Réseau des responsables de l'accès aux documents et de la protection des renseignements personnels

BULLETIN D'INFORMATION

BULLETIN N^{O} 15
Décembre 2019

Mot de la direction

En cette saison automnale, c'est avec plaisir que je vous transmets une nouvelle édition du bulletin d'information qui a été préparé pour vous.

Ce numéro est une édition spéciale au sujet des incidents de confidentialité étant donné les diverses fuites de renseignements personnels qui ont eu lieu au cours de la saison estivale. Mon équipe et moi souhaitons également aborder les travaux au sujet de la modernisation des lois en matière de protection des renseignements et des formations dont pourront bénéficier les responsables de l'accès à l'information et de la protection des renseignements personnels et leur équipe.

Bonne lecture!

Réda Haddoud, directeur
Direction de l'accès à l'information et de la protection des renseignements personnels

Dans ce numéro

VOUS EN APPRENDREZ DAVANTAGE SUR :

Votre gouvernement

QUOI DE NEUF?

Renforcement des lois en matière de protection des renseignements personnels

Le Secrétariat à l'accès à l'information et à la réforme des institutions démocratiques (SAIRID) a amorcé une réflexion au regard de la modernisation des lois dans le domaine de la protection des renseignements personnels afin, entre autres, de tenir compte des avancées technologiques et des nouveaux droits y étant associés. À cet égard, le SAIRID s'inspirera des tendances internationales et nationales.

De plus, trois ministres travaillent activement pour encadrer adéquatement la protection des renseignements personnels :

- Le ministre des Finances a déjà déposé un projet de loi pour encadrer les agences de crédits;
- Le ministre délégué à la Transformation numérique gouvernementale travaille actuellement sur une Politique québécoise de cybersécurité;
- Le ministre responsable des Institutions démocratiques, de la Réforme électorale et de l'Accès à l'information travaille sur un projet de loi pour encadrer la protection des renseignements personnels dans les secteurs public et privé, et également en matière de gestion des renseignements personnels par les partis politiques.

ACTUALITÉ

Incident de confidentialité

Les renseignements personnels détenus par une entreprise ou un organisme public dans ses systèmes informatiques ou sur tout autre support ne sont pas à l'abri d'incidents de confidentialité qui peuvent résulter d'erreurs humaines, de défaillances techniques ou d'actes de malveillance. En 2019 au Québec, plusieurs fuites ont compromis la confidentialité des renseignements personnels de nombreux Québécois (Mouvement Desjardins, Capital One, Revenu Québec et Industrielle Alliance, etc.)

Or, ces incidents sont susceptibles de mener à un vol d'identité ou à des conséquences graves sur la vie privée d'une personne, avec toutes les répercussions négatives que cela entraine chez les personnes concernées surtout si elles n'en sont pas informées afin qu'elles prennent des mesures protectrices adéquates. Il est donc important pour un organisme public ou une entreprise d'agir avec vigilance et diligence.

Outre l'impact qu'ils peuvent avoir sur les personnes concernées, les incidents de confidentialité constituent un risque d'affaires important pouvant porter atteinte à la confiance de la population envers les entreprises et les organismes publics.

Vraisemblablement, les vols de renseignements personnels continueront d'augmenter en raison d'une plus grande utilisation d'Internet et des technologies électroniques.

Les organismes publics et les entreprises n'ont pas seulement l'obligation de prendre des mesures pour assurer la protection des renseignements personnels, ils doivent également suivre les développements technologiques afin que leurs mesures soient à jour et optimales afin de limiter les incidents de confidentialité, surtout lorsque les renseignements personnels en cause sont sensibles.

Question d'application

Stratégie d'intervention lors d'un incident de confidentialité

Lors d'un incident de confidentialité, il est essentiel d'agir avec diligence et d'intervenir de manière efficace afin de prévenir ou de limiter les conséquences préjudiciables pour la personne concernée, l'organisme public ou l'entreprise. Un tel incident peut se matérialiser de différentes façons et il se manifeste le plus couramment par :

- un vol ou une perte d'un renseignement;
- un manquement au devoir de confidentialité (communication d'un renseignement personnel à une personne qui n'en a pas besoin dans le cadre de l'exercice de ses fonctions);
- une utilisation de renseignements personnels à des fins non autorisées par la loi;
- une communication d'un renseignement personnel transmise par erreur à un mauvais destinataire;
- une erreur de processus ou une défaillance opérationnelle (erreur de programmation).

Les principales étapes :

1. Limitation de l'incident de confidentialité et l'évaluation préliminaire

   A. Un organisme doit sans tarder prendre les mesures pour limiter et restreindre les conséquences de l'incident de confidentialité
      - *Limiter immédiatement la brèche de l'incident, par exemple* :
        - Cesser promptement la pratique non autorisée;

- Récupérer les dossiers, les renseignements ou exiger leurs destructions et une confirmation écrite de la personne qui les a détruits;
- Révoquer ou modifier les mots de passe ou les codes d'accès;
- Corriger les lacunes des systèmes informatiques ou des processus.

