Politique administrative concernant les règles de gouvernance en matière de protection des renseignements personnels de la Municipalité de Saint-Paulin

Préambule

La Municipalité de Saint-Paulin, organisme public assujetti à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q. c. A-2.1) (ci-après la « Loi sur l'accès »), s'engage à protéger les renseignements personnels qu'elle collecte et traite dans le respect des lois et règlements applicables.

Considérant que la Municipalité emploie en moyenne 50 salariés ou moins en 2022 et n'est donc pas assujettie à l'obligation de constituer un comité sur l'accès à l'information et la protection des renseignements personnels, la présente politique administrative a pour objectif de définir les règles de gouvernance en matière de protection des renseignements personnels.

Chapitre 1 — Application et interprétation

1. Définitions

- **CAI:** Commission d'accès à l'information.
- **Conseil:** Conseil municipal de la Municipalité de Saint-Paulin.
- **Cycle de vie:** Ensemble des étapes d'existence d'un renseignement (création, modification, transfert, consultation, transmission, conservation, archivage, anonymisation, destruction).
- **Loi sur l'accès:** Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.
- **Personne concernée:** Personne physique pour laquelle la Municipalité collecte, détient, communique, détruit ou anonymise des renseignements personnels.
- **Partie prenante:** Personne physique en relation avec la Municipalité (employé, fournisseur, etc.).
- **Politique de gouvernance PRP:** Politique administrative concernant les règles de gouvernance en matière de protection des renseignements personnels.
- **PRP:** Protection des renseignements personnels.
- **Renseignement personnel (RP):** Information concernant une personne physique et permettant de l'identifier (adresse, téléphone, courriel, numéro de compte bancaire, etc.).
- **Renseignement personnel sensible:** Renseignement personnel suscitant un haut degré d'attente raisonnable en matière de vie privée (informations financières, médicales, données biométriques, numéro d'assurance sociale, etc.).
- **Responsable de la protection des renseignement personnels (RPRP) :** Le maire de la municipalité ou la personne qu'il a désigné à la **CAI** comme responsable de la protection des renseignements personnels. Cette personne désignée est identifiée sur le site web de la municipalité de Saint-Paulin.
- **Responsable de l'accès aux documents (RAD):** Personne exerçant cette fonction et répondant aux demandes d'accès aux documents.

- **Actif informationnel:** Information contenant un renseignement personnel ou confidentiel, quel que soit son support.

2. Objectifs

La Politique de gouvernance PRP vise à :

- Énoncer les orientations et principes directeurs en matière de PRP.
- Protéger les RP tout au long de leur cycle de vie.
- Assurer la conformité aux exigences légales (Loi sur l'accès) et aux meilleures pratiques.
- Assurer la transparence du traitement des RP et des mesures de PRP appliquées.

2.1 Champ d'application

La présente politique s'applique à tous les employés, gestionnaires, élus, firmes externes et partenaires qui utilisent ou accèdent aux actifs informationnels de la Municipalité.

Chapitre II — Mesures de protection des renseignements personnels

3. Collecte des renseignements personnels

La Municipalité ne collecte que les RP nécessaires à ses activités, avec le consentement préalable, manifeste, libre et éclairé de la personne concernée, sauf exceptions prévues par la Loi sur l'accès.

Lors de la collecte, la Municipalité indique :

- Les fins de la collecte.
- Le caractère obligatoire ou facultatif de la demande.
- Les conséquences d'un refus ou d'un retrait de consentement.
- Les droits d'accès et de rectification.
- Les moyens de collecte.
- La durée de conservation.
- Les coordonnées du responsable de la PRP.

4. Conservation et utilisation des renseignements personnels

L'utilisation des RP est limitée aux fins pour lesquelles ils ont été recueillis, avec le consentement exprès de la personne concernée, sauf exceptions.

L'accès aux RP est limité aux personnes dont l'accès est requis pour l'exercice de leurs fonctions.

La Municipalité applique des mesures de sécurité équivalentes pour tous les RP, quelle que soit leur sensibilité.

Les données sont conservées pour la durée nécessaire à leur utilisation ou conformément au calendrier de conservation.

La Municipalité s'assure de l'exactitude des RP et la valide régulièrement auprès de la personne concernée.

5. Fichier de renseignements personnels

La Municipalité tient un inventaire de ses fichiers de renseignements personnels, contenant :

- La provenance des renseignements
- Les catégories de personnes concernées
- Les catégories de personnes ayant accès aux fichiers
- Les mesures de sécurité prises

Toute personne peut avoir accès à cet inventaire, sauf exceptions.

