POLITIQUE ADMINISTRATIVE CONCERNANT LES RÈGLES DE GOUVERNANCE EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS DE LA MUNICIPALITÉ

CHAPITRE I — APPLICATION ET INTERPRÉTATION

1. DÉFINITIONS

Aux fins de la présente politique, 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 de la MRC du Haut-Saint-François;

Cycle de vie : Désigne l'ensemble des étapes d'existence d'un renseignement détenu par la MRC et plus précisément sa création, sa modification, son transfert, sa consultation, sa transmission, sa conservation, son archivage, son anonymisation ou sa destruction ;

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 MRC collecte, détient, communique à un tiers, détruit ou rend anonyme, un ou des renseignements personnels ;

Partie prenante : Désigne une personne physique en relation avec la MRC dans le cadre de ses activités et, sans limiter la généralité de ce qui précède, un employé ou un fournisseur ;

Politique de gouvernance PRP : Désigne la politique administrative concernant les règles de gouvernance en matière de protection des renseignements personnels de la MRC ;

PRP : Désigne la protection 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 l'accès aux documents (ou RAD) : Désigne la personne qui, conformément à la Loi sur l'accès, exerce cette fonction et répond aux demandes d'accès aux documents de la MRC ;

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

2. OBJECTIFS

La Politique de gouvernance PRP vise les objectifs suivants :

· Énoncer les orientations et les principes directeurs destinés à assurer efficacement la PRP ;

· Protéger les RP recueillis par la MRC tout au long de leur cycle de vie ;

· Assurer la conformité aux exigences légales applicables à la PRP, dont la Loi sur l'accès, et aux meilleures pratiques en cette matière ;

· Assurer la confiance du public en la MRC, faire preuve de transparence concernant le traitement des RP et les mesures de PRP appliquées par la MRC et leur donner accès lorsque requis.

CHAPITRE II — MESURES DE PROTECTION DES RENSEIGNEMENTS PERSONNELS

3. COLLECTE DES RENSEIGNEMENTS PERSONNELS

3.1. La MRC ne collecte que les RP nécessaires aux fins de ses activités.

3.2. Sous réserve des exceptions prévues à la Loi sur l'accès, la MRC ne procède pas à la collecte de RP sans avoir préalablement obtenu le consentement de la personne concernée.

3.3. Est entendu que le consentement doit être donné à des fins spécifiques, pour une durée nécessaire à la réalisation des fins auxquelles il est demandé. Le consentement de la personne concernée doit être :

a) **Manifeste** : ce qui signifie qu'il est évident et certain ;

b) **Libre** : ce qui signifie qu'il doit être exempt de contraintes ;

c) **Éclairé** : ce qui signifie qu'il est pris en toute connaissance de cause.

3.4. Au moment de la collecte de tout RP, la MRC s'assure d'obtenir de façon expresse le consentement libre et éclairé de la personne concernée. La MRC doit notamment indiquer :

- Les fins auxquelles tout RP est requis ;

- Le caractère obligatoire ou facultatif de la demande de collecte de RP ;

- Les conséquences, pour la personne concernée, d'un refus de répondre à la demande ;

- Les conséquences, pour la personne concernée, d'un retrait de son consentement à la communication ou à l'utilisation des RP suivant une demande facultative ;

- Les droits d'accès et de rectification aux RP collectés ;

- Les moyens par lesquels tout RP est recueilli ;

- Les précisions nécessaires relativement (1) au recours par la MRC à une technologie afin de recueillir tout RP, comprenant des fonctions qui permettent l'identification, la localisation ou le profilage de la personne concernée et (2) aux moyens offerts, à la personne concernée, pour en activer ou désactiver les fonctions ;

- Les précisions relatives à la durée de conservation de tout RP ;

- Les coordonnées de la personne responsable de la PRP au sein de la MRC.

4. CONSERVATION ET UTILISATION DES RENSEIGNEMENTS PERSONNELS

4.1. La MRC restreint l'utilisation de tout RP aux fins pour lesquelles il a été recueilli et pour lequel la MRC a obtenu le consentement exprès de la personne concernée, le tout sous réserve des exceptions prévues par la Loi sur l'accès.

4.2. La MRC limite l'accès à tout RP détenu aux seules personnes pour lesquelles ledit accès est requis à l'exercice de leurs fonctions au sein de la MRC.

4.3. La MRC applique des mesures de sécurité équivalente, quelle que soit la sensibilité des RP détenus afin de prévenir les atteintes à leur confidentialité et à leur intégrité sous réserve des exceptions prévues à la Loi sur l'accès.

