Chapitre 3

Audit – Protection des renseignements personnels

Ville de Sherbrooke

Bureau du vérificateur général

TABLE DES MATIÈRES

LISTE DES ACRONYMES

AIPRP	Accès à l'information et protection des renseignements personnels
CAI	Commission d'accès à l'information
CE	Comité exécutif
CM	Conseil municipal
DG	Direction générale
EFVP	Évaluation des facteurs relatifs à la vie privée
PRP	Protection des renseignements personnels
RAD	Responsable de l'accès aux documents
RP	Renseignement personnel
RPRP	Responsable de la protection des renseignements personnels
STI	Service des technologies de l'information
SRH	Service des ressources humaines
SFIN	Service des finances
SGRE	Service du greffe
SPGT	Service de la planification et de la gestion du territoire
SPS	Service de police
UMQ	Union des municipalités du Québec
VG	Vérificateur général

RESSOURCES IMPLIQUÉES

Équipe de vérification

Yves Denis, CPA auditeur, vérificateur général de la Ville de Sherbrooke

Anne-Héloïse Bédard, Leader, Risques d'entreprise, Québec, MNP
Fatimata Do Rego, Directrice, Risques d'entreprise, MNP
Raphaël Huchet, Conseiller, Risques d'entreprise, MNP

Comité-conseil du Bureau du vérificateur général

Jean Cinq-Mars, Consultant, B. Sc. (Hon), M.A.P.
Maxime Pedneaud-Jobin, ancien maire de Gatineau, conférencier, auteur
Michel Samson, FCPA auditeur

Révision linguistique

Anne Fonteneau, docteure en littérature québécoise, réviseure linguistique agréée honoraire

1. VUE D'ENSEMBLE

1.1 Aperçu du sujet

1 Aujourd'hui, la protection des renseignements personnels (RP) s'avère un objet de gestion crucial. En effet, les risques d'atteintes à la vie privée ne cessent d'augmenter depuis plusieurs années, notamment en raison de l'utilisation de diverses technologies qui facilitent la collecte de RP, entre autres celles des réseaux sociaux.

2 À l'instar d'autres domaines, le cadre législatif auquel la Ville de Sherbrooke (« la Ville ») est assujettie a été récemment modernisé par le gouvernement du Québec, avec la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (LQ 2021, c. 25) qui a modifié la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (« Loi sur l'accès »).* Son entrée en vigueur, graduelle, s'étend de septembre 2022 à septembre 2024. Cette loi favorise la transparence et donne plus de pouvoir aux individus sur leurs RP. Elle permet en outre de formaliser et de déployer un encadrement beaucoup plus robuste et strict.

3 Pour se conformer à ce cadre, les organisations doivent définir des dispositions précises et effectuer différentes actions en ce qui a trait à la gestion[1] (ou cycle de vie) des RP.

4 Pour que soient mieux cernées les exigences de la *Loi sur l'accès*, quelques notions importantes sont définies ci-après.

Renseignements personnels

5 Un RP[2] est une information qui permet d'identifier, directement ou indirectement, une personne physique. Les RP[3] sont confidentiels, et leur confidentialité découle du droit à la vie privée, permettant à toute personne d'exercer un contrôle sur l'utilisation et la circulation de ses informations.

6 Pour que leur gestion en soit facilitée, les RP doivent être catégorisés et classés selon leur degré de sensibilité.

Catégories

7 Les catégories de RP données à titre d'exemple par le gouvernement du Québec sont les suivantes[4] :

- **Renseignements d'identification** : adresse, numéro de téléphone, sexe, âge, numéro d'assurance sociale, numéro d'assurance maladie, identifiant numérique, etc.
- **Renseignements de santé** : dossier médical, diagnostic, consultation d'une professionnelle ou d'un professionnel de la santé, médicament, ordonnance, renseignements sur la cause d'un décès, etc.

---

1 La gestion (ou le cycle de vie) réfère à la collecte, à l'utilisation, à la communication, au stockage et à la destruction des renseignements personnels.

2 *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, article 54.

3 Voir la définition à la Commission d'accès à l'information (CAI) : https://www.cai.gouv.qc.ca/protection-renseignements-personnels/sujets-et-domaines-dinteret/renseignement-personnel-definition.

4 Voir la *Présentation des concepts-clés liés aux renseignements personnels* : https://www.quebec.ca/gouvernement/travailler-gouvernement/travailler-fonction-publique/services-employes-etat/conformite/protection-des-renseignements-personnels/definitions-concepts/concepts.

- **Renseignements financiers** : revenu d'une personne, information relative à l'impôt, numéro de compte bancaire, biens possédés, numéros de cartes de crédit, etc.
- **Renseignements relatifs au travail** : dossier disciplinaire, motifs d'absence, dates de vacances, salaire, évaluation du rendement, heures d'entrée et de sortie liées au lieu de travail, etc.
- **Renseignements scolaires et relatifs à la formation** : inscription à des cours, choix de cours, résultats scolaires, diplômes, curriculum vitæ, etc.
- **Renseignements relatifs à la situation sociale ou familiale** : documents qui attestent l'état civil, le fait qu'une personne ait ou non des enfants, ou qu'elle reçoive des prestations d'aide sociale ou de chômage, etc.

Sensibilité

8 L'évaluation du degré de sensibilité permet, entre autres, de déterminer le niveau de protection des RP eu égard aux risques encourus en matière de disponibilité, d'intégrité et de confidentialité.

9 « Un renseignement personnel est sensible lorsqu'il suscite un haut degré d'attentes raisonnables en matière de vie privée, en raison de sa nature ou du contexte de son utilisation.[5] » Le niveau de sensibilité d'un RP est ainsi déterminé par le degré de préjudice que pourraient causer sa divulgation ou son accès non autorisé. Il est généralement évalué en fonction de la nature des informations, de la gravité des conséquences de sa divulgation pour la personne concernée et pour l'organisation qui le détient. Un RP est, par définition, considéré comme sensible s'il est de nature médicale, biométrique, ou autrement intime[6].

Évaluation des facteurs relatifs à la vie privée (EFVP)

10 L'EFVP[7] est une démarche préventive et évolutive visant à mieux protéger les RP et à respecter la vie privée des personnes physiques. Concrètement, il s'agit d'une analyse d'impact. Avant le début d'un projet, et au cours de celui-ci, cette démarche permet d'analyser les facteurs ayant un effet positif ou négatif sur le respect de la vie privée des personnes concernées. Ces facteurs sont :

- la conformité du projet aux lois applicables en matière de protection des RP et le respect des principes l'appuyant;
- l'identification des risques d'atteinte à la vie privée engendrés par le projet et l'évaluation de leurs conséquences;
- la mise en place et le maintien de stratégies pour éviter ou réduire efficacement ces risques, y compris éviter de collecter des RP inutilement).

Incident de confidentialité

11 Selon la *Loi sur l'accès*[8], un incident de confidentialité correspond à tout accès, toute utilisation ou toute communication d'un RP non autorisés par la loi, de même qu'à sa perte ou à toute autre atteinte à sa protection.

---

[5] Voir la CAI : https://www.cai.gouv.qc.ca/protection-renseignements-personnels/sujets-et-domaines-dinteret/renseignement-personnel-definition.

[6] Voir la note 4.

[7] Voir la CAI : https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_GU_EFVP.pdf?gt=%C3%A9valuation.

[8] Sources : Gouvernement du Québec et art. 63.9 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.*

12 Par exemple, un incident de confidentialité pourrait se produire lorsque :

- un membre du personnel consulte un RP sans autorisation;
- un membre du personnel communique des RP au mauvais destinataire;
- l'organisation est victime d'une cyberattaque : hameçonnage, rançongiciel, etc.

13 Si une organisation a des motifs de croire que s'est produit un incident de confidentialité impliquant un RP qu'elle détient, elle doit prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature se produisent.

1.2 Exigences légales et réglementaires auxquelles la Ville est assujettie

14 Outre la *Loi sur l'accès*, pour le secteur public, les lois suivantes (liste non exhaustive) contiennent des particularités en matière de protection des RP. Leur liste est présentée à l'annexe 1 de ce rapport.

- *Loi sur les archives (RLRQ, c. A-21.1);*
- *Loi concernant le cadre juridique des technologies de l'information (RLRQ, c. C-1.1);*
- *Loi sur la protection de la jeunesse (RLRQ, c. P-34.1);*
- *Charte des droits et libertés de la personne (RLRQ, c. C-12).*

1.3 Principaux enjeux et risques liés aux renseignements personnels

15 La gestion des RP comporte plusieurs enjeux et risques importants, principalement en raison des conséquences potentielles de leur divulgation sur la vie privée et la sécurité des individus.