6. Communication à des tiers

La communication de RP à des tiers est interdite sans consentement exprès de la personne concernée, sauf exceptions.

Toute transmission de RP à un tiers est consignée dans les registres.

7. Destruction ou anonymisation

Les RP sont détruits de manière irréversible ou anonymisés lorsqu'ils ne sont plus nécessaires ou lorsque le délai de conservation est expiré.

La procédure de destruction doit être approuvée par le greffier-trésorier.

L'anonymisation est irréversible et doit être approuvée par le greffier-trésorier.

Chapitre III — Rôles et responsabilités

8. Responsable de la protection des renseignements personnels (RPRP)

Le RPRP approuve la présente politique et veille à sa mise en œuvre, en s'assurant notamment que :

- Les décisions nécessaires sont prises
- Les directeurs de service promeuvent une culture de protection des RP
- Le RPRP et le RAD peuvent exercer leurs fonctions de manière autonome

9. Direction générale

La direction générale est responsable de la qualité de la gestion de la PRP et de l'utilisation des infrastructures technologiques à cette fin.

Elle met en œuvre la présente politique et s'assure notamment que :

- Le RPRP et le RAD peuvent exercer leurs fonctions de manière autonome
- Les valeurs et orientations en matière de PRP sont partagées
- Les appuis financiers et logistiques nécessaires sont fournis
- Son pouvoir d'enquête est exercé et les sanctions appropriées sont appliquées

10. RPRP

Le RPRP contribue à une saine gestion de la PRP et soutient le conseil, la direction générale et le personnel.

Il assume les tâches du Comité sur l'accès à l'information et la protection des renseignements personnels et s'assure notamment de :

- Définir et approuver les orientations en matière de PRP
- Déterminer la nature des RP à collecter, leur conservation, communication et destruction
- Suggérer les adaptations nécessaires en cas de modifications législatives
- Planifier et assurer la formation des employés en matière de PRP
- Formuler des avis sur les systèmes d'information et les services électroniques
- Formuler des avis sur les sondages et la vidéosurveillance
- Veiller à ce que la Municipalité connaisse les orientations de la CAI
- Évaluer le niveau de PRP
- Recommander l'anonymisation des RP
- Faire rapport annuel au conseil

11. RAD

Le RAD reçoit les demandes d'accès aux documents et y répond conformément à la Loi sur l'accès.

12. Directeur de service

Chaque directeur de service est responsable de la PRP au sein de son service et des infrastructures technologiques.

Il doit notamment :

- Faire connaître la présente politique aux employés et s'assurer de son application.

- S'assurer que les mesures de sécurité sont appliquées.
- Sensibiliser les employés aux enjeux de la PRP.
- Désigner un ou des employés responsables de la PRP au sein de son service.

13. Responsable de la PRP au sein des différents services

Chaque directeur de service doit identifier un responsable de la PRP au sein de son service.

Ces responsables travaillent en collaboration avec le RPRP pour inventorier les catégories de RP et maintenir cet inventaire à jour.

Ils doivent également s'assurer d'obtenir les consentements requis et les conserver.

14. Employés

Chaque employé doit :

- Prendre les mesures nécessaires pour protéger les RP.
- Respecter le cadre légal et les politiques de la Municipalité.
- N'accéder qu'aux RP nécessaires à l'exercice de ses fonctions.
- Signaler tout incident de confidentialité.
- Participer aux activités de sensibilisation et de formation.
- Collaborer avec le RPRP et le RAD.

15. Formation du personnel

Le RPRP établit le contenu et la fréquence des formations offertes aux employés en matière de PRP.

Les activités de formation ou de sensibilisation peuvent inclure :

- Formation à l'embauche.
- Formation sur la présente politique.
- Formation sur les nouveaux outils informatiques.
- Formation sur les mises à jour de la politique ou des mesures de sécurité.
- Discussions de cas lors de réunions d'employés.

Chapitre IV — Mesures administratives

16. Sondages

Avant d'effectuer un sondage, le RPRP doit évaluer la nécessité et l'aspect éthique du sondage, et faire des recommandations au conseil.

17. Incidents de confidentialité

L'accès, l'utilisation ou la communication non autorisés de tout RP ou sa perte constituent un incident de confidentialité au sens de la Loi sur l'accès.

