Directive en cas d'incident de confidentialité

Adoptée le 12 septembre 2023

Résolution 2023-09-430

Ici bat le cœur des Laurentides

Table des matières

1. But

Le but de cette directive est de déterminer une démarche à suivre en cas d'incident de confidentialité impliquant des renseignements personnels et assurer la prévention de tels incidents.

La Ville, dans le cadre de ces fonctions, recueille et détient des renseignements personnels. Elle doit donc prendre des mesures de sécurité pour protéger ces renseignements et intervenir en cas d'incident. Ces obligations découlent de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.*

2. Définitions

Comité : Comité sur l'accès à l'information et la protection des renseignements personnels de la Ville.

Incident de confidentialité : Accès non autorisé par la loi à un renseignement personnel, à son utilisation ou à sa communication, de même que sa perte ou toute autre forme d'atteinte à sa protection.

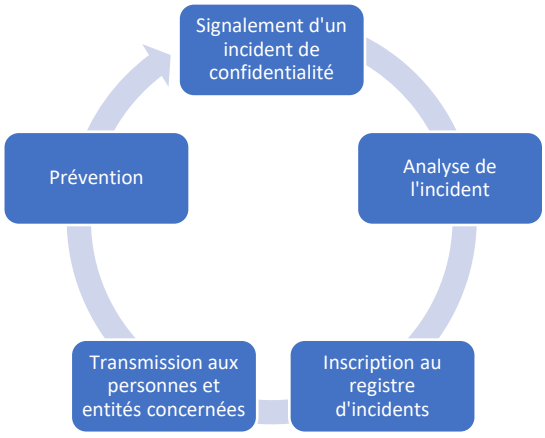
Renseignement personnel : Renseignement permettant d'identifier directement ou indirectement une personne physique.

Préjudice : Atteinte ou dommage subi par une personne.

3. Champ d'application

Cette directive concerne tout incident de confidentialité impliquant des renseignements personnels et s'applique à tout signalement du personnel de la Ville, de ses fournisseurs et de ses consultants.

4. Protocole de gestion des incidents de confidentialité



5. Schéma sur le traitement d'un incident de confidentialité

5.1. Signalement d'un incident de confidentialité

Tout employé qui détecte ou est informé d'un incident de confidentialité doit le signaler immédiatement à son directeur de service qui en informera la personne responsable de la protection des renseignements personnels, même si les circonstances laissent croire qu'il ne s'agit pas d'un incident réel ou qu'il ne causera aucun préjudice aux personnes concernées.

5.2. Analyse de l'incident

Le comité établit, en cas d'incident, les circonstances entourant l'incident. Il cible les renseignements personnels visés et les personnes concernées. Il met en place des mesures immédiates pour limiter les risques de préjudice et pour éviter que la situation se reproduise. Puis, il évalue s'il y a un préjudice et le niveau de préjudice, le cas échéant. Pour cette évaluation, le comité se base sur la grille d'évaluation du niveau de préjudice laquelle est jointe à la présente directive comme annexe A.

5.3. Inscription au registre d'incident

La personne responsable de la protection des renseignements personnels inscrit l'incident de confidentialité dans le registre à cet effet.

5.4. Transmission aux personnes et entités concernées

En cas de préjudice sérieux, la personne responsable de la protection des renseignements personnels avise la Commission d'accès à l'information de l'incident de confidentialité. L'avis doit contenir l'information prescrite par le formulaire de déclaration de la Commission. Elle avise aussi les personnes touchées par les renseignements personnels. L'avis doit être transmis, de préférence, par écrit. Elle doit contenir une description des renseignements personnels visés par l'incident, les circonstances de l'incident, les mesures mise en place pour diminuer les risques de préjudice et les coordonnées de la personne à contacter pour obtenir davantage d'information relative à l'incident.

5.5. Prévention

Le comité en cas d'incident évalue et prend en considération les préventions supplémentaires à appliquer pour qu'un tel incident ne se reproduise plus.

