



Municipalité de Saint-Étienne-de-Bolton

POLITIQUE ET PROCÉDURE DE PORTABILITÉ DES DONNÉES

Octobre 2024

POLITIQUE ET PROCÉDURE DE PORTABILITÉ DES DONNÉES

1. OBJECTIF

Cette politique a pour but de fournir des directives claires aux membres du personnel concernant la gestion des demandes de portabilité des données et des demandes d'accès aux renseignements personnels informatisés. Elle vise à s'assurer que ces demandes sont traitées de manière conforme, sécurisée, et en accord avec les règlements en vigueur, tout en protégeant les renseignements personnels des individus.

2. CHAMP D'APPLICATION

Cette politique s'applique à tous les membres du personnel de la Municipalité impliqués dans la gestion, la collecte, ou la transmission de renseignements personnels informatisés. Elle encadre le processus de traitement des demandes de portabilité des données et de gestion des plaintes.

3. DÉFINITIONS

- **Portabilité des données** : Le droit pour une personne de recevoir ses renseignements personnels informatisés dans un format structuré et couramment utilisé, ou de les transférer directement à une autre organisation autorisée.
- **Format technologique structuré et couramment utilisé** : Un format que des logiciels courants peuvent facilement reconnaître et extraire.
- **Renseignements personnels informatisés** : Les données personnelles collectées auprès de la personne concernée, directement ou indirectement.
- **Difficultés pratiques sérieuses** : Situations où la transmission des données dans un format structuré pourrait entraîner des coûts ou des complexités excessives.

4. RÔLES ET RESPONSABILITÉS

- **Responsable de la protection des renseignements personnels (RPRP)** :
 - Supervise et coordonne l'ensemble du processus de portabilité des données.
 - Vérifie l'identité des demandeurs avant la transmission des renseignements.
 - S'assure que les mesures de sécurité sont appliquées lors de la transmission des informations.
 - Gère les plaintes liées aux demandes de portabilité ou d'accès aux renseignements.
- **Membres du personnel** :
 - Réorientent toute demande de portabilité ou d'accès aux renseignements vers le RPRP.
 - Ne transmettent aucun renseignement personnel avant validation par le RPRP.
 - Signalent tout incident ou difficulté au RPRP sans délai.
- **Service informatique ou l'équivalent** :
 - Prépare les données dans un format structuré et couramment utilisé.

- Assure la sécurité des données pendant le transfert.
- **Service juridique ou l'équivalent :**
 - Fournit un soutien en cas de difficultés pratiques sérieuses ou de plaintes.

5. PROCÉDURE DE TRAITEMENT DES PLAINTES

5.1. Réception d'une demande

1. **Demande initiale** : Tout membre du personnel qui reçoit une demande de portabilité des données doit immédiatement la transmettre au RPRP.
2. **Vérification de l'identité** : Le RPRP est responsable de la vérification de l'identité du demandeur. Il doit s'assurer que la personne qui fait la demande est bien celle dont les renseignements sont demandés avant d'engager toute démarche de transfert.
 - **Méthodes de vérification** : Demander des documents d'identité officiels ou utiliser des systèmes de validation sécurisés.
3. **Confirmation de la demande** : Une fois l'identité vérifiée, le RPRP informe le demandeur que sa demande est en cours de traitement.

5.2. Préparation des données

1. **Format des données** : Le service informatique doit préparer les données dans un format structuré et couramment utilisé (ex : CSV, XML).
2. **Mesures de sécurité** : Les données doivent être chiffrées et sécurisées lors de la transmission pour garantir leur confidentialité et intégrité.

6. GESTION DES PLAINTES

Si le demandeur est insatisfait de la réponse à sa demande ou du traitement de celle-ci, il peut :

- **Contacter le RPRP** pour exprimer son mécontentement. Le RPRP doit répondre dans les plus brefs délais et, si possible, résoudre la situation.
- **Déposer une plainte formelle** auprès de la Commission d'accès à l'information.

7. RESPECT DES DÉLAIS LÉGAUX ET SENTIMENT D'URGENCE

Il est impératif que toutes les demandes de portabilité des données soient traitées **dans un délai de 30 jours ou moins**, conformément aux exigences légales. Ce délai est essentiel pour garantir que l'organisation respecte ses obligations légales et protège les droits des individus.

- **Responsabilité du RPRP** : Le RPRP est responsable de s'assurer que toutes les demandes sont traitées en temps voulu. Il doit surveiller de près le processus, depuis la réception de la demande jusqu'à la transmission des données, et s'assurer qu'aucun retard injustifié ne survient.
- **Sentiment d'urgence** : Tous les membres du personnel doivent être sensibilisés à l'importance du respect des délais prescrits par la loi. Toute demande reçue doit être transmise **immédiatement** au RPRP afin de garantir que le processus démarre sans délai. En cas de

risque de retard, le RPRP doit en informer immédiatement le demandeur et proposer des alternatives, tout en restant dans le cadre légal.

- **Suivi des délais légaux** : Il est important de noter que les délais légaux peuvent évoluer avec le temps. Le RPRP et le service juridique sont chargés de se tenir informés des modifications législatives afin de toujours respecter les délais en vigueur.

8. TRANSMISSION DES DONNÉES

1. **Transmission sécurisée** : Une fois les données prêtes, elles sont transmises de manière sécurisée au demandeur ou à une tierce partie désignée.
2. **Confirmation de réception** : Le RPRP doit s'assurer que les données ont bien été reçues par le demandeur ou la tierce partie.

9. GESTION DES DIFFICULTÉS PRATIQUES SÉRIEUSES

Si le traitement de la demande entraîne des coûts ou des complexités techniques excessives, le RPRP en collaboration avec le service juridique et informatique évaluera la situation. Si nécessaire, une solution alternative, comme la réduction du volume des données transmises, sera proposée.

10. PROTECTION DES DONNÉES

1. **Vérification de l'identité** : Avant toute transmission de renseignements personnels, il est impératif de vérifier l'identité du demandeur pour éviter tout transfert à des tiers non autorisés.
2. **Sécurisation des données** : Les membres du personnel doivent s'assurer que les informations sont transmises via des canaux sécurisés, incluant l'utilisation du chiffrement et d'autres mesures de protection contre l'accès non autorisé.
3. **Conservation des données** : Les informations relatives aux demandes de portabilité doivent être conservées conformément aux politiques de protection des renseignements personnels de l'organisation.

11. FORMATION ET SENSIBILISATION

Tous les membres du personnel doivent être formés pour reconnaître une demande de portabilité et savoir comment la traiter. Des séances de sensibilisation périodiques seront organisées pour rappeler les procédures à suivre et les bonnes pratiques en matière de protection des données.

12. RÉVISION ET MISE À JOUR

Cette politique sera revue annuellement pour assurer sa conformité avec les nouvelles réglementations et l'évolution des pratiques en matière de protection des données.