PROCÉDURE

PROCÉDURE DE TRAITEMENT DES INCIDENTS DE CONFIDENTIALITÉ

Adoptée le 17 octobre 2023

Résolution 182-10-2023

Table des matières

Malgré toutes les précautions que peut prendre la Municipalité afin de protéger vos renseignements personnels en vertu de la *Loi sur l'accès aux documents des organismes publics et la protection des renseignements personnels (ci-après appelée Loi sur l'accès)*, notamment en s'étant dotée d'une Politique concernant les règles de gouvernance en matière de protection des renseignements personnels de la Municipalité, il pourrait se glisser un incident de confidentialité. Selon la Loi, un incident de confidentialité correspond à tout accès, utilisation ou communication non autorisés par la Loi d'un renseignement personnel, de même qu'à la parte d'un renseignement personnel ou à toute autre atteinte à sa protection. Par exemple, un incident de confidentialité pourrait se produire lorsqu'un membre du personnel communique des renseignements personnels au mauvais destinataire ou la Municipalité est victime d'une cyberattaque, tel un hameçonnage, etc.

Lors de la séance ordinaire du 17 octobre 2023, le Conseil de la Municipalité a donc adopté à l'unanimité des Conseillers présents, la Procédure de traitement des incidents de confidentialité ci-après :

CONSIDÉRANT que la Municipalité de Saint-Placide (ci-après la « Municipalité ») est un organisme public assujetti à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ c. A -2.1 (ci-après la « Loi sur l'accès ») ;

CONSIDÉRANT que la Municipalité s'engage à protéger les renseignements personnels qu'elle collecte et traite dans le cadre de ses activités dans le respect des lois et règlements applicables ;

CONSIDÉRANT qu'en 2022, la Municipalité employait, en moyenne, 50 salariés ou moins, et qu'elle n'est donc pas assujettie à l'obligation de constituer un comité sur l'accès à l'information et la protection des renseignements personnels conformément au *Règlement excluant certains organismes publics de l'obligation de former un comité sur l'accès à l'information et la protection des renseignements personnels* ;

CONSIDÉRANT que pour s'acquitter des obligations prévues à la *Loi sur l'accès*, le Conseil a adopté ce jour, la Politique administrative concernant les règles de gouvernance en matière de protection des renseignements personnels et en conséquence, adopte par la présente résolution, la Procédure de traitement des incidents de confidentialité comme suit :

EN CONSÉQUENCE,

Il est proposé par Ghislaine Tessier, appuyée par Marie-Ève D'Amour et résolu :

LE CONSEIL DÉCRÈTE CE QUI SUIT :

Chapitre I – Application et interprétation

Objectif

La présente Procédure vise à encadrer les exigences à respecter ainsi que les mesures à prendre en cas d'incident de confidentialité, le tout en conformité avec les articles 63.8 à 63.11 de la *Loi sur l'accès aux documents des organismes publics et la protection des renseignements personnels* (RLRQ, c. A-2.1).

1. Définitions

Aux fins de la présente Procédure, les expressions ou les termes suivants ont la signification ci-dessous énoncée :

CAI : Désigne la Commission d'accès à l'information créée en vertu de la *Loi sur l'accès*;

Conseil : Désigne le Conseil municipal de la Municipalité de Saint-Placide;

Employé : Désigne un élu, un cadre ou un employé, à temps plein ou à temps partiel, permanent, saisonnier ou contractuel;

Incident de confidentialité : Désigne l'accès, l'utilisation ou la communication non autorisés par la *Loi sur l'accès* de tout renseignement personnel, sa perte ou toute autre atteinte à la protection d'un tel renseignement;

Loi sur l'accès : Désigne la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ c. A -2,1 ;

Personne concernée : Désigne toute personne physique pour laquelle la Municipalité collecte, détient, communique à un tiers, détruit ou rend anonyme, un ou des renseignements personnels ;

Renseignement personnel (ou RP) : Désigne toute information qui concerne une personne physique et qui permet de l'identifier directement ou indirectement, comme : l'adresse postale, le numéro de téléphone, le courriel ou le numéro de compte bancaire, que ce soit les données personnelles ou professionnelles de l'individu ;

Renseignement personnel (ou RP) sensible : Désigne tout renseignement personnel qui suscite un haut degré d'attente raisonnable en matière de vie privée de tout individu, notamment en raison du préjudice potentiel à la personne en cas d'incident de confidentialité, comme l'information financière, les informations médicales, les données biométriques, le numéro d'assurance sociale, le numéro de permis de conduire ou l'orientation sexuelle ;

Responsable de la protection des renseignements personnels (ou RPRP) : Désigne la personne qui, conformément à la *Loi sur l'accès*, exerce cette fonction et veille à la protection des renseignements personnels détenus par la Municipalité.

2. Responsable de l'application

Le RPRP est responsable de voir à l'application de la présente Procédure. Dans le cadre de ses fonctions, il peut se faire assister d'autres employés de la Municipalité. Il peut également, sous réserve des règles de gestion contractuelles et de délégation de pouvoir, utiliser des services externes spécialisés en la matière.

Tous les employés doivent collaborer avec le RPRP dans le cadre de l'application de la présente procédure.

3. Constat de l'incident de confidentialité

Tout employé de la Municipalité qui constate un incident de confidentialité avéré ou potentiel doit aviser sans délai la greffière-trésorière adjointe, à **dga@saintplacide.com** ou par téléphone.

En cas d'absence de cette personne, communiquer avec la greffière-trésorière, à **dg@saintplacide.com** ou par téléphone.