4.4. La MRC conserve les données et documents comportant des RP :

a) pour la durée nécessaire à l'utilisation pour laquelle ils ont été obtenus

OU

b) conformément aux délais prévus à son calendrier de conservation.

4.5. Lors de l'utilisation de tout RP, la MRC s'assure de l'exactitude du RP. Pour ce faire, elle valide son exactitude auprès de la personne concernée de façon régulière et, si nécessaire, au moment de son utilisation.

4.6. La MRC accorde le même haut taux d'attente raisonnable de protection, en matière de confidentialité et d'intégrité envers tout RP qu'elle collecte, conserve et utilise que le RP soit sensible ou non.

5. FICHIER DE RENSEIGNEMENTS PERSONNELS

La MRC établit et maintient à jour un inventaire de ses fichiers de renseignements personnels.

Cet inventaire doit contenir les indications suivantes :

a) la désignation de chaque fichier, les catégories de renseignements qu'il contient, les fins pour lesquelles les renseignements sont conservés et le mode de gestion de chaque fichier ;

b) la provenance des renseignements versés à chaque fichier ;

c) les catégories de personnes concernées par les renseignements versés à chaque fichier ;

d) les catégories de personnes qui ont accès à chaque fichier dans l'exercice de leurs fonctions ;

e) les mesures de sécurité prises pour assurer la protection des renseignements personnels.

Toute personne qui en fait la demande a droit d'accès à cet inventaire, sauf à l'égard des renseignements dont la confirmation de l'existence peut être refusée en vertu des dispositions de la Loi sur l'accès.

6. COMMUNICATION À DES TIERS

6.1. La MRC, ne peut communiquer à des tiers tout RP sans un consentement exprès de la personne concernée sauf exception prévue à la Loi sur l'accès.

6.2. La MRC indique, dans les registres exigés par la Loi sur l'accès, toutes les informations relatives à la transmission de tout RP à un tiers à quelques fins que ce soit.

7. DESTRUCTION OU ANONYMISATION

7.1. Lorsque des RP ne sont plus nécessaires aux fins pour lesquelles ils ont été recueillis et lorsque le délai prévu au calendrier de conservation est expiré, la MRC doit les détruire de façon irréversible ou les rendre anonymes.

7.2. La procédure de destruction devra être approuvée par le greffier-trésorier [ou greffier] et le RPRP afin de s'assurer notamment du respect de l'article 199 du Code municipal [ou 87 et 88 de la Loi sur les cités et villes].

7.3. L'anonymisation vise une fin sérieuse et légitime et la procédure est irréversible.

7.4. Sur recommandation du RPRP, toute procédure d'anonymisation doit être approuvée par le greffier-trésorier [ou greffier].

CHAPITRE III — RÔLES ET RESPONSABILITÉS À L'ÉGARD DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

8. CONSEIL

Le conseil approuve la présente Politique et veille à sa mise en œuvre, notamment en s'assurant :

a) De prendre les décisions nécessaires relevant de sa compétence pour voir à la mise en œuvre et au respect de la présente Politique ;

b) Que la direction générale et les directeurs de service de la MRC fassent la promotion d'une culture organisationnelle fondée sur la protection des RP et des comportements nécessaires afin d'éviter tout incident de confidentialité ;

c) Que le RPRP et le RAD puissent exercer de manière autonome leurs pouvoirs et responsabilités.

9. DIRECTION GÉNÉRALE

La direction générale est responsable de la qualité de la gestion de la PRP et de l'utilisation de toute infrastructure technologique de la MRC à cette fin.

À cet égard, elle doit mettre en œuvre la présente Politique en :

a) Veillant à ce que le RPRP et le RAD puissent exercer de manière autonome leurs pouvoirs et responsabilités ;

b) S'assurant que les valeurs et les orientations en matière de PRP soient partagées et véhiculées par tout gestionnaire et employé de la MRC ;

c) Apportant les appuis financiers et logistiques nécessaires à la mise en œuvre et au respect de la présente politique ;

d) Exerçant son pouvoir d'enquête et appliquant les sanctions appropriées aux circonstances pour le non-respect de la présente Politique ;

10. RESPONSABLE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Le PRPR, en collaboration avec le RAD, contribue à assurer une saine gestion de la PRP au sein de la MRC. Il soutient le conseil, la direction générale et l'ensemble du personnel de la MRC dans la mise en œuvre de la présente Politique. 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 (Décret 744-2023, 3 mai 2023), le RPRP assume les tâches qui sont dévolues au Comité sur l'accès à l'information et la protection des renseignements personnels prévu à l'article 8.1 de la Loi sur l'accès ainsi que les obligations qui en découlent.

