| | | |
|---|---|---|
| SPA mobile du Québec | **Procédure de gestion des incidents de confidentialité**<br>**SPA Mobile du Québec** | |
| | **Entrée en vigueur** | 21 septembre 2023 |
| | **Présenté par** | Conseil d'administration |
| | | |

## 1 - Incident de confidentialité

Les dispositions contenues dans les articles 63.8 à 63.11 de la Loi sur l'accès définissent le concept de violation de la confidentialité et énoncent les procédures auxquelles se conforme la SPA Mobile du Québec. Ces articles énumèrent les critères que l'entité publique concernée doit prendre en considération lors de l'évaluation des risques de préjudice pour une personne dont les données personnelles sont affectées par une violation de la confidentialité.

## 2 - Communication des notifications à la Commission d'accès à l'information et aux parties affectées

En cas d'incident présentant un risque significatif de préjudice pour les individus concernés, la SPA Mobile du Québec est tenue de notifier immédiatement la Commission d'accès à l'information (CAI). De plus, elle doit informer les parties concernées par l'incident, à moins que cela puisse entraver une enquête menée par une personne ou une entité autorisée par la loi à prévenir, détecter ou réprimer des activités criminelles ou des violations de la loi. Dès que l'information ne risque plus d'entraver une telle enquête, l'entité publique doit rapidement informer les personnes concernées.

## 3 - Évaluation du préjudice

Dans le cas d'une atteinte à la confidentialité, l'entité publique est tenue d'évaluer si cela comporte un risque potentiel de préjudice pour une personne dont les données personnelles sont en jeu. À cette fin, elle doit prendre en compte divers éléments, notamment :

1. La sensibilité des informations personnelles, telles que des données financières ou des informations d'identification ;

2. Les conséquences anticipées de l'utilisation de ces données, notamment le risque de vol d'identité, de fraude financière ou de graves atteintes à la vie privée ;

3. La probabilité que ces informations puissent être utilisées à des fins préjudiciables.

Un préjudice sérieux se réfère à un acte ou à un événement pouvant causer un dommage significatif à la personne concernée ou à ses biens, ayant un impact non négligeable sur ses intérêts. Cela peut engendrer, par exemple :

- La dégradation de la réputation ;
- Une perte financière ;
- L'humiliation ;
- Le vol d'identité ;
- Des répercussions négatives sur le dossier de crédit ;
- Une perte d'emploi.

## 4 - Tenue d’un registre des incidents de confidentialité

La SPA Mobile du Québec tient un registre exhaustif de tous les incidents de confidentialité auxquels elle a été confrontée, y compris ceux qui ne présentent pas de risque substantiel de préjudice pour les individus concernés.

La Commission d'accès à l'information (CAI) a le droit de consulter les données recueillies dans ce registre, et une copie de celui-ci doit lui être fournie sur demande.

## 5 - Pouvoirs d’ordonnance de la Commission d’accès à l’information

La SPA Mobile du Québec tient compte du fait que la Commission d'accès à l'information (CAI) détient plusieurs pouvoirs d'ordonnance en relation avec les incidents de confidentialité.

*Elle a notamment le pouvoir d'ordonner :*

- À un organisme public qui a été victime d'un incident entraînant un risque grave de préjudice et qui a omis d'informer les personnes dont les données personnelles sont concernées par cet incident, de les informer immédiatement.
- À toute partie de mettre en place les mesures nécessaires pour protéger les droits des personnes affectées.
- La restitution des informations personnelles impliquées dans l'incident de confidentialité à l'organisme public qui les détenait, ainsi que leur destruction.

Le gouvernement a mis en vigueur le *Règlement sur les incidents de confidentialité*, visant principalement à préciser les détails entourant les notifications à transmettre à la Commission d'accès à l'information et aux individus touchés lorsqu'un incident de confidentialité engendre un préjudice sérieux. Il spécifie également le contenu requis pour le registre à maintenir par les entités publiques.

## 6 - Gestion des incidents de confidentialité

### A. Évaluation de la situation :

Lorsque la SPA Mobile du Québec soupçonne qu’un incident de confidentialité impliquant des informations personnelles a eu lieu, l’entreprise entreprend les démarches suivantes :

- Examiner les circonstances entourant l'incident ;

- Identifier les données personnelles concernées ;

- Recenser les individus affectés ;

- Diagnostiquer la nature du problème, qu'il s'agisse d'une erreur, d'une faille de sécurité, ou autre. Cette évaluation doit se poursuivre jusqu'à ce que tous les éléments pertinents soient identifiés.

**B. Réduction des risques :**

La SPA Mobile du Québec doit réagir promptement en prenant des mesures raisonnables pour atténuer les risques, qu'ils soient graves ou non, et pour prévenir de futurs incidents similaires. Cela peut inclure des actions telles que :

- Mettre fin à toute pratique non autorisée ;

- Récupérer ou exiger la destruction des données personnelles affectées ;

- Corriger les vulnérabilités informatiques.

**C. Détermination de la nature du préjudice :**

L'objectif est d'établir si une notification à la Commission d'accès à l'information (CAI) et aux personnes concernées est nécessaire, ainsi que de définir les mesures à prendre pour réduire les risques. Par exemple :

- Inclure une note dans les dossiers associés aux risques de vol d'identité ;

- Exiger des vérifications supplémentaires.

**D. Enregistrement dans le registre :**

La SPA Mobile du Québec consigne l’événement dans le registre des incidents, qu'il soit qualifié de sérieux ou non en termes de préjudice potentiel.

**E. En cas de risque de préjudice sérieux :**

- Notification à la CAI : La SPA Mobile du Québec informe immédiatement la CAI, même si toutes les informations relatives à l'incident ne sont pas encore disponibles. La SPA Mobile du Québec peut ainsi signaler l'incident à la CAI et compléter la déclaration ultérieurement, y compris le nombre précis de personnes concernées.

- Notification des personnes affectées : La SPA Mobile du Québec informe toutes les personnes dont les informations personnelles sont affectées par l'incident, sauf si cette notification risque de compromettre une enquête en cours. Un délai peut s'appliquer entre la découverte de l'incident et la notification, afin de rassembler des informations essentielles, d'identifier les individus touchés, de résoudre la faille de sécurité, ou de ne pas entraver une enquête en cours. Ces notifications sont obligatoires.

**F. En cas de risque de préjudice sérieux :**

La SPA Mobile du Québec peut également informer toute personne ou organisation susceptible de réduire ce risque. Dans ce but, l'entreprise peut partager uniquement les informations personnelles nécessaires à cette fin, sans nécessiter le consentement préalable de la personne concernée. Cependant, la Personne responsable de la protection des données personnelles doit documenter cette communication en enregistrant les détails suivants :

- Les destinataires des informations ;
- Les circonstances entourant la communication ;
- Les informations spécifiques transmises ;
- Les objectifs de cette démarche.

**Dernière mise à jour : 21 septembre 2023**