnel est concerné par l'incident n'a pas à être avisée tant que cela serait susceptible d'entraver une enquête faite par une personne ou par un organisme qui, en vertu de la loi, est chargée de prévenir, détecter ou réprimer le crime ou les infractions aux lois.

13.6. L'avis à la Commission d'accès à l'information qu'un incident de confidentialité présente un risque qu'un préjudice sérieux soit causé est fait par écrit (Annexe 2) et doit contenir les renseignements suivants :

a) le nom et les coordonnées de la personne à contacter au sein du Conseil de gestion relativement à l'incident;

b) une description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description;

c) une brève description des circonstances de l'incident et, si elle est connue, sa cause;

d) la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période;

e) la date ou la période au cours de laquelle le Conseil de gestion a pris connaissance de l'incident;

f) le nombre de personnes concernées par l'incident et, parmi celles-ci, le nombre de personnes qui résident au Québec ou, s'ils ne sont pas connus, une approximation de ces nombres;

g) une description des éléments qui amènent le Conseil de gestion à conclure qu'il existe un risque qu'un préjudice sérieux soit causé aux personnes concernées, telles que la sensibilité des renseignements personnels concernés, les utilisations malveillantes possibles de ces renseignements, les conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables;

h) les mesures que le Conseil de gestion a prises ou entend prendre afin d'aviser les personnes dont un renseignement personnel est concerné par l'incident, de même que la date où les personnes ont été avisées ou le délai d'exécution envisagé;

i) les mesures que le Conseil de gestion a prises ou entend prendre à la suite de la survenance de l'incident, notamment celles visant à diminuer les risques qu'un préjudice soit causé ou à atténuer un tel préjudice et celles visant à éviter que de nouveaux incidents de même nature ne se produisent, de même que le délai où les mesures ont été prises ou le délai d'exécution envisagé;

j) le cas échéant, une mention précisant qu'une personne ou un organisme situé à l'extérieur du Québec et exerçant des responsabilités semblables à celles de

la Commission d'accès à l'information à l'égard de la surveillance de la protection des renseignements personnels a été avisée de l'incident.

Le Conseil de gestion doit également transmettre à la Commission d'accès à l'information tout renseignement dont il prend connaissance après lui avoir transmis l'avis exigé. L'information complémentaire doit alors être transmise avec diligence à compter de cette connaissance.

13.7. L'avis à la personne dont un renseignement personnel est concerné par un incident qui présente un risque qu'un préjudice sérieux soit causé doit contenir les renseignements suivants :

a) une description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description;

b) une brève description des circonstances de l'incident;

c) la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période;

d) une brève description des mesures que le Conseil de gestion a prises ou entend prendre à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé;

e) les mesures que le Conseil de gestion suggère à la personne concernée de prendre afin de diminuer le risque qu'un préjudice lui soit causé ou afin d'atténuer un tel préjudice;

f) les coordonnées permettant à la personne concernée de se renseigner davantage relativement à l'incident.

L'avis requis peut aussi être donné au moyen d'un avis public lorsque le fait de transmettre l'avis à la personne concernée est susceptible de causer à cette dernière un préjudice accru ou lorsqu'un tel avis est susceptible de représenter une difficulté excessive pour le Conseil de gestion ou lorsque ce dernier n'a pas les coordonnées de la personne concernée. Cet avis public peut être fait par tout moyen dont on peut raisonnablement s'attendre à ce qu'il permette de joindre la personne concernée.

13.8. Le Conseil de gestion doit tenir un registre des incidents de confidentialité (Annexe 3). Sur demande de la Commission d'accès à l'information, une copie de ce registre lui est transmise.

Ce registre contient les renseignements suivants :

a) une description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description;

b) une brève description des circonstances de l'incident;

c) la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période;

d) la date ou la période au cours de laquelle le Conseil de gestion a pris connaissance de l'incident;

e) le nombre de personnes concernées par l'incident ou, s'il n'est pas connu, une approximation de ce nombre;

f) une description des éléments qui amènent le Conseil de gestion à conclure qu'il existe ou non un risque qu'un préjudice sérieux soit causé aux personnes concernées, tels que la sensibilité des renseignements personnels concernés, les utilisations malveillantes possibles de ces renseignements, les conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables;

g) si l'incident présente un risque qu'un préjudice sérieux soit causé, les dates de transmission des avis à la Commission d'accès à l'information et aux personnes concernées, de même qu'une mention indiquant si des avis publics ont été donnés par l'organisation et la raison pour laquelle ils l'ont été, le cas échéant;

h) une brève description des mesures prises par le Conseil de gestion, à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé.

Les renseignements de ce registre doivent être tenus à jour et conservés pendant une période minimale de cinq ans après la date ou la période au cours de laquelle le Conseil de gestion a pris connaissance de l'incident.

14. Rôle et responsabilités

14.1. Le président directeur-général du Conseil de gestion veille à assurer le respect et la mise en œuvre de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et de la présente politique.

14.2. Il exerce la fonction de responsable de l'accès aux documents et celle de responsable de la protection des renseignements personnels. Il peut déléguer, en tout ou en partie, ces fonctions à un membre du personnel de direction.

