POLITIQUE D'ANONYMISATION ET DE DÉPERSONNALISATION

Table des matières

1. Portée, objectif et utilisateurs

Portée et objectif. Le but de ce document est de fournir des conseils à la Municipalité de Ferme-Neuve (ci-après la « **Municipalité** ») pour établir et maintenir la dépersonnalisation et d'anonymisation de renseignements personnels.

Utilisateurs. Ces lignes directrices s'appliquent à tous les employés de l'Établissement, et particulièrement au responsable de l'accès à l'information et de la protection des renseignements personnels (« **Responsable AIPRP** »), au responsable de la sécurité informatique, de même qu'aux responsables des directions traitantes de Renseignements personnels.

2. Documents de référence

- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, c. A-2.1, telle que modifiée par la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, LQ 2021 c 25 (la « **Loi sur l'accès** »);
- *Charte des droits et libertés de la personne,* RLRQ c C-12 (la « **CDLP** »)
- *Code civil du Québec*, RLRQ c CCQ-1991 (le « **CCQ** »).
- *Loi sur les archives* (chapitre A-21.1).

3. Définitions

Les mots et expressions qui suivent, lorsqu'ils apparaissent avec une première lettre en majuscule aux présentes lignes directrices, ont le sens qui leur est attribué ci-dessous, à moins d'une dérogation implicite ou explicite dans le texte.

« Dépersonnalisation » signifie toute méthode, incluant la suppression des noms et identifiants évidents, permettant de faire en sorte qu'un renseignement personnel ne permette plus d'identifier directement la personne concernée.

« Anonymisation » désigne le traitement de renseignements personnels dans le but d'empêcher de *manière irréversible* l'identification de la personne à laquelle ils se rapportent. Les renseignements personnels peuvent être considérés comme anonymisés lorsqu'ils ne permettent pas d'identifier les personnes auxquelles ils se rapportent, et lorsqu'il n'est pas possible pour une personne d'être identifiée à partir des renseignements personnels par tout traitement ultérieur de ces mêmes données, ou en traitant ces mêmes données avec d'autres données disponibles ou susceptibles d'être disponibles. Pour la plupart des entreprises, l'anonymisation complète n'est pas possible.

4. Dépersonnalisation et Anonymisation de renseignements personnels

Liste non exhaustive de techniques. Les présentes lignes directrices répertorient une liste non exhaustive de techniques d'Anonymisation et de Dépersonnalisation pouvant être utilisées par la Municipalité. Elles sont fournies à titre indicatif uniquement et sujettes à être modifiées quant à l'anonymisation, advenant que le gouvernement adopte un règlement aux fins de déterminer les critères et les modalités applicables à l'anonymisation. Les exemples rattachés à ces techniques ont été hautement simplifiés afin de faciliter leur compréhension. L'application des exemples qui s'y rattachent ne sera pas suffisant pour obtenir une anonymisation ou une dépersonnalisation. Dépersonnaliser ou anonymiser un renseignement personnel requiert les services et les conseils d'un expert.

Procédure. Lorsqu'on lui soumet une Activité de traitement nécessitant l'Anonymisation ou la Dépersonnalisation d'un Renseignement personnel, le Responsable AIPRP détermine les techniques appropriées d'Anonymisation et de Dépersonnalisation selon les Activités de traitement particulières de Renseignements personnels visés.

4.1. Anonymisation

Objectif de l'Anonymisation. En vertu de la Loi sur l'accès, lorsque les fins pour lesquelles un Renseignement personnel a été recueilli ou utilisé sont accomplies, la Municipalité doit le détruire ou l'anonymiser pour l'utiliser à des fins d'intérêt public, sous réserve de la *Loi sur les archives* (chapitre A-21.1). Le but de l'Anonymisation des renseignements personnels est de rendre impossible l'identification d'un individu dans l'ensemble de données anonymisées, même à l'aide des données d'origine, de sorte que les données anonymisées ne sont pas considérées comme des renseignements personnels.

Selon les meilleures pratiques. Il est important de noter qu'il n'existe pas de norme prescrite par la LPRPSP pour anonymiser un renseignement personnel. Celle-ci se limite à indiquer que l'Anonymisation doit se faire:

1. selon les meilleures pratiques généralement reconnues ; et

2. selon les critères et modalités déterminés par règlement.

