Cadre de gestion des incidents de confidentialité

Cadre de gestion des incidents de confidentialité

Table des matières

1. Objectifs

Ce document a pour but d'établir le cadre de gestion des incidents de confidentialité mis en place par le CSBE. Il précise entre autres les étapes à suivre pour le traitement d'un incident de confidentialité ainsi que les rôles et responsabilités des différents intervenants impliqués, et rappelle les principales obligations du CSBE en lien avec la déclaration et l'enregistrement des incidents de confidentialité.

2. Champ d'application

Ce cadre de gestion s'applique à l'ensemble du personnel du CSBE, y incluant les étudiants et les stagiaires, et à toute personne ou entité qui transige avec le CSBE, que ce soit à titre de mandataire ou de prestataire de services.

Il s'applique à tout renseignement personnel détenu par le CSBE ou par un tiers pour son compte, et ce, durant tout son cycle de vie, c'est-à-dire l'ensemble des étapes que franchit le renseignement et qui vont de sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation du CSBE.

3. Assises légales

Les dispositions de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1, ci-après « Loi sur l'accès »), telle que modifiée par le chapitre 25 des Lois du Québec 2021 (ci-après « Loi 25 ») encadrant les incidents de confidentialité sont de droit nouveau. Il s'agit des articles 63.8 à 63.11, 127.2 et 158. Ce sont les articles 63.8 à 63.11 de la Loi sur l'accès qui édictent les obligations des organismes publics quant au traitement des incidents des confidentialité, ainsi que le Règlement sur les incidents de confidentialité, adopté le 30 novembre 2022[1]. Plus précisément,

[1] Selon le décret no 1761-2022 du gouvernement du Québec, publié à la *Gazette officielle du Québec*, 14 décembre 2022, 154e année, no 50, pp. 6819-6822. Le Règlement entre en vigueur le 15e jour suivant ladite publication, soit le 29 décembre 2022.

- l'article **63.8** énonce les obligations et pouvoirs de l'organisme public lors de la survenance d'un incident de confidentialité, à savoir que ce dernier :
    - doit prendre les mesures raisonnables pour mitiger les risques d'un préjudice sérieux lorsqu'il a des motifs de croire qu'un incident de confidentialité impliquant un renseignement personnel s'est produit et éviter qu'une telle situation se reproduise;
    - doit aviser la Commission d'accès à l'information (CAI) s'il estime que l'incident risque de causer un préjudice sérieux. L'article 3 du Règlement sur les incidents de confidentialité précise quelles sont les informations à transmettre à la CAI;
    - doit en aviser également toute personne dont un renseignement personnel est concerné par l'incident. L'article 5 du Règlement sur les incidents de confidentialité précise quelles sont les informations à transmettre à ces personnes, et l'article 6 de ce règlement énonce dans quels cas un avis public de l'incident de confidentialité devrait être donné par l'organisme public;
    - peut aviser toute personne ou tout organisme susceptible de diminuer ce risque, en limitant la communication aux seuls renseignements personnels qui sont nécessaires à cette fin sans le consentement de la personne concernée (dans ce cas, la communication de renseignements doit être enregistrée par le ou la responsable de la protection des renseignements personnels);
- l'article **63.9** définit ce qu'on entend par « incident de confidentialité »;
- l'article **63.10** précise les éléments que doit considérer l'organisme public lorsqu'il évalue le risque qu'un préjudice soit causé à une personne dont un renseignement personnel est concerné par un incident de confidentialité;
- **l'article 63.11** consacre l'obligation pour l'organisme public de se doter d'un registre des incidents de confidentialité. L'article 7 du Règlement sur les incidents de confidentialité précise quelles sont les informations à inscrire dans un tel registre, et l'article 8 de ce règlement prévoit l'obligation de garder à jour et de conserver les renseignements qu'il

contient, à l'égard d'un incident de confidentialité, durant une période minimale de 5 ans à compter du moment où l'organisme a pris connaissance de cet incident.

Le texte complet de ces dispositions est reproduit à l'annexe 1.

