Politique sur l'accès et la protection des renseignements personnels
SQUAT Basse-Ville

Basé sur la Politique sur l'accès aux documents et la protection des renseignements personnels produite par le REGROUPEMENT DES AUBERGES DU CŒUR DU QUÉBEC

Adopté au conseil d'administration tenu le 26 novembre 2024 à Québec

PRÉAMBULE

La Politique sur l'accès aux documents et la protection des renseignements personnels est adoptée en application de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (Loi 25),* sanctionné le 22 septembre 2021, modernisant ainsi l'encadrement applicable à la protection des renseignements personnels.

Le SQUAT Basse-Ville est un organisme communautaire autonome assujetti à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (Loi sur l'accès) et doit s'assurer du respect du nouvel encadrement applicable. La présente politique va de pair avec la *Politique de confidentialité*.

1- OBJECTIFS

La Politique a pour objet de préciser la gouvernance à l'égard des renseignement personnels collectés et conservés par le SQUAT Basse-Ville dans le cadre de ses opérations et de renforcer la protection de la vie privée des personnes visées par ceux-ci, de favoriser la transparence et de moderniser l'encadrement applicable à la protection des renseignements.

La politique vise notamment les objectifs suivants :

1.1 Désigner le responsable de la protection des renseignements personnels et définir son rôle et ses responsabilités;
1.2 Définir la composition et le mandat du Comité sur l'accès à l'information et la protection des renseignements personnels;
1.3 Définir un cadre de gestion des incidents de confidentialité;
1.4 Définir un cadre de gestion portant sur l'utilisation ou la communication de renseignements personnels à des fins d'étude, de recherche ou de production de statistiques.

2- CHAMP D'APPLICATION

La Politique s'applique à tous les employés, administrateurs et bénévoles du SQUAT Basse-Ville, dans le cadre de l'exercice de leurs fonctions. La Politique continue de s'appliquer après la fin de l'emploi ou de l'implication comme administrateur ou bénévole.

3- RESPONSABLE DE L'APPLICATION

La direction générale est responsable de l'accès et de la protection des renseignements personnels est responsable de l'application de la Politique.

4- RÔLES ET RESPONSABILITÉS

4.1
La direction générale du SQUAT Basse-Ville veille à assurer le respect et la mise en œuvre de la Loi sur l'accès.

4.2
La direction générale peut, selon le besoin, déléguer sa fonction de responsable de l'accès aux documents ainsi que cette de responsable de la protection des renseignements personnels à un.e coordonnateur.trice à l'intervention.

4.3
La direction générale exerce les fonctions de manière autonome et indépendante.

4.4
La direction générale veille à la protection des renseignements personnels détenus par le SQUAT Basse-Ville.

4.5
Un comité sur l'accès à l'information et la protection des renseignements personnels (le Comité sur l'accès) est mis en place afin de renforcer la protection des renseignements personnels et favoriser l'harmonisation des pratiques qui guident les actions et influencent les stratégies.

4.6
Les employés et administrateurs du SQUAT Basse-Ville sont tenus de collaborer dans la rechercher de documents et d'informations faisant l'objet de toute demande d'accès.

4.7
Les employés et administrateurs du SQUAT Basse-Ville sont tenus de veiller à la protection des renseignements personnels tel que stipulé dans la *Politique de confidentialité* de l'organisme.

5- COMITÉ SUR L'ACCÈS À L'INFORMATION ET LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

5.1
Le comité sur l'accès est composé des personnes suivantes :

- Le responsable de l'accès et de la protection des renseignements personnels (la direction générale);
- Les coordonnateurs.trices des différents volets du SQUAT Basse-Ville;
- La présidence de la corporation;
- Tout autres administrateurs voulant s'impliquer sur le comité.

5.2

Les responsabilités du Comité sur l'accès comprennent notamment ce qui suit :

5.2.1 Soutenir la direction générale dans l'exercice de ses responsabilités et dans l'exécution de ses obligations;

5.2.2. Définir et approuver, aux besoins, les orientations en matière de protection des renseignements personnels;

5.2.3. Analyser et rendre un avis lors d'incidents de confidentialité;

5.2.4. Promouvoir les orientations, les directives et les décisions formulées par la Commission d'accès à l'information;

5.2.5. Évaluer lorsque requis le niveau de protection des renseignements personnels;

5.2.6. Évaluer les demandes d'accès à l'information.