16 Voici les principaux enjeux et risques généralement reconnus par la pratique.

Enjeux

- **Protection de la vie privée :** Les villes collectent des données sensibles telles que les noms, adresses, informations financières, etc. La protection de ces informations est essentielle pour maintenir la confiance des citoyens et citoyennes, assurer la confidentialité des données personnelles et respecter le droit à la vie privée des individus.
- **Conformité réglementaire :** Les villes doivent se conformer à des réglementations strictes concernant la gestion des données personnelles (comme le font l'Europe avec le Règlement général sur la protection des données (RGPD) et la Californie avec le California Consumer Privacy Act (CCPA), etc.), ce qui implique des processus robustes de gestion et de protection des données.
- **Transparence et responsabilité :** Les villes doivent être transparentes sur les types de données collectées, les raisons de cette collecte, et la manière dont elles sont utilisées, communiquées le cas échéant, et protégées.
- **Utilisation éthique des données :** Les villes doivent veiller à utiliser les données personnelles de manière éthique, et éviter l'abus de surveillance ou toute autre forme d'utilisation qui pourrait porter atteinte aux droits individuels.
- **Consentement éclairé** : Les villes doivent obtenir le consentement des individus pour que leurs données soient utilisées dans des buts précis.

- **Équité et non-discrimination** : Les villes doivent veiller à ce que les données personnelles ne soient pas utilisées pour discriminer ou stigmatiser des groupes ou des individus.
- **Sécurité des données** : Les villes doivent avoir la capacité de protéger les données personnelles contre les accès non autorisés, les pertes, les vols et les fuites d'information.
- **Gestion des données à grande échelle** : Les villes doivent gérer efficacement de grandes quantités de données tout en maintenant leur intégrité et leur confidentialité.
- **Interopérabilité et partage des données** : Les villes doivent faciliter le partage de données entre différents services et organisations tout en assurant la sécurité des informations.
- **Ressources** : Les villes doivent évaluer les moyens suffisants pour se conformer à la Loi 25, ainsi que le temps requis pour mettre en œuvre les exigences stipulées par cette loi.
- **Gestion continue et efficace des données :** Les villes doivent effectuer deux actions principales : mettre régulièrement à jour l'inventaire des RP pour refléter avec précision les données détenues, et organiser périodiquement des formations/sessions de sensibilisation pour maintenir une conscience et une compréhension élevées des exigences en matière de protection des RP autant dans les différents services et que chez les citoyennes et citoyens.

Risques

- **Fuite de données :** Il s'agit des risques de divulgation volontaire ou involontaire d'informations sensibles en cas de non-protection des données pouvant affecter la vie privée des individus. Les données personnelles étant une cible privilégiée pour les cyberattaques, les fuites de données peuvent exposer les citoyens et les citoyennes à des risques de fraude, d'usurpation d'identité et à d'autres formes de cybercriminalité.
- **Mauvaise gestion des données :** Une gestion inadéquate peut conduire à des erreurs dans le traitement des données, à des décisions basées sur des données incorrectes ou à des violations de la confidentialité.
- **Cyberattaque et rançongiciel :** Les systèmes municipaux sont souvent visés par des cyberattaques, y compris par des attaques de rançongiciel qui peuvent paralyser des services essentiels si les systèmes ne sont pas correctement sécurisés.
- **Surveillance excessive :** L'utilisation de technologies de surveillance, comme la reconnaissance faciale, peut conduire à une surveillance de masse et à une violation de la vie privée si elle n'est pas strictement réglementée.
- **Discrimination et biais :** Les décisions automatisées basées sur des ensembles de données peuvent perpétuer ou amplifier des biais existants, menant à une discrimination contre certains groupes de personnes.
- **Mauvaise utilisation ou abus de pouvoir** : Il s'agit du risque que les données soient utilisées à des fins non éthiques ou abusives par les autorités ou des tiers.
- **Obsolescence technologique :** Il s'agit du risque lié à l'utilisation de systèmes de stockage et de sécurité obsolètes, qui ne sont pas adaptés aux menaces actuelles.
- **Perte de confiance du public** : La mauvaise gestion des données peut entraîner une perte de confiance des citoyens et citoyennes envers les villes.
- **Réputation** : Les incidents de confidentialité en matière de RP peuvent nuire à la réputation des villes et des personnes concernées.

- **Sanctions légales et financières :** De nombreuses lois et réglementations exigent que les villes protègent les données personnelles de leurs citoyens et citoyennes. En cas de non-conformité, elles peuvent faire face à des amendes importantes ou à des poursuites judiciaires.

1.4 Politiques et procédures de la Ville

17 Les politiques et procédures pertinentes de la Ville sont présentées au tableau suivant :

Politiques et procédures	Description
Politique de sécurité de l'information de la Ville de Sherbrooke (ADM-2115) CM-2022-7544 (21 juin 2022)	Cette politique, adoptée par le conseil municipal, énonce : • les domaines d'application; • les principes généraux, dont la disponibilité, l'intégrité et la confidentialité des informations; • les principaux rôles et responsabilités, dont la personne responsable d'un actif informationnel.
Cadre de gestion de la sécurité de l'information CE-2022-2361 (21 juin 2022)	Ce cadre de gestion vise, en précisant les rôles et responsabilités, à assurer une mise en œuvre efficace et coordonnée des activités en matière de sécurité de l'information telles que la stratégie, la gestion des risques concertée ainsi que le respect de la conformité.
Utilisation d'Internet et des médias sociaux (ADM-2113) CM-2016-1934, 20 juin 2016	Cette politique administrative a pour but d'encadrer l'utilisation d'Internet et des médias sociaux tout en en maximisant les avantages. Elle vise essentiellement à établir les droits et les obligations des utilisatrices et utilisateurs et de la Ville pour un usage responsable d'Internet et des médias sociaux.
Procédure sur le mode d'octroi des autorisations d'accès aux salles informatiques de la Ville de Sherbrooke (ADM-2120) (janvier 2002, révisée en mars 2014)	Cette procédure administrative : • encadre les autorisations d'accès aux salles informatiques de la Ville; • détermine les rôles et responsabilités de chacun; • décrit le fonctionnement des systèmes de sécurité installés dans les salles informatiques de la Ville.
Assermentation des personnes ayant accès aux systèmes électroniques de la Ville de Sherbrooke (ADM-2126) (8 décembre 2000 – comité de gestion)	Cette procédure administrative vise à assermenter le personnel de la Ville et les fournisseurs ayant accès à ses systèmes informatiques pour s'assurer qu'ils s'engagent à : • agir en qualité de fonctionnaire municipal ou d'employé d'un fournisseur de la Ville, fidèlement et conformément à la loi, sans partialité, crainte, faveur ni affection; • respecter le caractère confidentiel de toute information (protégée par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*) obtenue en raison ou à l'occasion de leur travail à la Ville; • ne divulguer et à ne reproduire ou diffuser d'aucune façon les informations ou documents ainsi protégés ou susceptibles d'être ainsi protégés, ni à y donner accès à qui que ce soit; • prendre connaissance de la Politique de sécurité de l'information de la Ville de Sherbrooke et de la Politique d'utilisation de tous systèmes électroniques de la Ville de Sherbrooke et à s'y conformer.

Politiques et procédures	Description
Politique de confidentialité à l'égard des renseignements personnels CM-2024-9111 (adoptée le 6 février 2024)	Cette politique a pour objectifs : • d'énoncer les orientations et les principes directeurs destinés à assurer efficacement la confidentialité de tout RP collecté par tout moyen technologique; • de protéger la confidentialité de tout RP collecté par la Ville tout au long de son cycle de vie; • d'indiquer les moyens technologiques utilisés pour collecter tout RP, les fins auxquelles il est collecté et son traitement par la Ville; • d'assurer la confiance du public à l'égard de la Ville en faisant preuve de transparence concernant le traitement des RP et les mesures de protection et d'accès qui les encadrent.
Politique sur la gouvernance en matière de protection des renseignements personnels CM-2024-9110 (adoptée le 6 février 2024)	Cette politique a pour objectifs : • d'énoncer les principes encadrant la gouvernance de la Ville à l'égard des RP tout au long de leur cycle de vie et de l'exercice des droits des personnes concernées; • de prévoir le processus de traitement des plaintes relatives à la protection des RP; • de définir les rôles et responsabilités en matière de protection des RP à la Ville; • de décrire les activités de formation et de sensibilisation que la Ville offre à son personnel.

1.5 Rôles et responsabilités en matière de protection des renseignements personnels

18 La gestion et la protection des RP (PRP) sont grandement facilitées lorsque les rôles et responsabilités des principaux acteurs en la matière sont définis. Nous avons recensé ceux prévus par les politiques et procédures en matière de PRP de la Ville.