4. Contexte organisationnel

Le mandat du CSBE est défini à l'article 2 de sa loi constitutive (Loi sur le Commissaire à la santé et au bien-être, RLRQ, c. C-32.1.1, ci-après LCSBE), et ses pouvoirs et responsabilités sont énoncés dans cette même loi, tel que plus amplement décrit dans sa politique organisationnelle en matière d'accès à l'information et de protection des renseignements personnels.

Le CSBE ne rend pas de services directs à la population et n'administre pas, non plus, de programmes ou de mesures impliquant des interactions directes avec les citoyens. Ainsi, dans le cadre de ses activités de mission, hormis ceux qui sont nécessaires à l'exercice de ses responsabilités administratives (ressources humaines, gestion contractuelle, etc.), il ne recueille pas de renseignements personnels. Son rôle, en tant qu'organisme jouant un rôle conseil auprès du ministre de la Santé et des Services sociaux, est plutôt d'apprécier la performance globale du système québécois de santé et de services sociaux, d'un point de vue systémique, et de formuler au ministre des recommandations en vue d'améliorer cette performance.

Dans ce contexte, le CSBE doit travailler avec de nombreuses données, de diverses natures et provenant de sources variées, telles que, par exemple : revues de littérature, consultation d'experts et d'autres acteurs clés du système de santé et de services sociaux, consultations auprès des citoyens (y compris par des sondages), y incluant les membres du Forum de consultation, et consultation des banques de données, populationnelles notamment, détenues par d'autres organisations du domaine de la santé et des services sociaux.

Ainsi le CSBE doit, dans le cadre de ses travaux, accéder à des données dont certaines contiennent des renseignements personnels (ceux-ci sont toutefois anonymisés). Non seulement le CSBE doit-il s'assurer du respect du cadre légal

et réglementaire applicable à ces renseignements de nature confidentielle, mais encore doit-il offrir aux organisations qui lui rendent leurs données accessibles les meilleures garanties en ce qui concerne la consultation, l'utilisation, la communication, la conservation et la destruction de ces données.

Par ailleurs, en plus d'accéder à une importante quantité de données renfermant des renseignements personnels, le CSBE travaille avec de nombreux partenaires externes, aux intérêts parfois divergents, et, de ce fait, se trouve dépositaire de quantités d'information sensible.

5. Définitions

Incident de confidentialité

Toute divulgation non autorisée d'information confidentielle, et ce, peu importe le support sur lequel elle se trouve (papier, clé USB, ordinateur portable, tablette numérique, disquette, téléphone intelligent, etc.) et tout accès non autorisé à une telle information (dont des renseignements personnels). Ces bris peuvent être intentionnels ou accidentels. Ils peuvent résulter d'une erreur humaine ou de la défaillance d'un système. Selon la Loi sur l'accès, un *incident* de confidentialité peut résulter d'un accès non autorisé à un renseignement personnel, d'une utilisation ou d'une communication non autorisée d'un tel renseignement ou de toute autre atteinte à la protection d'un tel renseignement, y incluant sa perte.

Renseignement personnel

Renseignement qui concerne une personne physique et qui permet de l'identifier, c'est-à-dire de la distinguer d'une autre personne. Ce peut être notamment, mais non limitativement, un renseignement relatif à l'identité (nom, prénom[2], date de naissance, numéro d'assurance sociale, numéro de permis de conduire, numéro d'assurance-maladie, etc.), un renseignement à caractère financier (information sur les comptes bancaires, numéro de carte de crédit, etc.), une caractéristique d'une personne (origine ethnique, religion, expérience de travail, scolarité, état de santé), la photographie ou la vidéo d'une personne,

[2] Suivant l'article 56 de la Loi sur l'accès, le nom d'une personne physique n'est pas un renseignement personnel, sauf lorsqu'il est mentionné avec un autre renseignement la concernant ou lorsque sa seule mention révélerait un renseignement personnel concernant cette personne.

ou encore ses données biométriques (empreintes digitales, iris, voix). Un tel renseignement ne peut être communiqué sans le consentement de la personne concernée, sauf dans les cas d'exception permis par la loi.

Renseignement personnel sensible

Selon la définition qu'on en donne sur le site du gouvernement du Québec[3], « un renseignement personnel est considéré comme sensible lorsque, par sa nature notamment médicale, biométrique ou autrement intime ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de respect de la vie privée .