6. Équipe d'intervention en cas d'incident

6.1. Rôle et responsabilité des membres

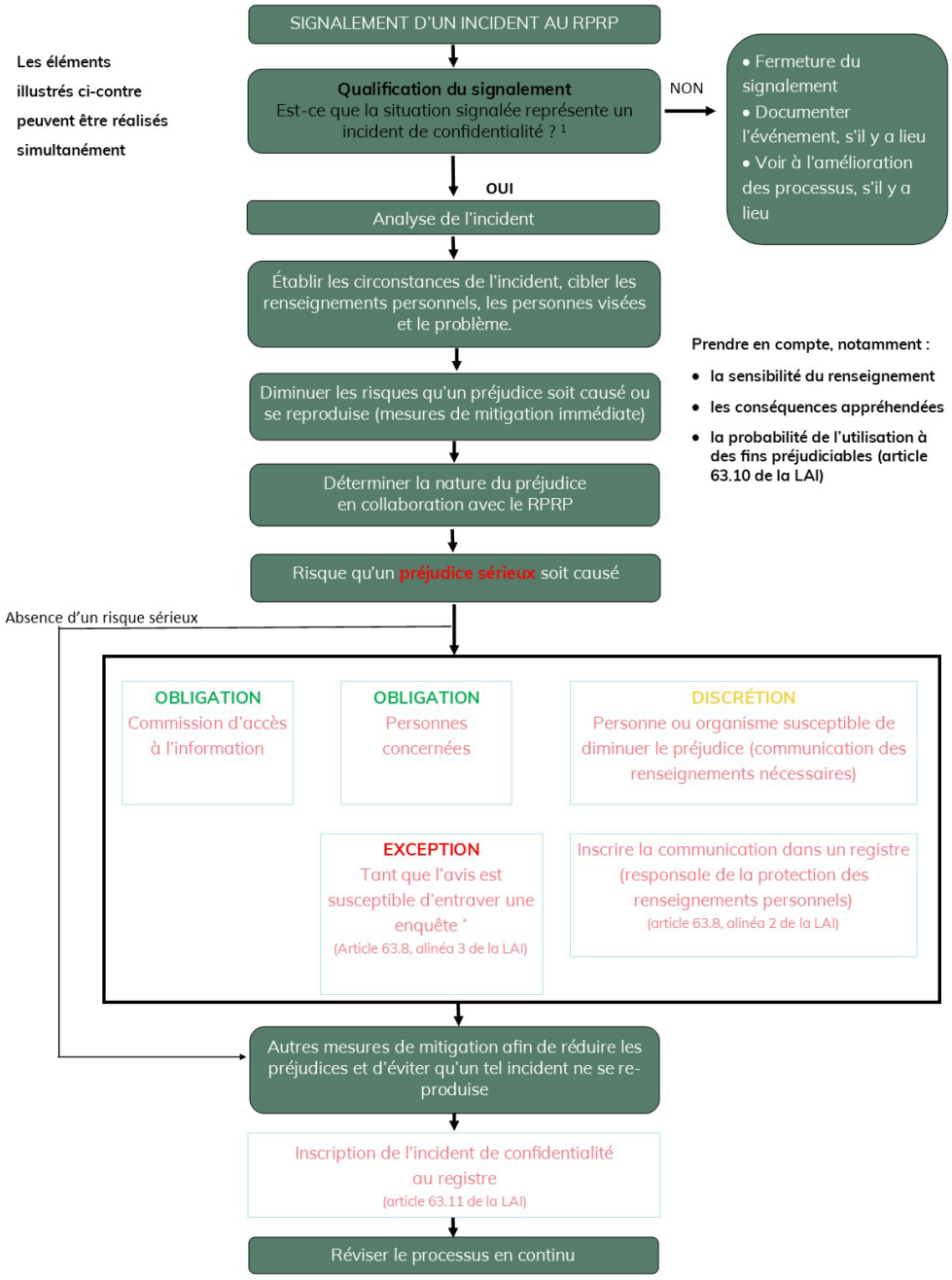
Le tableau ci-dessous présente les rôles et responsabilités des principaux acteurs dans le cadre d'une réponse aux incidents. La nature de l'incident pourrait nécessiter de remanier la composition de l'équipe, que ce soit en ce qui concerne ses membres, leurs rôles ou leurs responsabilités.

Rôle	Responsabilité
Responsable de la protection des renseignements personnels	• Coordonner la mise en place du plan de réponse incident; • Point de contact des communications relatives à l'incident; • Assurer le respect des obligations légales de la Ville.
Spécialiste en technologies de l'information	• Responsable des aspects techniques de l'incident; • Analyser l'incident et gérer les risques techniques; • Mettre en place des mesures de protection et de récupération adéquates.
Comité	• Conseille la Ville relativement à tout incident de confidentialité; • Révise le schéma sur le traitement d'un incident de confidentialité.

Annexe A : Grille d'évaluation des risques de préjudice

	Risque minime 1	Risque faible 2	Risque modéré 3	Risque élevé à inacceptable 4
Risque pour les personnes concernées	Aucun impact n'est envisagé pour les personnes concernées.	Les risques n'outrepassent pas la simple incommodité temporaire, disparaissent à court terme et ne sont pas de nature à affecter les droits et libertés des personnes concernées. Les renseignements personnels visés par le traitement ne sont pas sensibles.	Les personnes concernées sont susceptibles de subir un stress émotionnel, des pertes financières limitées ou couvertes par les assurances ou un sentiment d'intrusion. Les personnes concernées pourraient avoir à entreprendre des démarches relatives à la surveillance de leurs dossiers de crédit, par exemple.	Les risques visent le moyen et long terme. Ils peuvent inclure le vol d'identité, des pertes financières importantes, des effets négatifs sur les cotes de crédit, des pertes d'emplois, des dommages ou pertes de biens, la discrimination, l'extorsion, des menaces à l'intégrité de la personne et menacer la santé physique ou psychologique des personnes concernées.
Impact de la réalisation du risque	L'impact est très faible voire inexistant. Il n'engendre aucune conséquence pour les personnes, ou des conséquences très mineures pour une seule personne. Par exemple, si seuls des coordonnées professionnelles ou des renseignements à caractères publics.	L'impact engendre des conséquences mineures pour une personne ou pour un petit nombre de personnes. Par exemple, si peu de renseignements personnels dépersonnalisés sont touchés.	L'impact engendre des conséquences importantes pour une personnes ou des conséquences mineures pour un grand nombre de personnes. Par exemple, si les personnes touch.es sont des mineurs, des personnes ayant un handicap ou autre.	Le risque engendre des conséquences majeures pour une personne ou des conséquences importantes pour un grand nombre de personnes; si inacceptable, le risque engendre des conséquences trop importantes et/ou implique une non-conformité aux lois.
Probabilité de réalisation du risque	Le risque n'a aucune chance de se concrétiser.	Le risque a peu de chance de se concrétiser ou un événement similaire ne s'est jamais produit.	Le risque a de bonnes chances de se réaliser ou un événement similaire s'est déjà produit à une ou quelques reprises.	Le risque a de très grandes chances de se concrétiser ou un événement similaire s'est produit à plusieurs reprises.

Annexe B : Schéma sur le traitement d'un incident de confidentialité impliquant un renseignement personnel



1 Constitue un incident de confidentialité, toute consultation, utilisation ou communication non autorisée d'un renseignement personnel, la perte d'un tel renseignement, ainsi que toute autre atteinte à sa protection.

* 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.