Conseil municipal de la Ville

- S'assurer de la PRP que la Ville de Sherbrooke détient;
- S'assurer de la disponibilité des ressources nécessaires afin que la Ville puisse s'acquitter de ses obligations en matière de PRP;
- S'assurer de la disponibilité des ressources nécessaires à la gestion des incidents de confidentialité selon leur niveau de criticité et les conséquences qu'ils peuvent avoir sur la réputation de la Ville ou la vie de la personne concernée.

La personne ayant la plus haute autorité au sein de la Ville (mairesse)

- Veiller à assurer le respect et la mise en œuvre de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*;
- Veiller à faciliter la fonction de responsable de l'accès aux documents et celle de responsable de la protection des renseignements personnels (RPRP), dans la mesure où elle les délègue.

Direction générale

- S'assurer de soumettre aux instances toute demande visant la disponibilité des ressources nécessaires afin que la Ville puisse s'acquitter de ses obligations en matière de PRP;
- Siéger au comité AIPRP;
- S'assurer de soumettre aux instances concernées toute demande visant la disponibilité des ressources nécessaires à la gestion des incidents de confidentialité selon leur niveau de criticité et les conséquences qu'ils peuvent avoir sur la réputation de la Ville ou la vie de la personne concernée.

Comité AIPRP

- Émettre des recommandations au conseil municipal (CM) ou au comité exécutif (CE);
- Veiller à la mise en place de mesures visant la sensibilisation et la formation des membres du personnel et de la direction de la Ville sur les obligations et les pratiques en matière de PRP;
- Identifier les principaux risques en matière de PRP et en aviser la direction afin que des mesures correctives soient proposées;
- Approuver toute dérogation aux principes généraux qui auront été établis en matière de PRP;
- Émettre des directives pour la PRP, notamment leur stockage par des tiers et à l'extérieur du Québec;
- Être consulté, dès le début d'un projet et aux fins de l'EFVP, sur tous les projets d'acquisition, de développement et de refonte des systèmes d'information ou de prestation électronique de services impliquant des RP :
    - veiller à ce que la réalisation de l'EFVP soit proportionnelle à la sensibilité des renseignements concernés, aux fins auxquelles ils sont utilisés, à leur quantité et à leur distribution, et au support numérique sur lequel ils sont stockés;
    - le cas échéant, s'assurer que le projet permet de communiquer à la personne concernée les RP informatisés recueillis auprès d'elle dans un format technologique structuré et couramment utilisé;
- Transmettre ses recommandations non suivies à la personne responsable de la protection des renseignements personnels (RPRP);
- Être avisé de tout incident de confidentialité impliquant les RP et conseiller la Ville quant aux suites à y donner;
- Mettre à jour la procédure relative à la gestion des incidents de la Ville dans l'éventualité d'un incident de confidentialité;
- Mettre à jour les règles de collecte et de stockage des RP provenant de sondages;
- Étudier toute question d'intérêt touchant la PRP;
- Mettre à jour les mesures relatives à la vidéosurveillance et s'assurer du respect de la vie privée lors de son utilisation.

RPRP

19 Le rôle principal du ou de la RPRP est de veiller à ce que les RP collectés, utilisés, divulgués ou tout autrement traités, le soient de manière responsable et conforme aux lois et règlements applicables en matière de protection des RP. Cette personne est le point de contact principal pour les questions relatives à la PRP.

20 Les responsabilités du ou de la RPRP sont les suivantes :

- S'assurer de la PRP tout au long de leur cycle de vie, de leur collecte à leur destruction;
- Siéger au comité AIRP;
- Vérifier les obligations de confidentialité liées à la communication de RP lors de mandats ou de contrats de services confiés à des tiers, conformément à l'article 6.3.2 de la Politique sur la gouvernance en matière de protection des renseignements personnels;
- Agir comme personne-ressource pour toute question ou tout problème relatif à la sécurité et à la confidentialité des RP détenus par la Ville ou pour son compte;
- En cas d'incident de confidentialité, prendre en charge le traitement de l'incident et se faire assister, le cas échéant, par le directeur ou la directrice du Service des technologies de l'information, la personne responsable de la sécurité de l'information, le chef ou la cheffe de la division du contentieux du Service des affaires juridiques, le directeur ou la directrice du Service des communications, ainsi que par toute autre personne pouvant lui être utile selon la nature de l'incident. À ce titre, il ou elle doit :
  - Déterminer si l'incident de confidentialité est imputable à la Ville;
  - Diriger l'évaluation du risque de préjudice et, à cet effet, évaluer le risque qu'un préjudice soit causé et en déterminer le degré de sévérité. Lors de cette évaluation sont notamment analysées la sensibilité du renseignement concerné, les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables;
  - Évaluer les mesures préventives et correctrices mises en place à la suite de l'incident et suggérer les correctifs nécessaires le cas échéant;
  - Aviser, conformément à la Procédure relative à la gestion des incidents de confidentialité, la personne dont un RP est visé par l'incident, lorsque celui-ci présente un risque de préjudice sérieux;
  - Aviser, conformément à la Procédure relative à la gestion des incidents de confidentialité, toute personne ou tout organisme susceptible de faire diminuer le risque de préjudice sérieux;
  - Aviser la CAI lorsque l'incident de confidentialité présente un risque de préjudice sérieux, en respectant les dispositions du *Règlement sur les incidents de confidentialité* (RLRQ, c. A-2.1, r. 3.1);
  - Aviser, avec diligence, le chef ou la cheffe de la division du contentieux du Service des affaires juridiques afin que les assureurs de la Ville soient contactés, le cas échéant;
  - Aviser, avec diligence, le Service de police de Sherbrooke et le chef ou la cheffe de la division du contentieux du Service des affaires juridiques si, après analyse de l'incident, un crime semble avoir été commis, et assurer la conservation des éléments de preuve en collaboration avec la personne responsable de la sécurité de l'information;

- Inscrire l'incident de confidentialité dans un registre prévu à cet effet, dont le contenu est établi selon les exigences du *Règlement sur les incidents de confidentialité* (RLRQ, c. A-2.1, r. 3.1);
- Sur demande de la CAI, lui transmettre une copie de ce registre;
- Effectuer une analyse approfondie de l'incident et décider, en fonction de sa gravité, d'en discuter avec les différentes parties prenantes et d'apporter, s'il y a lieu, les modifications nécessaires à la procédure, le tout dans un objectif de performance du processus de gestion des incidents.

Responsable/répondant[9] ou répondante PRP

- Collaborer avec le ou la RPRP à la mise en œuvre des obligations prévues par la loi dans son unité administrative;
- Être au courant de tout incident de confidentialité impliquant les RP dans son unité;
- Contribuer aux EFVP impliquant son unité;
- Agir comme personne-ressource en matière de PRP et diffuser les obligations de la loi au personnel de son unité;
- Participer aux formations offertes par la Ville en matière de PRP;
- Participer à la mise en place et au maintien des mesures de prévention et de PRP dans son unité;
- Assister les membres de son unité administrative dans l'application de la Politique de confidentialité et de toutes procédures ou directives relatives à la PRP;
- Collaborer à la formation des membres de son unité;
- Recueillir le maximum d'information en lien avec un incident de confidentialité survenu dans son unité;
- Soutenir le ou la gestionnaire de son unité dans la mise en place des mesures de prévention correctrices qui s'imposent afin d'atténuer les conséquences de l'incident ou de le faire cesser;
- Soutenir le ou la gestionnaire de l'unité administrative dans la mise en œuvre des mesures préventives qu'il ou elle aura adoptées afin d'éviter qu'un tel incident ne se reproduise;
- Remplir le formulaire de déclaration de l'incident;
- Déclarer l'incident au ou à la responsable de la sécurité de l'information lorsqu'il résulte d'une action malveillante ou d'une défaillance technique ou technologique, afin de déclencher une investigation en ce qui concerne la cybersécurité.

Autres intervenants et intervenantes

- Diverses responsabilités transversales sont aussi décrites dans la politique-cadre de gouvernance pour les entités suivantes : communications, affaires juridiques, technologies de l'information, responsable de la sécurité de l'information, directions de service, arrondissements, personnel de la Ville et tiers.

[9] Personne identifiée par service en tant que responsable de la protection des RP dans son unité.

2. OBJECTIFS ET PORTÉE DE L'AUDIT

21 En vertu des dispositions de la *Loi sur les cités et villes*, j'ai réalisé une mission d'audit de performance portant sur la gestion de la protection des renseignements personnels (PRP). Cette mission a été réalisée conformément à la Norme canadienne de mission de certification (NCMC 3001), émise par le Conseil des normes d'audit et de certification soutenu par CPA Canada. Elle a couvert les aspects portant uniquement sur les RP découlant de la *Loi sur l'accès* depuis son entrée en vigueur en septembre 2022.