Ainsi, certains renseignements personnels sont sensibles par leur nature. Il peut s'agir, par exemple, de renseignements médicaux, biométriques, génétiques ou financiers, ou encore de renseignements sur la vie ou l'orientation sexuelle, les convictions religieuses ou bien l'origine ethnique ».

6. Traitement d'un incident de confidentialité

Cette section décrit le traitement d'un incident de confidentialité par le CSBE lorsque celui-ci a des motifs de croire de croire qu'un incident de confidentialité impliquant un renseignement personnel s'est produit.

Les principes qui y sont énoncés sont alignés sur les règles proposées par la CAI[4]. Le CSBE suit également le schéma de traitement d'un incident de confidentialité élaboré par le Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité (SRIDAIL) du ministère du Conseil exécutif[5]. Celui-ci est reproduit à l'annexe 2.

6.1. Évaluation sommaire de la situation

Au CSBE, toute personne alertée de la survenance réelle ou potentielle d'un incident de confidentialité, ou impliquée dans un tel incident, doit amorcer sans

[3] Source : En ligne, https://www.quebec.ca/gouvernement/travailler-gouvernement/travailler-fonction-publique/services-employes-etat/conformite/protection-des-renseignements-personnels/lexique#c123346 (page consultée le 26 août 2022)

[4] Source : *Aide-mémoire à l'intention des organismes et des entreprises – Quoi faire en cas de perte ou de vol de renseignements personnels?* En ligne, https://www.cai.gouv.qc.ca/documents/CAI_FI_vol_rens_pers_org-ent.pdf

[5] Source : En ligne, https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/sairid/schema-incident-confidentialite-renseignement-personnel.pdf?1642792255

délai la réalisation d'une évaluation sommaire de la situation. Ainsi, elle doit, seule ou avec les autres personnes alertées ou impliquées :

a) définir sommairement le contexte de l'incident, en identifiant :

- les renseignements personnels touchés et leur support, ainsi que les personnes affectées, leur nombre et leur groupe (clients, employés, etc.);
- le contexte des événements (date, heure, lieu, etc.);
- si possible, les circonstances de l'incident (cause, personnes susceptibles d'être impliquées dans l'incident, etc.);
- les mesures de sécurité physiques et informatiques en place lors de l'incident.

b) Informer le directeur de l'administration, qui informera la commissaire et évaluera, avec la responsable de de la protection des renseignements personnels (RPRP) au besoin, la nécessité d'informer les autorités externes concernées devant être avisées de l'incident de façon immédiate et avant l'évaluation des risques, telles que:

- les services informatiques du ministère de la Santé et des Services sociaux;
- le service de police, si les circonstances indiquent ou laissent supposer qu'un crime a été commis;
- la CAI.

Le directeur de l'administration désignera une personne ou une équipe responsable de la gestion de la situation, selon la gravité et l'ampleur de l'incident; il peut notamment s'agir de la RPRP.

6.2. Limitation de l'atteinte à la vie privée

Dès la survenance d'un incident de confidentialité, le CSBE prend sans tarder, s'il y a lieu, des mesures adéquates afin de limiter les conséquences, pour les personnes concernées, d'une possibilité d'utilisation malveillante de leurs renseignements personnels, ou encore de l'usurpation ou du vol de leur identité, à savoir :

a) faire le nécessaire pour limiter sans délai les conséquences d'une perte ou d'un vol de renseignements personnels en s'assurant de mettre fin à la pratique non conforme le cas échéant;

b) récupérer les dossiers physiques ou numériques, selon le cas;

c) révoquer ou modifier les mots de passe ou les codes d'accès informatiques;

d) contrôler les lacunes dans les systèmes de sécurité.