B. Un organisme doit procéder à l'évaluation préliminaire de la situation en désignant une personne coordonnatrice de l'évaluation. Cette personne s'adjoint les collaborateurs requis pour :

- *Établir le contexte de l'incident et obtenir, le cas échéant, les précisions requises* :
  - Identifier les renseignements confidentiels ainsi que le support utilisé (physique ou électronique);
  - Identifier les personnes concernées par l'incident;
  - Établir et identifier les circonstances de l'incident de confidentialité :
    - Que s'est-il passé?
    - Quelle en est la raison?
    - Quelles sont les personnes impliquées?
    - Quels sont les composantes ou les actifs affectés?
    - S'agit-il d'un incident isolé?
- *Répertorier les mesures de sécurité physiques et informatiques ou techniques en place;*
- *Identifier les vulnérabilités liées à l'incident.*

2. Évaluation des risques liés à l'incident

Afin de déterminer les risques de préjudices, procéder à une évaluation de ces risques en tenant notamment compte des facteurs suivants :

- *Des renseignements confidentiels en cause :*
  - La sensibilité des renseignements;
  - La quantité des renseignements et la possibilité de les combiner avec d'autres renseignements;
  - Les préjudices prévisibles pour les personnes concernées, l'utilisation qui peut être faite des renseignements personnels – fins frauduleuses, vol d'identité, etc., et les tierces parties impliquées. Il est à noter que plus les renseignements confidentiels sont sensibles, plus les risques de préjudice sont élevés.

- *De la cause et de l'étendue de l'incident de confidentialité :*
  - Établissement de la cause et de l'étendue de la situation;
  - Impact sur la mission de l'organisme public;
  - Évaluation des mesures prises pour limiter l'incident de confidentialité et y ajouter les mesures correctives si nécessaire pour prévenir tout risque d'incident similaire.
  - Si l'incident de confidentialité peut avoir des conséquences sérieuses, la Commission d'accès à l'information doit être avisée. Lorsqu'il y a possiblement une activité criminelle, la police doit également en être avisée.

3. Détermination et mise en œuvre des priorités d'actions

Afin d'atténuer les risques de préjudices pour les personnes concernées :

- *Notification de l'incident de confidentialité*
  - Déterminer les personnes qui doivent être avisées et le responsable de la démarche
- *Déterminer le moyen de communication et définir le contenu de la notification :*
  - Déterminer le moyen de communication approprié eu égard aux personnes concernées (par téléphone, par envoi postal ou en personne). Le recours à la notification générale et indirecte ne doit être envisagé que dans le cas d'un incident de confidentialité majeur, lorsqu'il n'est pas possible d'identifier clairement les personnes concernées par l'incident dans un délai raisonnable ou lorsqu'il n'est pas possible de rejoindre les personnes concernées (ex. : les coordonnées des personnes ne sont pas détenues).
  - Définir le contenu de la notification en fonction de la nature d'un incident de confidentialité et en tenant compte des catégories de personnes concernées (personne physique ou morale directement ou indirectement impliquée) :
    - Aperçu des faits;
    - Renseignements confidentiels en cause;
    - Description sommaire des mesures mises en place et des actions prises;

- Mesures que les personnes concernées peuvent prendre afin de réduire les risques de préjudice et les sources d'information aidant les personnes à se protéger, le cas échéant;
- Coordonnées d'une personne-ressource pour répondre aux interrogations;
- Principales mesures qui seront prises pour éviter que la situation ne se reproduise.

4. Évaluation approfondie et prévention

À la suite de la mise en place des mesures de prévention, les personnes responsables doivent :

- *Analyser adéquatement les circonstances ayant mené à l'incident de confidentialité (cause, ordre chronologique, date des interventions).*
- *Explorer la pertinence de mettre en place un plan de prévention, incluant les éléments suivants :*
  - Vérification de la sécurité physique et technique;
  - Examen des normes, des politiques ou des directives internes en place au moment de l'incident;
  - Vérification des pratiques du personnel impliqué et des mandataires ou partenaires, le cas échéant;
  - Élaboration de recommandations relatives aux solutions à mettre en place à moyen et long terme;
  - Révision d'un suivi sur les mesures mises en place.
- *Mettre en œuvre le plan de prévention, si nécessaire.*

Information de nature juridique

Manquement aux règles de protection des renseignements personnels en matière d'incidents de confidentialité

Il est important de rappeler au personnel qu'un incident peut avoir des conséquences regrettables.

- *La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (Loi sur l'accès)*

Une personne peut faire l'objet d'une poursuite pénale pour une infraction prévue à la section I du chapitre VII de la Loi sur l'accès. Ainsi, une personne qui communique des renseignements personnels sans que cela soit autorisé par la loi pourrait faire l'objet d'une poursuite pénale.

- *Contrat*

Sans oublier les prestataires de services et les mandataires. D'ores et déjà, lors de la signature d'un contrat dont le mandat requiert l'accès à des renseignements personnels, il est nécessaire d'inclure des clauses de protection des renseignements personnels et de prévoir la possibilité de résilier le contrat en cas de non-respect des exigences en matière de protection des renseignements personnels. De plus, il est possible de prévoir des pénalités en cas de non-respect de ces exigences. Par conséquent, si le contractant ne respecte pas ces obligations, l'organisme pourra agir et appliquer les pénalités prévues.

- *Mesures disciplinaires*

Un membre du personnel d'un organisme public peut, selon les normes en matière de relation de travail, faire l'objet de mesure disciplinaire allant jusqu'au congédiement, selon la gravité de la faute.

- *Accusation aux criminelles*

Le vol de renseignements personnels peut également donner lieu à des accusations aux criminelles.

Direction de l'accès à l'information et de la protection des renseignements personnels

Ministère du Conseil exécutif
875, Grande-Allée Est, 3e étage
Québec (Québec) G1R 4Y8

Pour nous joindre :

Téléphone : 418 528-8024

Messagerie :
DAIPRP@mce.gouv.qc.ca

Secrétariat à l'accès à l'information et à la réforme des institutions démocratiques
Québec