22 Mes travaux visaient à s'assurer, d'une part, que la Ville, a pris, en temps opportun, les mesures nécessaires pour respecter les exigences de la *Loi sur l'accès*, incluant le recensement et la documentation de la nature des RP qu'elle détient ou est amenée à détenir et, d'autre part, qu'elle s'est appuyée sur une analyse de risques et des coûts pour déterminer les mesures de protection à mettre en place et prioriser leur déploiement. Nos travaux de vérification ont pris fin en juillet 2024.

Responsabilité du vérificateur général

23 La responsabilité du vérificateur général de la Ville de Sherbrooke consiste à fournir une conclusion sur les objectifs de l'audit et il peut émettre des recommandations. Pour ce faire, j'ai recueilli les éléments probants suffisants et appropriés pour fonder ma conclusion et pour obtenir un niveau raisonnable d'assurance. Mon évaluation est basée sur les critères que j'ai jugés valables dans les circonstances et qui sont exposés à l'annexe 2 de ce rapport.

24 Le vérificateur général de la Ville de Sherbrooke applique la Norme canadienne de gestion de la qualité (NCGQ 1) et, en conséquence, maintient un système exhaustif de contrôle qualité qui comprend des normes internes documentées en ce qui concerne la conformité aux règles de déontologie, aux normes professionnelles et aux exigences légales et réglementaires applicables. De plus, il se conforme aux règles sur l'indépendance et aux autres règles du *Code de déontologie des comptables professionnels agréés du Québec,* lesquelles reposent sur les principes fondamentaux d'intégrité, d'objectivité, de compétence professionnelle et de diligence, de confidentialité et de conduite professionnelle.

3. RÉSULTATS DE L'AUDIT

25 La mise en place de règles de gouvernance pour assurer une PRP adéquate n'est pas encore achevée. Les rôles et responsabilités doivent être révisés, les politiques, amendées, et un meilleur encadrement des formations est nécessaire (section 3.1).

26 L'inventaire des RP n'est pas finalisé, et aucun processus n'a été mis en place par la Ville pour garantir la collecte exhaustive et la conservation appropriée de ces données (section 3.2).

27 La gestion des consentements des personnes concernées n'est pas suffisamment encadrée, et toutes les situations nécessitant leur collecte ne sont pas encore répertoriées (section 3.3).

28 Le cadre formel pour la communication des RP sans consentement n'est pas à jour au sein de la Ville, et aucun processus n'a été instauré pour identifier toutes les situations nécessitant une communication sans consentement, conformément aux exigences de la *Loi sur l'accès* (section 3.4).

29 De même, la Ville n'a pas encore élaboré de manière exhaustive les ententes de communication des RP lorsqu'elle les recueille pour le compte d'un autre organisme public avec lequel elle collabore, ou lorsqu'elle les communique sans le consentement des personnes concernées (section 3.5).

30 Les mesures prises jusqu'à présent en termes de conservation et de destruction des RP ne garantissent pas leur gestion sécurisée (section 3.6).

31 Il est nécessaire de mettre en place un dispositif de suivi des incidents de confidentialité et de mettre en œuvre des mesures de sécurité afin d'assurer la PRP et d'éviter toute atteinte à la vie privée des citoyens (section 3.7).

32 Par ailleurs, la Ville n'a pas encore réalisé d'analyse des risques par rapport aux coûts pour prioriser et valider les mesures de protection à mettre en place pour la gestion des RP (section 3.8).

33 Enfin, aucun mécanisme de reddition de comptes n'est en place pour assurer la transparence et la responsabilité dans la gestion des RP (section 3.9).

3.1 Responsabilités de la Ville de Sherbrooke

34 En tant qu'organisme public, la Ville de Sherbrooke est responsable de protéger les RP qu'elle recueille, détient, utilise, communique, conserve et détruit. Elle doit mettre en place des structures et des règles, et adopter des pratiques pour les protéger de manière adéquate.

3.1.1 Rôles et responsabilités du RPRP

35 La personne détenant la plus haute autorité au sein de la Ville est responsable de la PRP et doit veiller au respect et à la mise en œuvre de la *Loi sur l'accès*. Toutefois, une partie ou l'intégralité des fonctions de RPRP peut être déléguée à une personne ayant les compétences requises et un pouvoir décisionnel important. Cette délégation doit être documentée par écrit et effectuée par la personne détenant la plus haute autorité, en plus d'être notifiée à la CAI.

36 Il a été constaté que la nomination du RPRP a été officiellement documentée via un formulaire de désignation signé par la mairesse, en tant que plus haute autorité au sein de la Ville. De plus, la CAI a été avisée par écrit de cette nomination. Cependant, aucune communication générale interne n'a été réalisée concernant le titre et les coordonnées du RPRP, ni sur la manière de le contacter en cas de besoin concernant la *Loi sur l'accès*. De même, aucune communication générale interne n'a été effectuée concernant les répondantes et répondants désignés par service.

37 Par ailleurs, les rôles et responsabilités du RPRP sont partiellement définis dans les politiques et procédures de la Ville, conformément aux exigences de la *Loi sur l'accès* et aux directives de la CAI. Cependant, la politique de gouvernance ne précise pas toutes les responsabilités du RPRP en termes de droit à la portabilité, de sensibilisation et de formation, ainsi que de reddition de comptes en matière de PRP. De plus, la politique ne clarifie pas suffisamment la responsabilité du RPRP concernant la tenue des différents registres d'utilisation et de communication des RP. Bien que certains registres soient clairement désignés comme relevant de sa responsabilité, d'autres ne le sont pas, alors qu'il est chargé de les maintenir.

38 Il serait judicieux pour le RPRP d'envisager d'élargir les rôles et responsabilités des répondants et répondantes, qui possèdent une connaissance approfondie des activités de leurs services, afin de déléguer davantage. Cependant, il est important de garantir que les répondants et répondantes sont toujours bien informés et formés sur les questions de PRP.

RECOMMANDATIONS À LA VILLE DE SHERBROOKE
1. Inclure les dispositifs du droit à la portabilité dans la politique de gouvernance afin de se préparer aux exigences de la *Loi sur l'accès* prévu pour septembre 2024. Inclure dans la responsabilité du RPRP le fait de répondre aux demandes relatives à ce droit.
2. Ajouter dans les responsabilités du RPRP, dans la politique de gouvernance (section 15.3), le fait de tenir et de mettre à jour tous les registres mentionnés à la section 7 de la présente politique, de sensibiliser et de former les membres du personnel et de mettre en place un système de reddition de comptes en matière de PRP. Préciser également qu'il doit recevoir et traiter les avis de violations relatives aux obligations de confidentialité.
3. Mentionner sur le site public de la Ville que le RAD occupe également la fonction de RPRP et désigner des répondants et répondantes pour les 6 nouveaux services de la Ville créés ou restructurés en 2024 **(voir les services mis en évidence dans l'organigramme présenté à l'**annexe 3**)**.
4. Effectuer une communication générale pour tout le personnel de la Ville fournissant la liste des contacts et rôles des répondants et répondantes et du RPRP, et mentionnant l'existence d'une page intranet réservée.
5. Évaluer la capacité de l'organisation, dont celle du RPRP, à pouvoir entreprendre toutes les actions requises par la ***Loi sur l'accès*** afin de s'y conformer.
6. Ajouter des rôles et responsabilités pour les répondants et répondantes dans la Politique de gouvernance en matière de RP. Envisager d'ajouter leurs implications dans la mise à jour de l'inventaire des RP et des registres de communication et d'utilisation des RP, ainsi que dans l'identification des situations nécessitant la mise en place d'ententes, d'EFVP, de consentements, etc.

3.1.2 Comité AIPRP

39 À moins d'exceptions spécifiques établies par la CAI, chaque entité publique comme la Ville de Sherbrooke est tenue de former un comité AIPRP. Ce comité a pour mission de garantir la conformité, la transparence et la PRP de la Ville. Selon l'article 8.1 de la *Loi sur l'accès*, la composition et les responsabilités de ce comité relèvent de la Direction générale de la Ville.

40 On relève que la Ville a respecté cette obligation en constituant un comité AIPRP le 23 août 2023, placé sous l'autorité de la Direction générale. Le mandat du comité a été défini et validé par les autorités compétentes. Sa composition est également conforme à l'article 8.1 susmentionné, et des réunions avec ses membres sont organisées mensuellement.

41 Cependant, certaines lacunes ont été observées. Tout d'abord, l'absence d'une charte de comité laisse un vide en en ce qui a trait à l'encadrement pour la PRP et à la définition des rôles et responsabilités des membres. De plus, le calendrier des réunions n'est pas toujours respecté, et l'ordre du jour ne couvre pas systématiquement tous les sujets liés aux RP. En ce qui concerne les comptes rendus, ils ne sont pas rédigés de manière systématique après chaque réunion. Enfin, aucun processus formel n'a été établi pour suivre la mise en œuvre des plans d'action discutés lors des réunions du comité.