Notamment, le RPRP s'assure de :

a) Définir et approuver les orientations en matière de PRP au sein de la MRC ;

b) Déterminer la nature des RP devant être collectés par les différents services de la MRC, leur conservation, leur communication à des tiers et leur destruction ;

c) Suggérer les adaptations nécessaires en cas de modifications à la Loi sur l'accès, à ses règlements afférents ou l'interprétation des tribunaux, le cas échéant ;

d) Planifier et assurer la réalisation des activités de formation des employés de la MRC en matière de PRP ;

e) Formuler des avis sur les initiatives d'acquisition, de déploiement et de refonte de systèmes d'information ou de toute nouvelle prestation électronique de services de la MRC nécessitant la collecte, l'utilisation, la conservation, la communication à des tiers ou la destruction des RP, et ce, tant au moment de la mise en place de ces initiatives que lors de toute modification à celles-ci ;

f) Formuler des avis sur les mesures particulières à respecter quant aux sondages qui collectent ou utilisent des RP, ou encore en matière de vidéosurveillance ;

g) Veiller à ce que la MRC connaisse les orientations, les directives et les décisions formulées par la CAI en matière de PRP ;

h) Évaluer le niveau de PRP au sein de la MRC ;

i) Recommander au greffier-trésorier [ou greffier] de procéder à l'anonymisation de RP en lieu et place de la destruction de RP qui n'est plus utile à la MRC ;

j) Faire rapport au conseil et à la direction générale, sur une base annuelle, quant à l'application de la présente politique.

11. RESPONSABLE DE L'ACCÈS AUX DOCUMENTS

Dans le cadre de cette fonction, le responsable de la conformité doit :

a) Recevoir toutes les demandes qui sont de la nature d'une demande d'accès aux documents au sens de la Loi sur l'accès, y compris les demandes d'informations ;

b) Répondre aux requérants de l'accès à des documents en fonction des prescriptions de la Loi sur l'accès.

12. DIRECTEUR DE SERVICE

Chaque directeur de service est responsable de veiller à la PRP au sein du service qu'il dirige ainsi que des infrastructures technologiques nécessaires à cette fin auxquelles les employés du service et lui ont accès dans le cadre de leurs fonctions à la MRC.

À ce titre, chaque directeur de service doit :

a) Faire connaître la présente politique en matière de PRP aux employés de son service et s'assurer de son application et son respect par ceux-ci ;

b) S'assurer que les mesures de sécurité déterminées et mises en place soient appliquées systématiquement à l'occasion de son emploi et de celui des employés qu'il dirige dans le service dont il est responsable ;

c) Participer à la sensibilisation de chaque employé de son équipe aux enjeux de la PRP ;

d) Désigner, au sein de son service, le ou les employés dont la tâche inclue spécifiquement les fonctions de veiller à la collecte, la détention, la conservation ou la destruction des RP et leur protection ;

e) Dans le cas où aucun employé n'est désigné, le directeur de service assume les tâches et responsabilités prévues à l'article 13.

13. RESPONSABLE DE LA PRP AU SEIN DES DIFFÉRENTS SERVICES DE LA MRC

Chaque directeur de service de la MRC doit identifier le responsable de la PRP au sein de son service au RPRP. Les employés de chaque service de la MRC ainsi désignés sont responsables au sein de leur service de certaines étapes de la vie des RP, c'est-à-dire la collecte et la détention.

Chaque responsable au sein d'un service susmentionné travaille en étroite collaboration avec le RPRP afin d'inventorier les diverses catégories de RP recueillies, détenues, communiquées à des tiers, le cas échéant, détruites ou rendues anonymes et de maintenir à jour cet inventaire. Le responsable doit également voir à ce que les employés du service obtiennent tout consentement requis de tout individu aux fins de collecter, détenir ou transférer à des tiers le cas échéant. Le responsable doit voir à la conservation et au classement des consentements recueillis de manière que ceux-ci puissent être facilement retracés.

14. EMPLOYÉS

Chaque employé doit :

a) Prendre toutes les mesures nécessaires afin de protéger les RP ;

b) Mettre tout en œuvre pour respecter le cadre légal applicable et les mesures prévues aux différentes politiques et directives de la MRC en lien avec la protection des RP ;

c) N'accéder qu'aux RP nécessaires dans l'exercice de ses fonctions ;

d) Signaler au RPRP tout incident de confidentialité ou traitement irrégulier des RP ;

e) Participer activement à toute activité de sensibilisation ou formation données en matière de PRP ;

f) Collaborer avec le RPRP et le RAD.