Éléments à considérer. La Municipalité doit utiliser les mesures et les techniques généralement reconnues comme étant les meilleures pratiques en vue de faire l'Anonymisation de Renseignements personnels. En anonymisant un Renseignement personnel, la Municipalité doit tenir compte de la nature de ces renseignements, de leur quantité et des possibilités de faire des liens entre différents renseignements. Plusieurs techniques différentes peuvent être utilisées en combinaison.

Vulgarisation des méthodes. Les méthodes suivantes seront utilisées par la Municipalité en tenant compte du degré de risque et de l'utilisation prévue des renseignements personnels.

1. **Remplacement de l'annuaire** – Modification du nom des personnes intégrées dans les listes de renseignements personnels, tout en maintenant la cohérence entre les valeurs, telles que « code postal + Municipalité », « âge + sexe ».

2. **Brouillage** – Implique un mélange ou un obscurcissement des lettres. Le processus peut parfois être réversible. Par exemple : Robert pourrait devenir Betror.

3. **Masquage** – Permet de masquer une partie des renseignements personnels avec des caractères aléatoires ou d'autres données.

4. **Flou** – Approximation des valeurs des renseignements personnels pour rendre leur signification obsolète et/ou rendre impossible l'identification des individus.

5. **Confidentialité différentielle** – Cette méthode peut être utilisée chaque fois que la Municipalité donne à un tiers l'accès à un ensemble de données anonymisées. Une copie des renseignements personnels d'origine reste avec la Municipalité, et le destinataire tiers ne reçoit qu'un ensemble de données anonymes.

6. **Agrégation** – Une personne concernée est regroupée avec plusieurs autres personnes concernées qui partagent tout ou partie des renseignements personnels.

Mises en garde importante. En date du 2024-02-14, la position officielle de la Commission d'accès à l'information est que l'Anonymisation n'est pas encore possible au Québec en raison de l'absence de règlementation à cet effet. De plus, même en présence d'un règlement, il serait en raison des avancées technologiques actuels et futures, « quasi impossible » de certifier que des renseignements anonymisés ne pourraient pas éventuellement être réidentifiés. Ces mises en garde de la Commission implique que même en présence de règlement, il sera impératif pour une entreprise ou une organisation désireuse d'anonymiser des renseignements personnels d'avoir recours à une expertise et qu'il serait sage de faire preuve de grande prudence avant de présenter que l'on « anonymise » des renseignements personnels.

4.2. Dépersonnalisation

Objectif de la Dépersonnalisation. En vertu de la Loi sur l'accès, la Municipalité peut utiliser un Renseignement personnel sans le consentement de la Personne concernée lorsque son utilisation est nécessaire à des fins d'étude, de recherche ou de production de statistiques et qu'il est dépersonnalisé.

Limiter les risques d'identification. Pour ce faire, la Municipalité doit prendre les mesures raisonnables afin de limiter les risques que quiconque procède à l'identification d'une personne physique à partir de Renseignements personnels dépersonnalisés.

Exemples de méthodes. Le Responsable AIPRP établira les méthodes de Dépersonnalisation appropriées telles que :

1. **Chiffrement (à l'aide d'une clé secrète)** – Les renseignements personnels sont chiffrés à l'aide d'une clé secrète. Le détenteur de la clé secrète peut réidentifier les personnes concernées en déchiffrant l'ensemble de renseignements personnels.

2. **Fonctions de hachage** – Utilisées pour mapper des renseignements personnels de n'importe quelle taille à des codes de taille fixe (notez qu'il existe plusieurs techniques de hachage (par exemple, salage, hachages à clé, etc.). Le salage est une méthode permettant de renforcer la

sécurité des informations qui sont destinées à être hachées en y ajoutant une donnée supplémentaire afin d'empêcher que deux informations identiques conduisent à la même empreinte.

3. **Tokenisation** – Processus de substitution d'un élément de données sensibles par un équivalent non sensible, appelé jeton (Token). Le jeton est une référence (c'est-à-dire un identifiant) qui correspond aux données sensibles via un système de Tokenisation. Le système de Tokenisation fournit aux applications de traitement de données l'autorité et les interfaces nécessaires pour demander des jetons ou revenir à des données sensibles.

5. Mise à jour

La présente Politique est révisée, au besoin, suivant l'évolution du cadre normatif applicable en matière de protection des Renseignements personnels.

6. Entrée en vigueur

Ce document entre en vigueur à la date de son adoption par le Conseil municipal.