RECOMMANDATIONS À LA VILLE DE SHERBROOKE
7. Mettre en place une charte de comité afin de fournir un cadre commun de compréhension des activités du comité et définir les rôles et responsabilités de tous ses membres.
8. Intégrer au minimum dans l'ordre du jour du comité AIPRP, en plus des sujets existants, les suivants : 1/ Statut sur l'inventaire et/ou la cartographie des RP; 2/ Incidents de confidentialité; 3/ Évaluation des facteurs relatifs à la vie privée; 4/ Projets d'acquisition de logiciels et de systèmes; 5/ Communication des RP; 6/ Planification de la prochaine réunion.
9. Établir un processus d'approbation des comptes rendus des comités par les autorités compétentes de la Ville, en particulier si ces comptes rendus doivent être diffusés ou publiés. Cela garantira la vérification et la validation des informations contenues dans les comptes rendus avant leur diffusion officielle.
10. Mettre en place un processus formel de suivi des plans d'action discutés lors des rencontres du comité AIPRP. Ce processus devra inclure l'attribution de responsabilités claires aux parties prenantes concernées et des mécanismes de suivi régulier pour garantir que tous les engagements pris seront respectés avant la prochaine rencontre du comité.

3.1.3 Règles de gouvernance à l'égard des renseignements personnels

42 Il est essentiel que la Ville de Sherbrooke ait des règles de gouvernance en ce qui concerne les RP, et les rende accessibles sur son site Web. Ces règles, qui doivent être approuvées par le comité AIPRP, peuvent prendre la forme d'une politique, d'une directive ou d'un guide, et doivent inclure les éléments suivants :

- Définition des rôles et des responsabilités du personnel tout au long du cycle de vie des RP;
- Processus de traitement des plaintes liées à la PRP;
- Description des activités de formation et de sensibilisation à la PRP offertes au personnel;
- Mesures de protection particulières à l'égard des RP recueillis ou utilisés dans le cadre d'un sondage.

43 Ces exigences, énoncées à l'article 63.3 de la *Loi sur l'accès*, visent à assurer la transparence quant au traitement des RP et à la PRP, permettant ainsi à la population de mieux comprendre leur utilisation.

44 La Ville a développé une politique sur la gouvernance en matière de PRP ainsi qu'une politique de confidentialité, approuvées respectivement le 4 décembre 2023 et le 15 janvier 2024 par le comité AIPRP. Cependant, ces politiques présentent plusieurs lacunes :

- Certains aspects, tels que la désindexation, le droit à la portabilité, la décision automatisée et la biométrie, ne sont pas abordés;
- Le traitement des plaintes liées à la PRP est incomplet, ne détaillant pas suffisamment le processus de gestion des plaintes alors qu'il est requis par la *Loi sur l'accès;*
- La politique de gouvernance en matière de PRP couvre partiellement certains aspects tels que la communication sans consentement, les ententes de communication et les registres à tenir;
- Les rôles et responsabilités des plus hautes autorités de la Ville (mairesse, conseil municipal) et de la Direction générale ne sont pas définis de manière exhaustive;
- La politique de confidentialité des RP ne mentionne pas toutes les mesures exigées par la loi, et certaines directives devraient être intégrées dans la Politique de gouvernance en matière de RP. De plus, la Politique de protection des RP du Service de police (SPS) est obsolète et non alignée avec la politique de la Ville.

RECOMMANDATIONS À LA VILLE DE SHERBROOKE
11. Intégrer dans la Politique-cadre de gouvernance en matière de RP et mettre en place des procédures spécifiques sur les aspects suivants : la désindexation, le droit à la portabilité, la décision fondée exclusivement sur un traitement automatisé, la biométrie et le processus de gestion des plaintes comme le stipule l'article 63.3 de la *Loi sur l'accès*.
12. Réviser la Politique de gouvernance en matière de RP pour inclure de manière exhaustive les mesures prévues concernant le deuil dans les articles 88.0.1, 88.1 et 89.1 de la *Loi sur l'accès*. Ces directives devraient être intégrées dans la Politique de gouvernance en matière de RP et non seulement dans la Politique de confidentialité de la Ville.
13. Amender les politiques-cadres de gouvernance en matière de PRP et de confidentialité. Cela inclut l'ajout des rôles et responsabilités de la mairesse et du conseil municipal ainsi que l'ajustement en conséquence des rôles et responsabilités de la Direction générale.

14. Harmoniser la Politique de protection des données et des renseignements confidentiels du SPS avec la Politique de gouvernance en matière de RP de la Ville pour assurer leur cohérence et leur conformité avec les normes établies.

3.1.4 Formation

45 La sensibilisation et la formation sur la PRP sont essentielles pour garantir que les employés et employées comprennent leurs obligations et les pratiques de gestion des RP, conformément aux articles 63.3 et 63.6 de la *Loi sur l'accès*. La Ville a mis en place une capsule de sensibilisation en ligne intitulée « Respect de la vie privée et protection des renseignements personnels », obligatoire pour la plupart de ses employés et employées (environ 1 200). Le nouveau personnel doit obligatoirement suivre cette formation. À ce jour, 92 % des employés et employées l'ont suivie, mais celles et ceux qui n'ont pas d'adresse de courriel de la Ville, comme certains cols bleus, n'y ont pas eu accès. Aucune session en présentiel n'est prévue dans ce cas.

46 Le contenu de la capsule, qui aborde les notions de base de la *Loi sur l'accès*, ne mentionne rien concernant les ententes, la biométrie, les procédés de destruction et de conservation, les obligations des tiers détenant des RP de la Ville, ni les droits des personnes concernées.

47 En outre, son contenu présente parfois des incohérences avec les politiques et procédures de la Ville, notamment en ce qui concerne certains rôles et responsabilités ainsi que les étapes à suivre en cas d'incident de confidentialité. De plus, il n'est pas suffisamment adapté aux politiques et procédures spécifiques de la Ville.

48 La Ville a également créé une page intranet consacrée à la PRP, mais les politiques et procédures n'y sont pas publiées. De plus, les répondants et répondantes n'ont pas reçu de formation spécifique sur l'EFVP, bien qu'ils soient tenus de contribuer à cet aspect selon la Politique de gouvernance en matière de protection des RP. Enfin, lorsqu'il y a un changement de répondant ou répondante dans un service, aucune formation n'est offerte à la recrue.

49 Par ailleurs, on constate que la communication des informations par les répondants et répondantes n'est pas uniforme au sein des services de la Ville, ce qui souligne le besoin de leur fournir de meilleurs outils de communication et de contenu sur certains aspects de la *Loi sur l'accès*. De plus, la Ville devrait organiser plus de sessions de sensibilisation obligatoires pour son personnel.

50 Les répondantes et répondants eux-mêmes ne sont pas uniformément informés des enjeux et des avancées en matière de PRP au sein de la Ville, car le RPRP n'organise pas de réunions ni n'effectue de communications régulières avec eux. Cela limite la transmission efficace d'informations et de sensibilisation, et entrave le développement de l'autonomie des répondants et répondantes.

RECOMMANDATIONS À LA VILLE DE SHERBROOKE

15. Adapter le contenu de la capsule de sensibilisation pour qu'il concorde avec les politiques et procédures en vigueur de la Ville. Fournir des détails supplémentaires sur les actions à entreprendre en cas d'incident, en précisant les rôles de chacun et chacune au sein de la Ville. Organiser des formations en présentiel pour le personnel qui n'a pas suivi la capsule de sensibilisation en ligne.

16. Mettre à disposition de tout le personnel un deuxième module de formation sur la PRP afin de couvrir des aspects plus détaillés de la *Loi sur l'accès.* Ce module pourrait aborder des sujets tels que l'EFVP, les ententes, les procédures de destruction et de conservation, les obligations des tiers détenant des RP de la Ville, les droits des personnes concernées, la biométrie, les incidents de confidentialité, etc.

17. Mettre en place un système de rappels périodiques par courriel pour fournir régulièrement des conseils sur la PRP, rappeler les procédures en cas d'incident, informer sur les mises à jour réglementaires et transmettre des exemples de bonnes pratiques en matière de sécurité des RP.

18. Renforcer la formation des répondants et répondantes pour accroître leur autonomie et leur contribution aux activités liées à la *Loi sur l'accès* et veiller à ce que toutes les recrues soient formées. Les former spécifiquement sur les EFVP pour qu'elles puissent pleinement remplir leur rôle selon la Politique de gouvernance en matière de RP. Organiser des communications régulières et des rencontres avec les répondants et répondantes pour favoriser leur développement et transmettre les informations de manière uniforme.