15. FORMATION DU PERSONNEL DE LA MRC EN VUE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Le RPRP établit le contenu et le choix des formations offertes à tous les employés de la MRC et détermine la fréquence à laquelle les employés doivent suivre toute formation établie.

Les activités de formation ou de sensibilisation inclus notamment : [à compléter par la MRC]

Exemples :

- Formation à l'embauche sur l'importance de la PRP et les actions à prendre dans son travail ;

- Formation à tous les employés sur la mise en œuvre de la présente politique ;

- Formation aux employés utilisant un nouvel outil informatique impliquant des RP ;

- Formation sur les mises à jour de la présente politique ou des mesures de sécurité des RP, le cas échéant ;

CHAPITRE IV — MESURES ADMINISTRATIVES

16. SONDAGES

Avant d'effectuer, ou de permettre à une tierce partie d'effectuer un sondage auprès des personnes concernées pour lesquelles la MRC détient, recueille ou utilise des RP, le RPRP devra préalablement faire une évaluation des points suivants :

- la nécessité de recourir au sondage ;

- l'aspect éthique du sondage compte tenu, notamment, de la sensibilité des renseignements personnels recueillis et de la finalité de leur utilisation.

Suivant cette évaluation, le RPRP devra faire des recommandations au conseil et à la direction générale.

17. ACQUISITION, DÉVELOPPEMENT OU REFONTE D'UN SYSTÈME D'INFORMATION OU DE PRESTATION ÉLECTRONIQUE

17.1. Avant de procéder à l'acquisition, au développement ou à la refonte des systèmes de gestion des RP, la MRC doit procéder à une évaluation des facteurs relatifs à la vie privée.

Aux fins de cette évaluation, la MRC doit consulter, dès le début du projet, son RPRP.

17.2. Dans le cadre de la mise en œuvre du projet prévu à l'article 17.1, le RPRP peut, à toute étape, suggérer des mesures de protection des RP, dont notamment :

a) la nomination d'une personne chargée de la mise en œuvre des mesures de PRP ;

b) des mesures de PRP dans tout document relatif au projet, tel qu'un cahier des charges ou un contrat ;

c) une description des responsabilités des participants au projet en matière de PRP ;

d) la tenue d'activités de formation sur la PRP pour les participants au projet.

17.3. La MRC doit également s'assurer que dans le cadre du projet prévu à l'article 17.1, le système de gestion des renseignements personnels permet qu'un RP informatisé recueilli auprès de la personne concernée soit communiqué à cette dernière dans un format technologique structuré et couramment utilisé.

17.4. La réalisation d'une évaluation des facteurs relatifs à la vie privée doit être proportionnée à la sensibilité des renseignements concernés, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support.

18. 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 MRC assure la gestion de tout incident de confidentialité conformément à la procédure de gestion des incidents de confidentialité dont font partie les règles suivantes :

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

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

· Inscrire l'information pertinente au registre des incidents de confidentialité de la MRC ;

· Aviser la CAI et toute personne concernée par l'incident de confidentialité ;

· Identifier et recommander l'application de mesures d'atténuation appropriées, le cas échéant.

19. TRAITEMENT DES PLAINTES

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

19.1. Une plainte ne peut être considérée uniquement que si elle est faite par écrit par une personne physique qui s'identifie.

19.2. Telle demande est adressée au RPRP de la MRC.

19.3. Le RPRP avise par écrit le requérant de la date de la réception de sa plainte et indique les délais pour y donner suite.

19.4. Le RPRP donne suite à une plainte avec diligence et au plus tard dans les vingt jours suivant la date de sa réception.

19.5. Si le traitement de la plainte dans le délai prévu à l'article 19.4 de la présente Politique paraît impossible à respecter sans nuire au déroulement normal des activités de la MRC, 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.

19.6. Dans le cadre du traitement de la plainte, le RPRP peut communiquer avec le plaignant et faire une enquête interne.

19.7. À l'issue de l'examen de la plainte, le RPRP transmet au plaignant une réponse finale écrite et motivée.

19.8. 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.

20. SANCTIONS

Tout employé de la MRC 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. La direction générale, de concert avec le Service des Ressources humaines, est chargée de décider de l'opportunité d'appliquer la sanction appropriée, le cas échéant. La MRC 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.

21. DISPOSITION FINALE

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

ADOPTÉE