6.3. Évaluation des risques

Après avoir réalisé les actions prioritaires et urgentes ci-dessus, le CSBE procède à l'évaluation des risques que l'incident de confidentialité cause un préjudice sérieux aux personnes concernées. L'évaluation doit comporter les étapes suivantes :

a) compléter une évaluation préliminaire des risques, en considérant la sensibilité des renseignements personnels en cause et en tenant compte notamment de leur nature, de leur quantité, de la possibilité de les combiner avec d'autres renseignements, des personnes concernées, etc.;

b) déterminer le contexte de l'incident, en s'intéressant notamment aux éléments suivants :

- la cause (par exemple, s'agit-il d'un geste délibéré ou d'un accident, d'une erreur humaine, d'une faille informatique, etc.);
- les auteurs connus ou probables de la perte ou du vol de renseignements personnels (par exemple, une organisation criminelle, le public en général, etc.);
- l'étendue de la situation (nombre de personnes touchées, secteurs touchés);
- le caractère systémique ou non de la disparition des renseignements personnels (en particulier lorsque la perte n'est pas générée directement par une intervention humaine);

- une évaluation de la probabilité qu'un événement similaire se reproduise;

c) évaluer la possibilité que les renseignements personnels concernés fassent l'objet d'une utilisation susceptible de nuire aux personnes concernées en tenant compte, entre autres, des mesures de sécurité prises pour les protéger, de leur difficulté d'accès et de leur intelligibilité (mot de passe, encodage, etc.);

d) évaluer le caractère réversible ou non de la situation, dont la possibilité de récupérer les renseignements personnels;

e) évaluer si les mesures immédiates qui ont été prises étaient adéquates pour limiter l'atteinte, et les compléter si nécessaire;

f) déterminer les préjudices potentiels, notamment en évaluant les possibilités d'utilisation future des renseignements personnels par des personnes malveillantes, notamment pour le vol d'identité;

g) déterminer les priorités et les actions à prendre sur la base des résultats de l'évaluation ainsi réalisée.

6.4. Avis aux personnes et organismes concernés

Une fois l'évaluation des risques effectuée,

a) le CSBE détermine qui doit être mis au courant de la perte ou du vol de renseignements personnels, en fonction de son évaluation des risques :

- le service de police : lorsque la disparition peut résulter de la commission d'un crime, le service de police concerné doit d'abord être informé des éléments entourant cette disparition, puis de toutes les démarches subséquentes. On doit prendre garde à ne pas nuire à l'enquête et veiller à préserver les éléments de preuve qui pourraient être pertinents;

- les personnes concernées : si la perte ou le vol de renseignements personnels risque de leur causer préjudice, celles-ci devraient en

être avisées sans tarder, afin qu'elles puissent prendre les mesures nécessaires pour protéger leurs renseignements personnels. Les informations à transmettre à ces personnes, ainsi que l'énoncé des situations où un avis public devrait être donné, sont précisés à la section III (articles 5 et 6) du Règlement sur les incidents de confidentialité;

- la CAI : si les personnes concernées par les renseignements personnels perdus ou volés proviennent du Québec, la CAI pourrait amorcer une inspection ou une enquête et jouer un rôle de conseiller dans la recherche de solutions. Le formulaire prescrit par la CAI peut être utilisé pour informer cette dernière de la survenance d'un incident de confidentialité[6];

- autres : selon les circonstances, il pourrait aussi être nécessaire d'aviser d'autres intervenants, tels que les agences de crédit, un mandataire, un cocontractant, une instance gouvernementale, un syndicat, un ordre professionnel, etc. Toutefois, en leur fournissant des informations au sujet de la perte de renseignements personnels, on doit prendre garde à ne pas aggraver le préjudice que pourraient subir les personnes concernées (par exemple, limiter au minimum les renseignements personnels fournis dans les avis).

b) le CSBE désigne les personnes responsables d'aviser les intervenants externes identifiés précédemment ainsi que le moment et le moyen (lettre, courriel, téléphone;

c) s'il y a lieu, il consigne par écrit les motifs justifiant sa décision de ne pas aviser les personnes concernées et les autres intervenants.

Un aide-mémoire pour guider la démarche d'avis aux personnes et organismes concernés est reproduit à l'annexe 3.

[6] Ce formulaire est adapté suivant les exigences de l'article 3 du Règlement sur les incidents de confidentialité, qui énonce les informations à transmettre à la CAI. L'article 4 de ce même Règlement prévoit en outre que l'organisme doit transmettre à la CAI tout renseignement énoncé à l'article 3 porté à sa connaissance après la transmission de l'avis visé à ce même article et ce, avec diligence.