19. Encourager les répondants et répondantes à offrir des formations au personnel de leur unité sur les obligations de la *Loi sur l'accès*. Mettre à leur disposition des outils de communication et du contenu sur les aspects de cette loi pour les accompagner.

20. Mettre à jour la page intranet consacrée à ce sujet en ajoutant les politiques et procédures de la Ville dans la section Documents de référence pour assurer la disponibilité et l'accessibilité de ces documents. Dans la section Formation de la Politique de gouvernance en matière de RP, supprimer les deux derniers paragraphes en doublon.

3.1.5 Évaluation des facteurs relatifs à la vie privée (EFVP)

51 Dans certaines situations impliquant des RP, un organisme public comme la Ville de Sherbrooke doit effectuer une EFVP. La CAI a identifié 5 situations obligatoires à ce sujet, détaillées à l'annexe 4 de ce rapport. Cette obligation vise à renforcer la protection du droit fondamental des citoyens et citoyennes à la vie privée, tel que protégé par la *Charte des droits et libertés de la personne*.

52 À ce jour, la Ville a réalisé trois EFVP, principalement pour répondre aux exigences des projets en cours. Cependant, toutes les situations nécessitant une EFVP n'ont pas encore été identifiées, et le RPRP ne voit aucun des RP communiqués à l'extérieur du Québec. Il nous a été indiqué qu'une liste des projets de la Ville sera établie pour déterminer ceux qui requièrent une EFVP.

53 De plus, la documentation relative aux EFVP n'est pas encore complète. Il manque notamment un modèle de rapport spécifique adapté aux besoins de chaque projet, la Ville utilisant actuellement le modèle fourni par la CAI. De même, une procédure détaillée encadrant les EFVP doit être élaborée, ce qui entrave la capacité des différents services de la Ville à mener efficacement ces évaluations. En ce qui concerne le formulaire d'analyse d'EFVP élaboré selon

le modèle de l'Union des municipalités du Québec, une uniformisation est nécessaire pour intégrer toutes les spécificités de la Ville.

54 Enfin, le processus relatif aux EFVP n'est pas encore opérationnel pour le personnel de la Ville, et aucune échéance n'a été définie pour mettre en œuvre les actions nécessaires.

RECOMMANDATIONS À LA VILLE DE SHERBROOKE
21. Identifier toutes les situations telles que les projets, programmes, initiatives et communications y compris celles qui se déroulent à l'extérieur du Québec, qui impliquent des RP et nécessitent une EFVP, conformément aux exigences précisées dans *la Loi sur l'accès.*
22. Établir des critères de priorisation des projets en fonction de leur envergure, de leur sensibilité et de leur impact potentiel sur la vie privée, afin de déterminer l'ordre de réalisation des EFVP.
23. Élaborer une procédure détaillant les étapes à suivre pour mener à bien une EFVP, en précisant les démarches nécessaires à chaque phase du processus, l'évaluation des risques et des mesures d'atténuation, les rôles et responsabilités des différentes parties prenantes ainsi qu'une révision périodique des EFVP pour les adapter aux évolutions légales et technologiques, et maintenir une protection adéquate de la vie privée.
24. Élaborer un modèle de formulaire et de rapport d'EFVP afin de standardiser le processus d'évaluation tout en favorisant son adaptation aux spécificités de chaque projet.

3.2 Collecte des renseignements personnels

55 La collecte est la première étape du cycle de vie du RP. Un dispositif doit être mis en place à cet effet pour garantir la PRP du personnel de la Ville et de la population.

3.2.1 Inventaire des renseignements personnels

56 La Ville de Sherbrooke, en tant qu'organisme public, est tenue d'établir et de maintenir un inventaire actualisé des fichiers contenant les RP détenus pour le compte de son personnel et de sa population. Cet inventaire est primordial pour assurer la conformité légale et protéger la vie privée des individus, conformément à l'article 76 de la *Loi sur l'accès*. Selon cet article, l'inventaire doit contenir les informations suivantes :

1. la désignation de chaque fichier, les catégories de renseignements qu'il contient, les fins auxquelles les renseignements sont conservés et le mode de gestion de chaque fichier;
2. la provenance des renseignements versés à chaque fichier;
3. les catégories de personnes concernées par les renseignements versés à chaque fichier;
4. les catégories de personnes qui ont accès à chaque fichier dans l'exercice de leurs fonctions;
5. les mesures de sécurité prises pour assurer la PRP.

57 Nous avons constaté que la Ville n'a pas encore commencé l'inventaire des RP collectés sur support papier ni de ceux répertoriés dans les fichiers Excel utilisés par ses différents services. De plus, il faudrait effectuer des mises à jour pour l'inventaire des RP collectés de manière numérique, notamment ceux obtenus via les applications, les sites Web et les courriels, en vue de refléter leur état actuel. Des lacunes et des incohérences ont également été décelées lors de l'analyse de l'inventaire des RP collectés via des logiciels. À titre d'exemple :

- certains champs de l'inventaire des RP sont laissés vides, tels que la durée de conservation, l'accès/transfert, la provenance, la liste des identifiants et le nombre de personnes impliquées;
- l'inventaire ne comprend pas certaines informations essentielles exigées par la *Loi sur l'accès*, telles que les catégories de renseignements, les fins de conservation, le mode de gestion, la provenance des données, les personnes concernées et celles y ayant accès, ainsi que la durée estimée de conservation des données.

58 De manière préoccupante, aucun processus n'a encore été instauré par la Ville pour garantir que toutes les informations relatives aux RP sont correctement collectées et conservées. Cela souligne l'urgence d'établir des directives claires pour assurer la conformité aux exigences légales et une PRP adéquate.

RECOMMANDATIONS À LA VILLE DE SHERBROOKE
25. Réaliser un inventaire exhaustif des RP collectés sur support papier et via les fichiers Excel, en conformité avec les directives de l'article 76 de la *Loi sur l'accès*.
26. Mettre à jour l'inventaire des RP collectés à travers les applications, les sites Web et les courriels, et corriger les éventuelles incohérences dans l'inventaire des RP collectés via les logiciels.
27. Établir un processus robuste pour garantir la collecte et la conservation complètes des RP de la Ville, en assurant leur conformité aux normes légales et une protection adéquate des données.

3.2.2 Mesures biométriques

59 Lorsque la Ville souhaite utiliser la biométrie, elle a l'obligation de divulguer à la CAI qu'elle compte :

- vérifier ou confirmer l'identité au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques;
- créer une banque de caractéristiques ou de mesures biométriques – dans ce cas, la divulgation doit être faite au moins 60 jours avant la mise en service de la banque.

60 À ce jour, le seul service identifié comme utilisant une banque de caractéristiques ou de mesures biométriques dans le cadre de son activité est le SPS de la Ville, qui effectue des analyses d'ADN et du bertillonnage. Cependant, l'utilisation de ces mesures biométriques par le SPS pour vérifier ou confirmer l'identité d'une personne n'a pas été divulguée à la CAI, qui l'a approuvée.

61 De plus, aucun processus n'a été mis en place par la Ville pour cibler ou planifier l'utilisation d'une banque de caractéristiques ou de mesures biométriques par les autres services de la Ville ou pour avoir accès à cette information.

RECOMMANDATIONS À LA VILLE DE SHERBROOKE
28. Recenser auprès des différents services de la Ville, à l'exception du SPS : ○ les personnes qui collectent, utilisent ou partagent une banque de caractéristiques ou des mesures biométriques, conformément aux cas identifiés par la CAI. ○ les personnes qui prévoient l'utilisation d'une banque de caractéristiques ou des mesures biométriques. Pour ces cas, effectuer une EFVP préalablement à la mise en place de cette banque.
29. Soumettre à la CAI une déclaration relative aux mesures biométriques utilisées par le SPS dans le cadre de son activité en remplissant le formulaire de *Déclaration d'un système biométrique ou procédé permettant de saisir des caractéristiques ou des mesures biométriques* mis à la disposition des organismes publics par la CAI.
30. Informer les individus de la collecte et de l'utilisation de leurs données biométriques, et obtenir leur consentement au préalable. Le consentement doit être clair, précis et s'appliquer à toutes les activités pour lesquelles les données biométriques sont recueillies. Il peut être collecté en utilisant le formulaire de *Consentement à la collecte, à l'utilisation et à la conservation de renseignements biométriques* fourni par la CAI. De plus, mettre en place une solution de rechange à la collecte de données biométriques en cas de refus de consentement, et donner la possibilité de retirer le consentement à tout moment.
31. Mettre en place des mesures de sécurité robustes pour protéger les données biométriques, telles que le cryptage, l'accès restreint et la surveillance continue. En cas de violation des données biométriques, en informer les individus concernés et la CAI dans les délais prescrits.