6- INCIDENTS DE CONFIDENTIALITÉ

6.1

Un incident de confidentialité correspond à un accès non autorisé par la loi à un renseignement personnel, à son utilisation ou à sa communication, de même que sa perte ou toute autre forme d'atteinte à sa protection.

6.2

La direction générale du SQUAT Basse-Ville, si elle a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'elle détient, doit prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent.

6.3

Le Comité d'accès procède à l'évaluation du préjudice selon la procédure prévue à l'ANNEXE 1.

6.4

Le SQUAT Basse-Ville doit tenir un registre des incidents de confidentialité et, sur demande de la Commission d'accès à l'information, lui en transmettre une copie.

6.5

Les renseignements contenus au registre des incidents de confidentialité doivent être tenus à jour et conservés pendant une période minimale de 5 ans après la date ou la période au cours de laquelle l'organisme a pris connaissance de l'incident.

7- UTILISATION OU COMMUNICATION DE RENSEIGNEMENTS PERSONNELS

7.1
Le SQUAT Basse-Ville dans le cadre des services rendu consigne dans un dossier tous renseignements permettant d'accompagner et faire état du suivi du jeune et de sa famille.

7.2
Un jeune de 14 ans et plus a le droit d'accès à son dossier et d'avoir communication des renseignements personnels le concernant.

7.3
Un jeune de 14 ans et plus doit donner son autorisation écrite pour que ses titulaires de l'autorité parentale puissent avoir accès à son dossier (peu importe l'âge qu'avait ce jeune lorsque son dossier fut constitué). Les parents déchus de leur autorité parentale n'ont toutefois pas accès au dossier de leur enfant.

7.4
Un jeune de moins de 14 ans n'a pas le droit d'être informé de l'existence ni de recevoir de communication d'un renseignement de nature médicale ou sociale contenu dans son dossier, sauf par l'intermédiaire de son avocat dans le cadre d'une procédure judiciaire.

7.5
Toute information divulguée à la direction générale, à la coordination de l'intervention, aux employés, aux stagiaires et aux bénévoles de l'organisme, peut, si elle est jugée nécessaire, être inscrite dans son dossier personnel. Pour les fins de leur travail, ceux-ci ont accès au dossier de chaque jeune et peuvent discuter entre eux des informations qui y sont consignées tel que stipulé dans la *Politique de confidentialité* de l'organisme.

7.6
L'organisme ne peut révéler des renseignements personnels sans en avoir reçu l'autorisation écrite de la personne concernée. Un jeune de 14 ans et plus peut y consentir lui-même. Pour un jeune de moins de 14 ans, l'autorisation doit être donnée par un titulaire de l'autorité parentale.

7.7
Le dossier personnel d'un jeune est conservé sur une période de 2 ans après la fin des services. Ce dossier est conservé dans un serveur sécurisé et dans un classeur verrouillé afin d'en préserver la confidentialité.

7.8
Un requérant, c'est-à-dire un jeune de 14 ans et plus ou un titulaire de l'autorité parentale d'un jeune de moins de 14 ans peut effectuer une demande pour prendre connaissance des renseignements dans son

dossier personnel. Une telle demande doit se faire par écrit adressée à la direction générale. L'accès au dossier est gratuit. Un formulaire indiquant qu'une copie d'une partie ou de la totalité du dossier fut remise au requérant doit être signé par ce dernier.

7.9

L'organisme doit répondre à une demande d'accès au dossier dans les 30 jours où elle lui est faite. Le Comité d'accès analyse la demande et doit remettre par écrit adressé au requérant les motifs motivant l'acceptabilité ou le refus de la demande. Dans le cas d'un refus, le requérant peut contacter la Commission d'accès à l'information dans les 30 jours suivant la date du refus de la demande ou de l'expiration du délai pour y répondre.

7.10

Le Comité d'accès a le droit de refuser momentanément de mentionner l'existence de renseignements ou de communiquer une information à une personne si tels renseignements ou informations sont susceptibles de nuire à la sécurité, de causer un préjudice grave à sa santé ou celle d'autrui, de mettre sa vie en danger ou celle d'autrui.

7.11

Un requérant de 14 ans et plus ou le titulaire de l'autorité parentale d'une jeune de moins de 14 ans a le droit de consulter son dossier, de faire corriger les erreurs qu'il contient et de faire supprimer des informations qui sont fausses, équivoques ou non pertinentes après une rencontre avec la direction générale de l'organisme.