La Municipalité assure la gestion de tout incident de confidentialité conformément à la procédure de gestion des incidents de confidentialité dont font partie les règles suivantes :

a. Tout incident de confidentialité avéré ou potentiel doit être rapporté le plus rapidement possible au RPRP par toute personne qui s'en rend compte ;

b. Le RPRP doit réviser l'information rapportée afin de déterminer s'il s'agit d'un incident de confidentialité et dans l'affirmative :

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

ii. Aviser la CAI et toute personne concernée par l'incident de confidentialité ; iii. Identifier et recommander l'application de mesures d'atténuation appropriées, le cas échéant.

18. Traitement des plaintes

Toute personne physique qui estime que la Municipalité n'assure pas la protection des RP de manière conforme à la Loi sur l'accès peut porter plainte de la manière suivante :

1) Une plainte ne peut être considérée uniquement que si elle est faite par écrit par une personne physique qui s'identifie.
2) Telle demande est adressée au RPRP de la Municipalité.
3) Le RPRP avise par écrit le requérant de la date de la réception de sa plainte et indique les délais pour y donner suite.
4) Le RPRP donne suite à une plainte avec diligence et au plus tard dans les vingt jours suivant la date de sa réception.
5) Si le traitement de la plainte dans le délai de la présente Politique paraît impossible à respecter sans nuire au déroulement normal des activités de la Municipalité, le RPRP peut, avant l'expiration de ce délai, le prolonger d'une période raisonnable et en donne avis au requérant, par tout moyen de communication permettant de joindre ce dernier.
6) Dans le cadre du traitement de la plainte, le RPRP peut communiquer avec le plaignant et faire une enquête interne.
7) À l'issue de l'examen de la plainte, le RPRP transmet au plaignant une réponse finale écrite et motivée.
8) Si le plaignant n'est pas satisfait de la réponse obtenue ou du traitement de sa plainte, il peut s'adresser par écrit à la CAI.

19. Sanctions

Tout employé de la Municipalité qui contrevient à la présente Politique ou aux lois et à la réglementation en vigueur applicable en matière de PRP s'expose, en plus des pénalités prévues aux lois, à une mesure disciplinaire pouvant notamment mener à une mesure disciplinaire et pouvant aller jusqu'au congédiement. Le directeur général est chargée de décider de l'opportunité d'appliquer la sanction appropriée, le cas échéant. La Municipalité peut également transmettre à toute autorité judiciaire les informations colligées sur tout employé, qui portent à croire qu'une infraction à l'une ou l'autre loi ou règlement en vigueur en matière de PRP a été commis.

20. Résumé des principes

La collecte des renseignements par la municipalité de Saint-Paulin s'effectue en toute transparence avec le consentement libre et éclairé de l'utilisateur et uniquement dans le cas où la collecte d'informations est nécessaire.

La collecte de renseignements personnels est réalisée uniquement lorsqu'elle est essentielle dans les activités de la municipalité et dans le but d'offrir un service personnalisé dans les limites des lois et des règles applicables.

Par conséquent les municipalités de Saint-Paulin recueille et utilise dans le cadre de ces opérations des renseignements personnels pour les fins suivantes :

a) Vérifiez l'identité de l'usager;
b) Déterminer l'admissibilité à un service offert;
c) Exécuter les mandats conférés à la municipalité en vertu d'une loi;
d) Communiquer de l'information aux citoyens et partenaires qui en font la demande;
e) Élaborer des statistiques;
f) Améliorer les services offerts.

La municipalité de Saint-Paulin veille à ce que les renseignements personnels qu'elle détient soient exacts, mis à jour et conservés uniquement le temps nécessaire pour réaliser les fins pour laquelle ils ont été recueillis. Des règles de sécurité pour assurer la protection des renseignements personnels et confidentiels s'applique tout au long de leur cycle de vie.

De plus des mesures de contrôle sont mises en place et maintenues afin de protéger les installations, les employés et les actifs informationnels contre les accès non autorisés. La gestion des accès comprend notamment un accès verrouillé en tout temps aux espaces administratifs à la salle des serveurs à la salle des archives ainsi qu'une directive interne sur la gestion des clés et des accès des immeubles de la municipalité,

Tout incident de confidentialité doit obligatoirement être rapporté sans délai aux responsables de la protection des renseignements personnels qui consignera l'incident dans un registre.

Une analyse entourant l'incident et alors réalisé afin d'évaluer si des stratégies d'atténuation ou de contrôle supplémentaire doivent être appliquées.

Lorsqu'un incident de confidentialité implique un préjudice sérieux le responsable de la protection des renseignements personnels veille à informer la commission d'accès à l'information et à établir une stratégie de communication pour informer les personnes dont les renseignements personnels ont été compromis.

Réalisé par Jean Lacroix, avocat le 31 Janvier 2025