3.3 Consentement des personnes concernées

62 Les RP sont confidentiels, et leur confidentialité est garantie par le droit à la vie privée, qui donne aux individus le contrôle sur l'utilisation et la circulation de leurs informations. C'est pourquoi le consentement revêt une importance capitale dans la *Loi sur l'accès*.

63 À la Ville, la Politique de gouvernance en matière de RP établit les critères de nécessité et de validité des consentements. Cependant, elle ne précise pas suffisamment les rôles et responsabilités associés à leur rédaction ni le contenu attendu des libellés de consentement, et n'implique pas un processus de mise à jour régulière de ces consentements. De plus, la Politique ne couvre pas les règles particulières applicables aux consentements des mineurs de moins de 14 ans ni aux utilisations des technologies de biométrie.

64 Bien qu'un inventaire des consentements existants ait été lancé fin 2023, il a été interrompu, ce qui signifie que la Ville n'a pas de vue d'ensemble des consentements en vigueur à ce jour, ce qui compromet la vérification de leur conformité à la *Loi sur l'accès*. De plus, il n'y a pas eu d'harmonisation des libellés de consentement.

65 En dehors des consentements existants, la Ville n'a pas dressé d'inventaire de toutes les situations de collecte de RP se faisant sans consentement, sauf pour les exceptions prévues par la *Loi sur l'accès*, pour lesquelles un consentement doit être obtenu. Par conséquent, elle n'a pas de vision exhaustive des consentements manquants.

66 Il est impératif que la Ville finalise son inventaire des RP collectés et des fins auxquelles ces RP sont utilisés afin de garantir que les consentements sont complets et appropriés.

RECOMMANDATIONS À LA VILLE DE SHERBROOKE
32. Intégrer à la Politique sur la gouvernance en matière de protection des RP des règles précises concernant le consentement des mineurs de moins de 14 ans, ainsi que des directives relatives à l'utilisation des technologies de biométrie.
33. Élaborer des libellés génériques de consentement et développer une procédure spécifique sur la rédaction des consentements, précisant les attentes en termes de contenu, les situations où les consentements sont requis par la ***Loi sur l'accès*** ainsi que les rôles et responsabilités associés à leur rédaction et à leur validation, avec un processus de mise à jour en cas de nouvelles utilisations ou de communication de ces RP.
34. Identifier toutes les situations existantes nécessitant un consentement, conformément aux exigences légales, vérifier la présence de consentements valides et finaliser l'inventaire des RP de la Ville pour garantir l'exhaustivité et l'adéquation des consentements.
35. Définir une fréquence de révision obligatoire à des intervalles précis de la Politique de confidentialité de la Ville dans la section « Disposition finale ».

3.4 Communication de renseignements personnels

67 Un cadre formel et à jour est indispensable à la communication de RP sans le consentement des personnes concernées. La Politique sur la gouvernance en matière de protection des RP aborde partiellement les cas autorisés de communication sans consentement ainsi que les exigences légales à respecter avant certaines communications sans consentement. Cependant, elle ne couvre pas les situations où la communication se fait sans le consentement de la personne concernée, telles que mentionnées aux articles 59, 59.1, 60, 60.1 et 68 de la *Loi sur l'accès*.

68 En plus des constats précédents, d'autres lacunes ont été relevées, qui nécessitent des corrections :

- La Ville n'a pas établi de directive par la plus haute autorité, conforme aux communications sans consentement mentionnées dans l'article 59.1 (en vue de prévenir un acte de violence);
- Il n'existe pas de processus de mise à jour et de vérification régulières des registres de communication des RP sans consentement;

- Aucun processus n'a été mis en place pour identifier toutes les situations nécessitant une communication sans consentement et requérant la mise en place des exigences prévues par la *Loi sur l'accès*;
- Le RPRP n'a pas accès aux registres et aux ententes liés à la gestion des RP tenus par le SPS de la Ville, or ces éléments devraient être placés sous sa supervision, conformément à la *Loi sur l'accès*.

69 Par ailleurs, pour assurer un encadrement complet de la communication sans consentement, des procédures particulières concernant les EFVP et les ententes de communication doivent être mises en place.

RECOMMANDATIONS À LA VILLE DE SHERBROOKE
36. Élaborer une procédure pour la mise à jour et la révision régulières des différents registres de communication, ainsi qu'un processus d'identification à fréquence adéquate des situations dans lesquelles une communication se fait sans consentement et qui nécessiterait le respect des exigences prévues par la *Loi sur l'accès.*
37. Intégrer dans la Politique de gouvernance en matière de RP les exigences en cas de communication sans le consentement de la personne concernée, conformément aux articles 59, 59,1, 60, 60.1 et 68 de la *Loi sur l'accès* afin d'assurer l'exhaustivité de la politique sur les exceptions de consentement que la loi prévoit.
38. Conformément à l'article 59.1, établir une directive par la mairesse, en tant que plus haute autorité, concernant les communications sans consentement relatives aux cas prévus dans cet article.
39. Assurer une meilleure supervision par le RPRP des registres et des ententes liés aux communications de RP sans consentement effectuées par le SPS de la Ville.

3.5 Ententes

70 Afin de se conformer à la *Loi sur l'accès,* la Ville doit développer des ententes de communication de RP lorsqu'elle recueille des RP pour le compte d'un autre organisme public avec qui elle collabore ou lorsqu'elle communique des RP sans le consentement des personnes concernées, par exemple à des fins de recherche.

71 On note que l'entente en cours de validation avec Entreprendre Sherbrooke présente des lacunes par rapport aux exigences de l'article 64 de la *Loi sur l'accès*. En effet, elle ne définit pas clairement les moyens de collecte des RP, les mesures de protection ni la nature ou le type de RP collectés. Par ailleurs, et bien que cette entente ne soit pas encore en vigueur, elle n'a pas été enregistrée dans le registre prévu à l'article 67.3 de la loi.

72 On relève également que la Politique de gouvernance en matière de protection de RP aborde partiellement les cas nécessitant la mise en place d'ententes conformément à la *Loi sur l'accès.* De plus*,* la Ville ne dispose pas actuellement d'une procédure de rédaction des ententes pour toutes les situations prévues par la *Loi sur l'accès*, définissant les rôles et responsabilités associés et précisant la mise à jour du registre des ententes.

73 Par ailleurs, le RPRP envisage d'établir, en 2024, un inventaire des ententes qui ne sont pas sous sa responsabilité. Cependant, il n'a pas prévu à court terme de réaliser un inventaire des situations au sein de la Ville qui impliquent la mise en place d'une entente conformément aux cas prévus par la *Loi sur l'accès*. Il ne dispose donc pas d'une vue exhaustive des ententes existantes à la Ville.

RECOMMANDATIONS À LA VILLE DE SHERBROOKE
40. Intégrer dans la Politique de gouvernance en matière de protection de RP toutes les situations nécessitant la mise en place d'une entente conformément aux articles 64 et 68 de *Loi sur l'accès*, afin d'assurer une couverture exhaustive des situations qu'elle prévoit.
41. Mettre en place une procédure de rédaction des ententes pour toutes les situations prévues par la *Loi sur l'accès*, définissant les rôles et responsabilités liés à leur mise en place et à leur validation ainsi que la mise à jour du registre des ententes. Élaborer un gabarit d'entente afin de standardiser le processus.
42. Démarrer l'inventaire des ententes existantes auprès des différents services de la Ville afin de compléter le registre des ententes. Établir également une cartographie des situations actuelles dans lesquelles mettre en place une entente serait nécessaire, conformément aux exigences légales. Évaluer l'intérêt d'une contribution active des répondants et répondantes pour réaliser ces deux activités.

3.6 Conservation et destruction des renseignements personnels

74 En tant qu'organisme public, il incombe à la Ville de Sherbrooke de garantir une gestion sécuritaire des RP qu'elle détient, depuis leur collecte jusqu'à leur destruction. Lorsqu'elle n'a plus besoin d'utiliser ces RP pour les objectifs préalablement définis, il est impératif qu'elle les détruise de manière sécuritaire. Dans certaines situations, il est possible d'anonymiser ou de dépersonnaliser les RP, ce qui peut autoriser la Ville à les conserver tout en préservant la confidentialité des individus concernés.

75 Actuellement, la Ville n'a pas finalisé l'inventaire de ses RP (voir la section 3.2.1) et n'a donc pas encore mis en place des mesures de sécurité (voir la section 3.2) propres à assurer la sécurité et la conservation des RP.

76 En ce qui concerne la destruction des RP, la Ville n'a pas de procédure établie pour l'encadrer après leur utilisation. Cependant, une nouvelle procédure est en cours de développement et sera soumise au comité AIPRP en 2024. Cette procédure prévoit l'utilisation d'une déchiqueteuse pour les documents papier, mais pas l'incinération des documents classés très confidentiels, bien que ce soit recommandé par la CAI. De plus, elle ne s'applique pas aux tiers qui détruisent des RP de la Ville.