6.5. Inscription au registre des incidents de confidentialité

Tout incident de confidentialité doit être inscrit au registre des incidents de confidentialité du CSBE par la personne ou l'équipe responsable de la gestion de la situation / de l'incident). La RPRP doit en être informée.

6.6. Évaluation approfondie et prévention

Après avoir posé les gestes à caractère plus urgent identifiés plus haut, le CSBE doit réaliser une évaluation plus approfondie de l'incident, dans un souci de prévention et d'amélioration de ses façons de faire. Plus précisément, il doit :

a) approfondir l'analyse des circonstances de l'incident et effectuer une description chronologique des événements et des actions prises face à cet incident, incluant les dates et les intervenants concernés;

b) répertorier et examiner son cadre normatif (normes, politiques ou directives internes) en place au moment de l'incident, autant sur les plans de la sécurité informatique, lorsque l'information est en cause, que de la protection des renseignements personnels en général;

c) vérifier si ce cadre normatif a été suivi par les personnes impliquées (et déterminer les raisons pour lesquelles elles n'ont pas été suivies, le cas échéant);

d) s'il s'agit d'une erreur de procédure ou d'une défaillance opérationnelle, les consigner au dossier de sécurité et adapter ses processus pour éviter qu'un tel incident se reproduise;

e) évaluer la nécessité de se doter d'un énoncé de politique et/ou de règles plus spécifiques en matière de traitement d'une perte ou d'un vol de renseignements personnels;

f) formuler des recommandations relatives à des solutions à moyen et à long terme et à d'éventuelles stratégies de prévention, s'il l'estime nécessaire;

g) s'assurer de la réelle nécessité de la collecte des renseignements personnels concernés;

h) s'assurer du suivi devant être accordé, notamment en ce qui concerne :

- le processus de traitement qui doit être appliqué lors d'une perte ou d'un vol de renseignements personnels et les résultats obtenus, afin de l'améliorer, s'il y a lieu;
- les mesures de sécurité requises à la suite de l'incident et leur performance;
- la communication de l'information pertinente à la CAI et au service de police impliqué, s'il y a lieu.

7. Rôles et responsabilités

Au CSBE, les rôles et responsabilités, en matière d'accès à l'Information et de protection des renseignements personnels, sont définis dans sa politique organisationnelle.

Plus spécifiquement lors d'un incident de confidentialité,

7.1. La personne impliquée dans celui-ci ou alertée de la survenance réelle ou potentielle d'un tel incident

a) elle procède à l'évaluation sommaire de la situation;

b) elle informe le directeur de l'administration;

c) elle collabore avec le ou les responsables de la gestion de l'événement, le directeur de l'administration et la RPRP tout au long du processus.

7.2. Le Directeur de l'administration

a) il informe la RPRP;

b) il détermine, avec cette dernière s'il y a lieu, le partage des responsabilités pour les suites à donner;

c) il désigne la personne ou l'équipe responsable de la gestion de la situation;

d) il informe les intervenants concernés à l'interne.

7.3. La personne (l'équipe) responsable de la gestion de la situation

a) elle collabore avec le directeur de l'administration, notamment quant au partage des responsabilités pour les suites à donner;

b) elle prend au besoin les mesures adéquates afin de limiter les conséquences, pour les personnes concernées, d'une possibilité d'utilisation malveillante de leurs renseignements personnels; au besoin, elle sollicite la collaboration de la RPRP;

c) elle inscrit l'incident au registre des incidents de confidentialité du CSBE.

7.4. La responsable de la protection des renseignements personnels (RPRP)

a) En cohérence avec ses responsabilités suivant la politique organisationnelle du CSBE, elle coordonne la mise en œuvre, l'application et la mise à jour du présent cadre de gestion, en collaboration avec le directeur de l'administration;

b) En collaboration avec le directeur de l'administration,

- elle évalue la nécessité d'informer les autorités externes concernées;
- elle procède à l'évaluation des risques de préjudice sérieux;
- elle détermine, sur la base de son évaluation, qui doit être mis au courant de la perte ou du vol de renseignements personnels, et selon quelles modalités;
- elle réalise *a posteriori* une évaluation plus approfondie de l'incident;

c) elle fournit à ce dernier, ainsi qu'à toute autre personne impliquée dans un incident de confidentialité, son soutien et son expertise de pointe en matière de protection des renseignements personnels;

d) elle offre de façon générale son soutien et son expertise à l'ensemble du personnel du CSBE., notamment par des activités de sensibilisation et de formation, en ce qui a trait aux incidents de confidentialité.