Exemples d'incidents de confidentialité :

- Communication par erreur des renseignements personnels à un mauvais destinataire;
- Un vol de dossier ou de données au moyen de divers moyens technologiques (clé USB, piratage, etc.);
- Accès à des renseignements personnels par une personne non autorisée.

4. Analyse de l'incident de confidentialité

Le RPRP doit analyser l'événement rapporté conformément à l'article 4 de la présente Politique afin de déterminer s'il s'agit effectivement d'un incident de confidentialité.

- **Dans la négative :** aucune action particulière ne doit être prise. Toutefois, considérant les circonstances, le RPRP peut décider d'effectuer un diagnostic afin d'évaluer si les mesures de sécurité mises en place sont fonctionnelles et bien adaptées aux circonstances.
- **Dans l'affirmative :** poursuivre les prochaines étapes.

5. Évaluation de la situation

Le RPRP doit évaluer le risque qu'un préjudice soit causé à une personne concernée dont un RP est touché par l'incident de confidentialité.

Afin d'évaluer le risque de préjudice, le RPPR devra notamment répondre aux questions suivantes :

- Quand l'incident a-t-il eu lieu?
- Quand l'incident a-t-il été constaté?
- Où l'incident a-t-il eu lieu?
  - Dans les locaux de la Municipalité? Lesquels?
  - Chez un tiers détenant des renseignements personnels pour la Municipalité?
  - Est-ce un incident de confidentialité impliquant un lieu physique, un système informatique ou technologique, etc. ?
- Quelles sont les causes probables de l'incident ?
  - S'agit-il d'enjeux de sécurité physique, humaine, technologique, etc.?
  - Quelles mesures de sécurité étaient en place?
  - Pourquoi n'ont-elles pas été efficaces?
- Qui peut avoir eu accès aux RP (employé non autorisé, mandataire, fournisseur, tiers, etc.)?
  - Qui sont les personnes concernées (employés, fournisseur, citoyens, clients, etc.)?
  - Combien y a-t-il de personnes concernées?
  - Quelle est la nature des RP visés par l'incident (à caractère public, renseignements nominatifs, sensibles, etc.)?
  - Il y a-t-il un risque de préjudice sérieux pour les personnes concernées?

Pour évaluer le risque de préjudice, il faut considérer notamment :

- La sensibilité du RP concerné;
- Les utilisations malveillantes possibles;
- Les conséquences appréhendées de son utilisation;
- La probabilité qu'il soit utilisé à des fins préjudiciables.

6. Mise en place de mesure pour diminuer les risques

En fonction de l'évaluation de la situation, le RPRP doit s'assurer que des mesures raisonnables soient mises en place afin de diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature se produisent.

7. Avis en cas de risque de préjudice sérieux

Lorsque l'évaluation de la situation mène à la conclusion qu'il y a un risque de préjudice sérieux pour les personnes concernées :

a. Avis à la CAI

Un avis doit être transmis avec diligence à la CAI. Un modèle d'avis est disponible sur le site internet de la CAI à l'adresse : **https://www.cai.gouv.qc.ca/documents/CAI_FO_avis_incident_confidentialite.pdf**

b. Avis à toutes les personnes concernées

Un avis doit être transmis par écrit, dans les meilleurs délais, aux personnes concernées le tout, conformément au modèle joint en Annexe A de la présente procédure. Dans le but d'agir rapidement et de diminuer ou d'atténuer les risques de préjudices sérieux, un avis public peut également être fait. Toutefois, la publication d'un avis public n'exempte pas la Municipalité de l'envoi d'un avis à chaque personne concernée sauf dans les cas suivants :

- La transmission de l'avis peut causer un plus grand préjudice à la personne concernée;
- La transmission de l'avis représente une difficulté excessive pour la Municipalité;
- La Municipalité n'a pas les coordonnées de la personne concernée;
- Avant de communiquer avec la personne concernée, le RPRP doit s'assurer qu'il détient les bonnes coordonnées.

NOTE : La personne concernée n'a pas à être avisée tant que cela est susceptible d'entraver une enquête faite par une personne ou un organisme chargé par la loi de prévenir, détecter ou réprimer le crime ou les infractions aux lois.

8. Inscrire l'information pertinente au registre des incidents de confidentialité de la Municipalité

Le RPRP doit veiller à ce qu'un registre des incidents de confidentialité soit mis en place à la Municipalité.

Il doit également y inscrire tous les incidents de confidentialité, et ce, même s'ils ne présentent pas de risque de préjudice sérieux.

Les renseignements du registre doivent être conservés pour une période minimale de cinq (5) ans, après la date ou la période de prise de connaissance de l'incident par la Municipalité.

9. Mise à jour et modification de la procédure

La présente procédure devra être modifiée en fonction des changements législatifs, règlementaires, ou autres recommandations de la CAI ou du gouvernement, le cas échéant, afin de s'assurer qu'elle demeure en tout temps en conformité avec les lois applicables et les meilleures pratiques en cette matière.

En cas de modification, tous les employés de la Municipalité devront en être informés afin qu'ils puissent en prendre connaissance.

10. Disposition finale

La présente politique entre en vigueur dès son adoption par le Conseil.

Adoptée le 17 octobre 2023.

POLITIQUE RECONNUE VÉRITABLE
ET ANNEXÉE À LA RÉSOLUTION
NUMÉRO 182-10-2023

_____	_____
Daniel Laviolette, Maire	Lise Lavigne, directrice générale et greffière-trésorière