7.12

Tous autres renseignements personnels que le SQUAT Basse-Ville détient concernant les employés et les administrateurs sont conservé dans un serveur sécurisé par mot de passe et dans un bureau sous clefs et seuls les membres autorisés peuvent y avoir accès.

8- ENTRÉE EN VIGUEUR

La politique est adoptée le 16 avril 2002 et entre en vigueur en *date de son adoption*.

ANNEXE 1

Procédure à suivre en cas d'incidents de confidentialité

Les étapes qui suivent peuvent être réalisées simultanément.

1. **Évaluer la situation.** L'organisme qui a des raisons de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel qu'il détient doit notamment :
   - Établir les circonstances de l'incident;
   - Identifier les renseignements personnels impliqués;
   - Identifier les personnes concernées;
   - Trouver le problème, que ce soit une erreur, une vulnérabilité, etc.

   Cette évaluation doit se poursuivre tant que tous les éléments n'ont pas été identifiés.

2. **Diminuer les risques.** L'organisme doit prendre rapidement les mesures raisonnables qui s'imposent afin de diminuer les risques qu'un préjudice, qu'il soit sérieux ou non, ne soit causé et pour éviter que de nouveaux incidents de même nature ne surviennent, par exemple :
   - Cesser la pratique non autorisée;
   - Récupérer ou exiger la destruction des renseignements personnels impliqués;
   - Corriger les lacunes informatiques.

3. **Identifier la nature du préjudice.** L'objectif consiste à déterminer s'il faut aviser la Commission d'accès à l'information et les personnes concernées ainsi qu'établir les mesures à mettre en place pour diminuer les risques notamment :
   - Inscrire une notre dans les dossiers visés par un risque de vol d'identité;
   - Exiger des vérifications supplémentaires.

   Évaluation du préjudice

   Lors d'un incident de confidentialité, l'organisme doit évaluer s'il en découle un risque qu'un préjudice soit causé à une personne dont un renseignement personnel est concerné. Il doit alors considérer plusieurs facteurs, dont :

   - La sensibilité des renseignements personnels tels un renseignement financier ou un renseignement d'identité;
   - Les conséquences appréhendées de l'utilisation de ces renseignements comme un vol d'identité, une fraude financière, une atteinte importante à la vie privée;
   - La probabilité que ces renseignements puissent être utilisées à des fin préjudiciables.

Un préjudice sérieux correspond à un acte ou à un événement susceptible de porter atteinte à la personne concernée ou à ses biens et de nuire à ses intérêts de manière non négligeable. Il peut conduire, par exemple :

- À l'humiliation;
- À une atteinte à la réputation;
- À une perte financière;
- À un vol d'identité;
- À des conséquences négatives sur un dossier de crédit;
- À une perte d'emploi.

4. **Inscrire l'incident au registre,** que le risque de préjudice soit qualifié ou non de sérieux.

5. **S'il y a un risque de préjudice sérieux.** L'organisme doit :

   - **Aviser la Commission d'accès à l'information dès que possible,** même s'il n'a pas colligé l'ensemble des informations relatives à l'incident, et remplir la déclaration par la suite. Il peut ainsi aviser commission d'accès à l'information de l'incident et, plus tard, confirmer le nombre de personnes concernées;
   - **Aviser toute personne dont un renseignement personnel est concerné par l'incident,** à moins que cet avis ne soit susceptible d'entraver une enquête. Un délai peut s'appliquer entre le moment où l'organisme prend connaissance de l'incident et celui où il en avise les personnes concernées. Ce délai peut être nécessaire afin, par exemple, d'identifier les renseignements personnels impliqués, les personnes concernées, la faille de sécurité et pour colmater celle-ci ou pour éviter d'entraver une enquête en cours.

   Ces avis sont <u>obligatoires</u>

6. **S'il y a un risque de préjudice sérieux :** l'organisme peut aussi aviser toute personne ou tout organisme susceptible de diminuer ce risque. À cette fin, il ne peut lui communiquer que les renseignements personnels qui sont nécessaires à la poursuite de cet objectif. L'obtention du consentement de la personne concernée par les renseignements transmis n'est pas requise. Toutefois, la personne responsable de la protection des renseignements personnels doit enregistrer la communication pour garder des traces documentaires de celle-ci comme :
   - À qui ces renseignements sont communiqués;
   - Dans quelles circonstances;
   - Quels renseignements ont été transmis;
   - Quels sont les objectifs de cette démarche.