8. Adoption et entrée en vigueur

Le présent cadre de gestion entre en vigueur le jour de son adoption.

Signé à Québec ce 19e jour de janvier 2023

_____

Joanne Castonguay, commissaire

ANNEXE 1

Dispositions de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1) relatives aux incidents de confidentialité (articles 63.8 à 63.11)

« **63.8.** Un organisme public qui 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. Si l'incident présente un risque qu'un préjudice sérieux soit causé, l'organisme doit, avec diligence, aviser la Commission. Il doit également aviser toute personne dont un renseignement personnel est concerné par l'incident, à défaut de quoi la Commission peut lui ordonner de le faire. Il peut également aviser toute personne ou tout organisme susceptible 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 la protection des renseignements personnels doit enregistrer la communication.

Malgré le deuxième alinéa, 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 chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois. Un règlement du gouvernement peut déterminer le contenu et les modalités des avis prévus au présent article.

63.9. Pour l'application de la présente loi, on entend par « incident de confidentialité » : 1° l'accès non autorisé par la loi à un renseignement personnel; 2° l'utilisation non autorisée par la loi d'un renseignement personnel; 3° la communication non autorisée par la loi d'un renseignement personnel; 4° la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

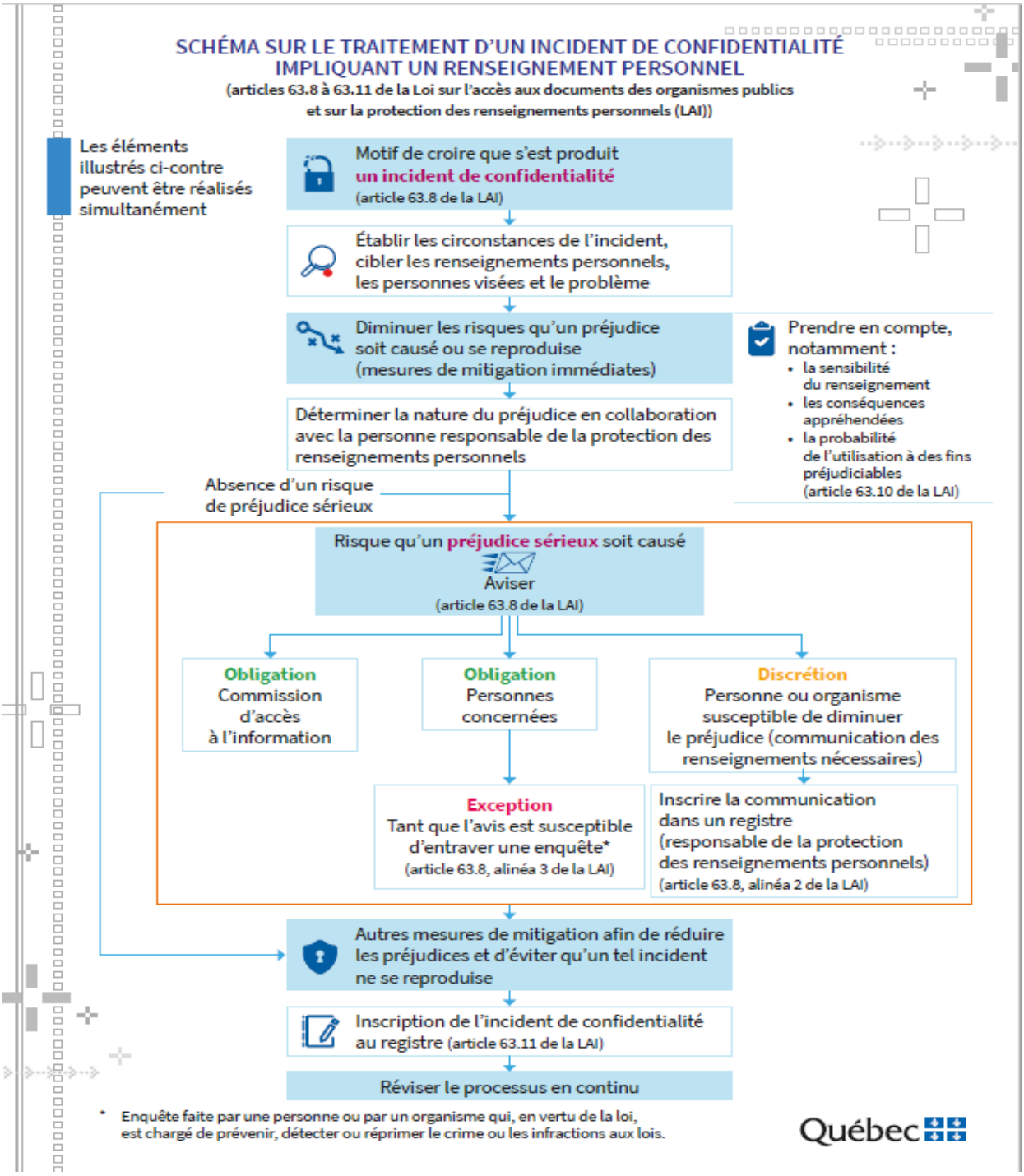
63.10. Lorsqu'il évalue le risque qu'un préjudice soit causé à une personne dont un renseignement personnel est concerné par un incident de confidentialité, un organisme public doit considérer notamment la sensibilité du

