



AIDE-MÉMOIRE

À L'INTENTION DES ORGANISMES ET DES ENTREPRISES

QUE FAIRE EN CAS DE PERTE

OU DE VOL DE RENSEIGNEMENTS PERSONNELS?

La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* ainsi que la *Loi sur la protection des renseignements personnels dans le secteur privé* imposent aux organismes publics et aux entreprises privées des obligations en ce qui a trait à la collecte, à la conservation, à l'utilisation et à la communication des renseignements personnels.

En règle générale, les renseignements personnels qu'une entreprise ou un organisme détient sont confidentiels, sauf exceptions prescrites par la Loi. Les organismes et les entreprises ont l'obligation de prendre les mesures de sécurité propres à assurer la protection de ces renseignements personnels.

La Commission d'accès à l'information est convaincue que des mesures de sécurité adéquates peuvent contribuer à limiter les risques d'utilisation ou de communication inappropriée de renseignements personnels. Toutefois, une perte ou un vol de ces renseignements personnels peut survenir et mettre en cause la confidentialité de l'information.

Lorsqu'une perte de renseignements personnels se produit, une des préoccupations de la Commission d'accès à l'information est de s'assurer que l'entreprise ou l'organisme prend les moyens nécessaires afin d'éviter ou de limiter le préjudice que les personnes concernées par les renseignements personnels peuvent subir. Informer rapidement les personnes concernées est un moyen efficace de limiter ou même de prévenir tout préjudice.

Il est également essentiel que des mesures de sécurité adéquates soient prises afin d'éviter qu'un tel incident ne se reproduise. La Commission d'accès à l'information peut vous accompagner et vous conseiller dans vos démarches.

Cet aide-mémoire est un outil que la Commission d'accès à l'information met à la disposition des organismes et des entreprises pour les aider à évaluer la situation lors d'une perte ou d'un vol de renseignements personnels. Il s'agit d'un guide et les principales étapes énoncées ne sont pas exhaustives.

Québec (siège)
Bureau 1.10
575, rue Saint-Amable
Québec (Québec) G1R 2G4
Téléphone : 418 528-7741
Télocopieur : 418 529-3102

Montréal
Bureau 18.200
500, boul. René-Lévesque Ouest
Montréal (Québec) H2Z 1W7
Téléphone : 514 873-4196
Télocopieur : 514 844-6170

Téléphone sans frais pour les deux bureaux : 1 888 528-7741

Courrier électronique : cai.communications@cai.gouv.qc.ca

Site Internet : www.cai.gouv.qc.ca

PRINCIPALES ÉTAPES À SUIVRE LORS D'UNE PERTE OU D'UN VOL DE RENSEIGNEMENTS PERSONNELS

ÉTAPE 1 : ÉVALUATION PRÉLIMINAIRE DE LA SITUATION

1. Définir sommairement le contexte de la perte ou du vol de renseignements personnels :

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

2. Informer les autorités externes concernées qui doivent être avisées de l'incident immédiatement (avant l'évaluation des risques) :

- Service de police (si les circonstances laissent croire à la possibilité d'un crime);
- Commission d'accès à l'information.

3. Désigner une personne ou une équipe responsable de la gestion de la situation.

4. Informer les intervenants concernés à l'interne :

- Dirigeants de l'organisme ou de l'entreprise;
- Responsable de l'unité administrative concernée;
- Responsable de la protection des renseignements personnels;
- Conseiller juridique;
- Direction des communications (gestion des médias et des appels de la clientèle).

ÉTAPE 2 : LIMITER L'ATTEINTE À LA VIE PRIVÉE

L'organisme ou l'entreprise doit prendre sans tarder des mesures adéquates pour limiter les conséquences pour les personnes concernées d'une possibilité d'utilisation malveillante de leurs renseignements personnels, de l'usurpation ou du vol de leur identité :

- 1. Prendre des mesures afin de limiter immédiatement 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;**
- 2. Récupérer les dossiers physiques ou numériques, selon le cas;**
- 3. Révoquer ou modifier les mots de passe ou les codes d'accès informatiques;**
- 4. Contrôler les lacunes dans les systèmes de sécurité.**

