



Municipalité de Saint-Étienne-de-Bolton

POLITIQUE ET PROCÉDURE DE TRANSFERT DE DONNÉES PERSONNELLES

Octobre 2024

POLITIQUE ET PROCÉDURE DE TRANSFERT DES DONNÉES PERSONNELLES

1. OBJECTIF

Cette politique a pour objectif de définir des lignes directrices claires pour le transfert sécurisé des données personnelles en réponse à une demande de portabilité, tout en garantissant la conformité avec les exigences légales, notamment la Loi 25. Elle couvre les formats de données, les méthodes sécurisées de transfert, ainsi que les règles de rétention et de destruction des informations personnelles après le transfert.

2. RESPONSABILITÉ

Le Responsable de la protection des renseignements personnels (RPRP) est chargé de superviser l'ensemble du processus, mais n'a pas accès aux données personnelles sensibles. Le service informatique et d'autres services pertinents collaborent pour effectuer les transferts de données sécurisés dans le format demandé.

3. FORMATS DE DONNÉES ACCEPTÉS POUR LE TRANSFERT

Les formats couramment utilisés pour transférer les données personnelles comprennent :

- CSV (Comma-Separated Values)
- XLS/XLSX (Microsoft Excel)
- XML (eXtensible Markup Language)

Le demandeur peut choisir parmi ces formats, en fonction de la nature des données demandées.

4. PROCÉDURE DE TRAITEMENT DES DEMANDES DE TRANSFERT DE DONNÉES

Étape 1 : Réception de la demande

Le RPRP reçoit la demande de portabilité et valide les informations de base. Il collabore ensuite avec le service informatique pour extraire les données sans accéder directement aux renseignements personnels.

Étape 2 : Sélection du format de transfert

Le RPRP, avec le service informatique, sélectionne le format le plus approprié pour le transfert des données et informe le demandeur.

Étape 3 : Préparation des données

Le service informatique ou l'équivalent extrait les données personnelles, les formate conformément aux spécifications et applique des techniques de masquage ou d'anonymisation si nécessaire.

Étape 4 : Sécurité des données en transit

Les données doivent être protégées à chaque étape du transfert. Les méthodes sécurisées suivantes sont obligatoires :

- Transfert sécurisé : Utilisation de protocoles sécurisés tels que :
 - SFTP (Secure File Transfer Protocol) pour les transferts de fichiers.

- Services de courrier électronique crypté pour envoyer des informations sensibles.
- Portails sécurisés pour permettre le téléchargement sécurisé par le demandeur.
- Authentification multi-facteurs (MFA) : Un code d'authentification envoyé par SMS ou courriel peut être requis pour accéder aux données.

Étape 5 : Transmission des données

Les données sont transmises via un canal sécurisé choisi en fonction de la méthode la plus appropriée, telle qu'un lien de téléchargement sécurisé.

Étape 6 : Confirmation de la réception

Le RPRP ou le service informatique contacte le demandeur pour s'assurer que les données ont bien été reçues dans le format demandé. Le demandeur est invité à signaler tout problème d'accès ou d'exactitude.

5. SÉCURITÉ DES DONNÉES EN TRANSIT

Afin de garantir la sécurité des données personnelles en transit, les pratiques suivantes doivent être respectées :

- Protocole sécurisé (SFTP) : Le transfert des fichiers doit être effectué via des protocoles comme SFTP qui garantissent une communication sécurisée entre les serveurs.
- Portails sécurisés : Les utilisateurs doivent télécharger les fichiers via des portails sécurisés, accessibles après vérification de l'identité (MFA).

6. RÉTENTION ET DESTRUCTION DES RENSEIGNEMENTS PERSONNELS APRÈS LE TRANSFERT

Les renseignements personnels extraits et transférés dans le cadre d'une demande de portabilité seront conservés conformément à nos politiques de rétention et de destruction des données personnelles, ainsi qu'aux lois et règlements en vigueur.

Confirmation avec le demandeur

Lors de la communication avec le demandeur, il est recommandé de préciser que les renseignements seront gérés selon les politiques internes de conservation et les exigences légales applicables. La destruction des informations sera effectuée en conformité avec les délais prévus, sauf si des obligations légales imposent leur conservation pour une période prolongée.

Obligations légales de conservation

Dans certains cas, des obligations légales peuvent nécessiter la conservation des renseignements personnels pour une durée définie, notamment en cas d'enquêtes, d'obligations fiscales ou de litiges.

Ces données seront conservées en toute sécurité pour la période requise avant leur destruction.

7. ÉCHEC DE LA TRANSMISSION DES DONNÉES

En cas d'échec de la transmission des données personnelles (par exemple, à cause d'un problème technique, d'une interruption de service ou d'un défaut de connexion), les actions suivantes doivent être entreprises :

- **Notification immédiate** : Le demandeur doit être informé immédiatement de l'échec de la transmission et des mesures qui seront prises pour résoudre le problème.
- **Nouvelle tentative de transmission** : Le RPRP, en collaboration avec le service informatique, doit identifier la cause de l'échec et tenter une nouvelle transmission des données par le même canal sécurisé ou, si nécessaire, par un autre moyen sécurisé (SFTP, courriel crypté, clé USB cryptée, etc.).
- **Journalisation de l'incident** : Un rapport détaillant l'échec de transmission, la cause identifiée et les mesures correctives doit être enregistré afin de prévenir de futurs incidents.
- **Confirmation de réception** : Une fois le problème résolu et la transmission effectuée, le RPRP doit confirmer avec le demandeur que les données ont bien été reçues et sont accessibles sans erreur.

8. CONSERVATION DES DONNÉES ET PROTECTION DES RENSEIGNEMENTS PERSONNELS

Toutes les données traitées pendant le processus de portabilité doivent être protégées selon les normes de sécurité. Les données sont conservées temporairement pour la durée du processus et sont supprimées de manière sécurisée après confirmation de la réception. Les données soumises à des obligations légales de conservation seront conservées en toute sécurité pendant la période requise avant leur destruction.

9. FORMATION ET SENSIBILISATION DU PERSONNEL

Tous les membres du personnel participant au processus de transfert doivent être formés sur les mesures de sécurité à respecter et sur les politiques de rétention et de destruction des données.

Cela inclut la manipulation des formats de données, le chiffrement, et les protocoles de transfert sécurisés.

10. RÉVISION DE LA POLITIQUE

Cette politique sera révisée annuellement pour assurer sa conformité aux lois et aux meilleures pratiques en matière de protection des données.