renseignement concerné, les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables. L'organisme doit également consulter son responsable de la protection des renseignements personnels.

63.11. Un organisme public doit tenir un registre des incidents de confidentialité. Un règlement du gouvernement peut déterminer la teneur de ce registre. Sur demande de la Commission, une copie de ce registre lui est transmise. »

Cliquez sur le lien pour accéder au Règlement sur les incidents de confidentialité.

ANNEXE 2



Source
[En ligne], https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/conseil-executif/publications-adm/sairid/schema-incident-confidentialite-renseignement-personnel.pdf?1642792255

ANNEXE 3

Avis aux personnes concernées par une perte ou un vol
de leurs renseignements personnels

AVIS AUX PERSONNES CONCERNÉES PAR UNE PERTE OU UN VOL DE LEURS RENSEIGNEMENTS PERSONNELS :

Selon les circonstances, il pourrait s'avérer nécessaire d'aviser les personnes victimes de la perte ou du vol de leurs renseignements personnels. Cet avis pourrait inclure certains des éléments suivants :

- le contexte de l'incident et le moment où il s'est produit ainsi qu'une description de la nature des renseignements personnels touchés ou potentiellement touchés, sans dévoiler de renseignements personnels spécifiques;
- une description sommaire des mesures prises afin de limiter ou de prévenir tout préjudice, ainsi que la liste des personnes qui ont été informées de la situation (service de police, Commission d'accès à l'information, etc.);
- les actions prises par les organismes et les entreprises pour aider les personnes concernées (service d'aide et d'information, abonnement à une alerte de crédit, etc.);
- les mesures que les personnes concernées peuvent prendre afin de réduire les risques de préjudice ou pour mieux se protéger (référence au document « Le vol d'identité en bref! » disponible sur le site Internet de la Commission d'accès à l'information);
- les autres documents d'information générale conçus pour aider les personnes à se prémunir contre le vol d'identité;
- les coordonnées d'un interlocuteur de l'organisation qui peut répondre aux questions et à qui il est possible d'effectuer tout signalement;
- les principales mesures qui seront prises pour éviter que la situation ne se reproduise (changement de pratique ou de processus, formation du personnel, révision ou élaboration de politiques, vérification, suivi périodique, etc.).

Source : *Aide-mémoire à l'intention des organismes et des entreprises – Quoi faire en cas de perte ou de vol de renseignements personnels?*, [En ligne], https://www.cai.gouv.qc.ca/documents/CAI_FI_vol_rens_pers_org-ent.pdf