14.3. Celui-ci exerce alors les fonctions de responsable de l'accès aux documents et de la protection des renseignements personnels. Cette fonction est exercée de manière autonome. Il veille notamment à la protection des renseignements personnels, répond aux demandes d'accès et de rectification, fait réaliser les évaluations des facteurs relatifs à la vie privée et tient à jour les registres prescrits par la loi. Il s'assure de la diffusion sur le site Internet des documents et des renseignements prévus au Règlement sur la diffusion des documents et sur la protection des renseignements personnels.

14.4. Le personnel du Conseil de gestion doit collaborer avec le responsable de l'accès aux documents et de la protection des renseignements personnels et veiller à la protection des renseignements personnels et des renseignements confidentiels.

14.5. Le Conseil de gestion est un organisme public de moins de cinquante (50) salariés et est donc exclu de l'obligation de former un comité sur l'accès à l'information et sur la protection des renseignements personnels. Les fonctions de ce comité sont confiées au responsable de l'accès aux documents et à la protection des renseignements personnels.

15. Formation des membres du personnel

Cette politique est partagée aux membres du personnel du Conseil de gestion. Des activités de formation et de sensibilisation sont offertes périodiquement en matière de protection des renseignements personnels.

16. Diffusion de la politique

La présente politique est diffusée sur le site Internet du Conseil de gestion.

17. Dispositions finales

La coordination de la mise en œuvre de la présente politique ainsi que sa mise à jour relèvent du responsable de l'accès aux documents et de la protection des renseignements personnels.

18. Entrée en vigueur

La présente politique entre en vigueur le 22 septembre 2023.

(s.) Marie Gendron

_____

Marie Gendron
Présidente du conseil d'administration et
Présidente-directrice générale

ANNEXE 1
GRILLE D'ÉVALUATION DU RISQUE DE PRÉJUDICE SÉRIEUX

INCIDENT DE CONFIDENTIALITÉ
Date :
Description :

ÉVALUATION
Est-ce que les renseignements concernés sont de nature sensible?
Quelles sont les utilisations malveillantes possibles de ces renseignements?
Quelles sont les conséquences appréhendées de leur utilisation?
Quelles sont les probabilités que ces renseignements soient utilisés à des fins préjudiciables?

CONCLUSION
Est-ce qu'il y a un risque qu'un préjudice sérieux soit causé aux personnes concernées?

ÉVALUATEUR
Nom :
Titre :
Signature :
Date :

ANNEXE 2
AVIS À LA COMMISSION D'ACCÈS À L'INFORMATION QU'UN INCIDENT DE CONFIDENTIALITÉ PRÉSENTE UN RISQUE QU'UN PRÉJUDICE SÉRIEUX SOIT CAUSÉ

INCIDENT DE CONFIDENTIALITÉ	
Description des renseignements personnels visés par l'incident[1]	
Brève description des circonstances de l'incident[2]	
Date ou la période où l'incident a eu lieu[3]	
Date ou la période au cours de laquelle le Conseil de gestion a pris connaissance de l'incident	

PERSONNES CONCERNÉES	
Nombre de personnes concernées par l'incident	
Et, parmi celles-ci, le nombre de personnes qui résident au Québec[4]	

RISQUE DE PRÉJUDICE SÉRIEUX
Description des éléments qui amènent le Conseil de gestion à conclure qu'il existe un risque qu'un préjudice sérieux soit causé aux personnes concernées[5]

MESURES	
Mesures que le Conseil de gestion a prises ou entend prendre afin d'aviser les personnes dont un renseignement personnel est concerné par l'incident	
la date où les personnes ont été avisées ou le délai d'exécution envisagé	

1 ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description;
2 et, si elle est connue, sa cause;
3 ou, si cette dernière n'est pas connue, une approximation de cette période;
4 ou, s'ils ne sont pas connus, une approximation de ces nombres;
5 tels que la sensibilité des renseignements personnels concernés, les utilisations malveillantes possibles de ces renseignements, les conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables;

Mesures que le Conseil de gestion a prises ou entend prendre à la suite de la survenance de l'incident, notamment celles visant à diminuer les risques qu'un préjudice soit causé ou à atténuer un tel préjudice et celles visant à éviter que de nouveaux incidents de même nature ne se produisent	
le délai où les mesures ont été prises ou le délai d'exécution envisagé	

MENTION	
Mention, le cas échéant, précisant qu'une personne ou un organisme situé à l'extérieur du Québec et exerçant des responsabilités semblables à celles de la Commission d'accès à l'information à l'égard de la surveillance de la protection des renseignements personnels a été avisé de l'incident	
Nom de la personne ou l'organisme	

PERSONNE À CONTACTER AU SEIN DU CONSEIL DE GESTION	
Nom	
Coordonnées	

ANNEXE 3
REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ[6]

INCIDENT				PERSONNE CONCERNÉES			CAI	CONSEIL DE GESTION	
Date	**Renseignements**	**Circonstances**	**Préjudice sérieux (éléments)**	**Nombre**	**Date de l'avis**	**Avis public**	**Date de l'avis**	**Date de connaissance**	**Mesures prises**

[6] Les renseignements contenus au registre des incidents de confidentialité doivent être tenus à jour et conservés pendant une période minimale de cinq ans après la date ou la période au cours de laquelle le Conseil de gestion a pris connaissance de l'incident.