ÉTAPE 3 : ÉVALUER LES RISQUES

- 1. Compléter une évaluation préliminaire des risques, en considérant la sensibilité des renseignements personnels en cause, tenant compte de leur nature, leur quantité, la possibilité de les combiner avec d'autres renseignements, les personnes concernées, etc.;**
- 2. Déterminer le contexte de l'incident incluant :**
 - La cause (ex. : le caractère délibéré ou non de la perte ou du vol de renseignements personnels, l'erreur humaine, une faille informatique, etc.);
 - Les auteurs connus ou probables des renseignements personnels perdus ou subtilisés (ex. organisation criminelle, public en général, etc.);
 - L'étendue de la situation (nombre de personnes touchées et secteurs touchés);
 - Le caractère systémique ou non de la disparition des renseignements personnels (particulièrement lorsque la perte n'est pas générée directement par une intervention humaine);
 - Une évaluation de la probabilité qu'un événement similaire se reproduise.
- 3. Évaluer la possibilité que les renseignements personnels concernés fassent l'objet d'une utilisation préjudiciable pour les personnes concernées en tenant compte, notamment, des mesures de sécurité prises pour les protéger, de leur difficulté d'accès et de leur intelligibilité (mot de passe, encodage, etc.);**
- 4. Évaluer le caractère réversible ou non de la situation, dont la possibilité de récupérer les renseignements personnels;**

5. **Évaluer si les mesures immédiates prises étaient adéquates pour limiter l'atteinte et les compléter si nécessaire;**
6. **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;**
7. **Déterminer les priorités et identifier les actions à prendre à partir des résultats de l'évaluation de ces risques.**

ÉTAPE 4 : AVISER LES ORGANISATIONS ET PERSONNES CONCERNÉES

1. Déterminer qui doit être mis au courant de la perte ou du vol de renseignements personnels en fonction de l'évaluation des risques :

- Service de police : dans les cas où la disparition peut résulter de la commission d'un crime, le service de police concerné doit être avisé des éléments entourant cette disparition tout d'abord et, ensuite, de toutes les démarches subséquentes. Il est nécessaire de porter une attention particulière afin de ne pas nuire à l'enquête et de préserver les éléments de preuve pouvant être pertinents;
- Personnes concernées : si la perte ou le vol de renseignements personnels présente un risque de préjudice pour les personnes concernées, celles-ci devraient en être avisées sans tarder. Il ne s'agit pas d'alarmer mais de prévenir afin de leur permettre de prendre les mesures pertinentes pour protéger leurs renseignements personnels;
- Commission d'accès à l'information : si les personnes concernées par les renseignements personnels proviennent du Québec, la Commission pourrait amorcer une inspection ou une enquête et jouer un rôle de conseiller dans la recherche de solution;
- Autres : il peut également 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, dans la diffusion des informations concernant la perte de renseignements personnels, une attention particulière doit être portée afin de ne pas aggraver le préjudice que pourraient subir les personnes concernées (ex. : limiter au minimum les renseignements personnels dans les avis).

2. **Désigner les personnes responsables d'aviser les intervenants externes identifiés précédemment ainsi que le moment et le moyen (lettre, courriel, téléphone);**
3. **Le cas échéant, identifier et consigner les motifs à l'origine de la décision de ne pas aviser les personnes concernées et les autres intervenants.**

**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 alerte 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 » disponible à 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, la formation du personnel, la révision ou l'élaboration de politiques, une vérification, un suivi périodique, etc.).

ÉTAPE 5 : ÉVALUATION APPROFONDIE DE LA SITUATION ET PRÉVENTION

- 1. Approfondir l'analyse des circonstances de la perte ou du vol des renseignements personnels et effectuer une description chronologique des événements et des actions prises face à cet incident, incluant les dates et les intervenants concernés;**
- 2. Répertorier et examiner les normes, politiques ou directives internes en place au moment de l'incident, autant au niveau de la sécurité informatique, lorsque l'information est en cause, que de la protection des renseignements personnels en général;**
- 3. Vérifier si ces normes, politiques ou directives internes ont été suivies par les personnes impliquées; identifier les raisons pour lesquelles elles n'ont pas été suivies, le cas échéant;**

- 4. S'il s'agit d'une erreur de procédure ou d'une défaillance opérationnelle, les consigner au dossier de sécurité et adapter les processus pour éviter qu'un tel incident ne survienne à nouveau;**
- 5. Évaluer la nécessité d'élaborer une politique en matière de traitement d'une perte ou d'un vol de renseignements personnels au sein de l'organisme ou de l'entreprise;**
- 6. Formuler les recommandations relatives aux solutions à moyen et long termes et aux stratégies de prévention;**
- 7. S'assurer de la réelle nécessité, pour l'organisme ou l'entreprise, de la collecte des renseignements personnels concernés;**
- 8. Prévoir le suivi devant être accordé.**

ÉTAPE 6 : SUIVI

Il est important d'effectuer le suivi :

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