77 Les clauses administratives standards prévues dans les offres de services et contrats de la Ville ont été mises à jour pour renforcer la protection des RP détenus par des tiers. Cependant, ces nouvelles clauses n'ont pas été validées par le RPRP et ne comprennent pas la possibilité pour la Ville d'auditer l'ensemble des mesures de sécurité du prestataire. De plus, les contrats et offres de service avec des tiers, avec lesquels la Ville échange des RP, n'ont pas été mis à jour selon ces nouvelles clauses administratives propres à la PRP.

78 Quant au contrat actuel avec le prestataire de destruction de documents, nous relevons qu'il ne spécifie pas le processus utilisé pour la destruction ni ne prévoit que le prestataire doit informer la Ville s'il fait appel à un sous-traitant pour cette destruction, alors que ces mentions sont requises par la CAI dans les contrats de destruction impliquant un prestataire externe.

RECOMMANDATIONS À LA VILLE DE SHERBROOKE
43. Finaliser et approuver la procédure de destruction actuellement en développement. Inclure explicitement les tiers dans le champ d'application de cette procédure. Prévoir également l'incinération en plus du déchiquetage pour la destruction des documents très confidentiels.
44. Finaliser l'inventaire des RP conservés par la Ville afin d'assurer que son calendrier de conservation est à jour.
45. Intégrer, dans les nouvelles clauses administratives consacrées à la PRP, une clause d'audit plus étendue sur les mesures de sécurité en place chez le prestataire. Faire valider ces nouvelles clauses par le RPRP et le service juridique.
46. Lors du renouvellement des contrats et des offres de service avec des tiers, avec lesquels la Ville échange des RP, inclure de nouvelles clauses administratives consacrées à la PRP. Concernant celui du prestataire de destruction de documents, inclure la mention du procédé de destruction et prévoir que le prestataire informe la Ville en cas de sous-traitance pour la destruction, conformément aux exigences de la CAI.

3.7 Incidents de confidentialité et mesures de sécurité

79 De leur collecte à leur destruction, les RP doivent être rigoureusement protégés. Tout organisme public a le devoir de mettre en place des mesures de sécurité afin d'éviter les incidents de confidentialité pouvant porter atteinte à la vie privée des citoyens et citoyennes.

3.7.1 Incidents de confidentialité

80 L'encadrement des incidents de confidentialité garantit une gestion responsable des RP et renforce la confiance du personnel de la Ville et des citoyens et citoyennes.

81 Nous constatons que la Ville a élaboré une procédure relative à la gestion des incidents de confidentialité impliquant des RP. Cependant, cette procédure n'est pas publiée sur son site Web. De plus, des incohérences mineures ont été constatées concernant la responsabilité de la mise en œuvre de mesures préventives et correctives entre les différentes sections de la procédure de gestion des incidents et le logigramme correspondant.

82 Conformément à la *Loi sur l'accès*, la procédure exige que la CAI et la personne concernée soient avisées en cas d'incident de confidentialité présentant un risque sérieux de préjudice. Un registre des incidents de confidentialité a été créé par la Ville et est tenu à jour. En revanche, il

n'existe pas de processus pour assurer le suivi des incidents signalés et la mise en œuvre des actions correctives.

83 De même, l'implication des répondants et répondantes dans la gestion des incidents de confidentialité varie d'un service à l'autre. Dans un service, il a été constaté que le répondant n'est pas toujours informé de tous les incidents de confidentialité, alors que la Politique de gouvernance en matière de RP stipule explicitement qu'il doit l'être.

RECOMMANDATIONS À LA VILLE DE SHERBROOKE
47. Corriger les incohérences mineures concernant certains rôles et responsabilités entre les différentes sections de la procédure de gestion des incidents et le logigramme correspondant. Intégrer dans la procédure une grille d'évaluation du préjudice sous forme de questionnaire.
48. Effectuer un rappel aux répondants et répondantes concernant leurs rôles et responsabilités dans la gestion des incidents de confidentialité. S'assurer que chaque répondant ou répondante en est informé et est impliqué dans la déclaration et l'analyse des incidents de confidentialité.

3.7.2 Mesures de sécurité

84 La mise en place de mesures de sécurité adéquates est obligatoire et essentielle pour garantir la protection des RP collectés, utilisés, communiqués, conservés ou détruits. Cette obligation est définie par l'article 63.1 de *la Loi sur l'accès*, qui stipule la nécessité d'établir des mesures de sécurité raisonnables, tenant compte de la sensibilité des données, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support.

85 Actuellement, la Ville ne dispose pas d'une matrice de contrôles ni d'une liste de mesures raisonnables pour la PRP. De plus, aucune échéance n'a été fixée pour la mise en place de ces mesures. L'absence d'un tel dispositif rend difficile la vérification de la corrélation entre ces contrôles/mesures et l'analyse approfondie des risques liés aux RP, en prenant en considération leur sensibilité, leur utilisation, leur volume, leur répartition et leur format.

86 À la suite de nos échanges avec le RPRP, il est prévu que ces mesures de sécurité soient mises en place une fois finalisé le processus relatif à la collecte des RP.

RECOMMANDATIONS À LA VILLE DE SHERBROOKE
49. Effectuer une évaluation des risques associés aux RP traités afin de déceler les vulnérabilités et mettre en place des mesures de sécurité adéquates.
50. Limiter l'accès aux RP aux seuls employés et employées autorisés en utilisant des contrôles d'accès, des mots de passe robustes à changer régulièrement et des niveaux d'autorisation appropriés. Crypter les données sensibles pour les protéger contre tout accès non autorisé.
51. Vérifier que les contrôles/mesures mis en place sont basés sur une analyse approfondie des risques liés aux RP, en prenant en compte leur sensibilité, la finalité de leur utilisation, leur volume, leur répartition et leur format.

3.8 Analyse de risques

87 La Ville devrait dresser une liste des risques, effectuer et documenter une analyse des risques et des coûts afin de prioriser et de confirmer les mesures de protection à mettre en place pour la gestion des RP. Cependant, nous constatons :

- qu'aucune analyse des risques par rapport aux coûts n'a été effectuée pour prioriser et valider les mesures de protection à mettre en place pour la gestion des RP;
- qu'il n'existe pas de plan de priorisation des mesures de protection pour la gestion des RP, plan découlant de cette analyse. Le plan d'action de la Ville dans le cadre du Projet PRP, comprenant les actions à mettre en œuvre, n'est pas encore finalisé.

RECOMMANDATIONS À LA VILLE DE SHERBROOKE
52. Effectuer et documenter une analyse de risques et des coûts afin de prioriser et de confirmer les mesures de protection à mettre en place pour la gestion des RP.
53. Finaliser le plan d'action Projet PRP précisant la stratégie retenue, le plan opérationnel et la priorisation des mesures de protection, et définir des indicateurs de réussite pour effectuer un suivi optimal. Définir également des échéanciers clairs pour la mise en œuvre de toutes les actions requises pour la mise en conformité de la Ville avec la *Loi sur l'accès*.

3.9 Reddition de comptes

88 La reddition de comptes joue un rôle important au sein de la gouvernance en visant à assurer que les actions entreprises sont conformes aux décisions prises et que les résultats escomptés sont atteints. Au sein de la Ville, plusieurs lacunes ont été décelées :

- Aucun rapport ni indicateur ne porte sur les activités de la Ville en lien avec la *Loi sur l'accès*;
- L'absence de ces rapports et indicateurs rend difficile l'assurance d'une prise de décision en temps opportun;
- Les actions et activités ne font pas encore l'objet d'une reddition de comptes régulière et pertinente.

RECOMMANDATION À LA VILLE DE SHERBROOKE
54. Élaborer des rapports et/ou indicateurs relatifs aux actions et activités de la Ville en lien avec *la Loi sur l'accès* afin de pouvoir réaliser des redditions de comptes.

4. COMMENTAIRES DE L'ADMINISTRATION

Le Service du greffe de la Ville de Sherbrooke a pris acte des constats et des recommandations du vérificateur général dans son rapport portant sur la gestion de la protection des renseignements personnels à la Ville de Sherbrooke.

Le Service du greffe, à titre de service responsable de la protection des renseignements personnels, accueille favorablement les recommandations du vérificateur général, celles-ci étant cohérentes avec les obligations légales et les bonnes pratiques en matière de protection des renseignements personnels. Ces recommandations représentent pour la Ville un levier afin d'améliorer ses pratiques.

La Ville accorde une très grande importance à la protection des renseignements personnels en sa possession. Comme en fait état le rapport du vérificateur général, la Ville a mis en place plusieurs actions pour respecter ses obligations légales et certaines sont encore en cours d'implantation.

Toutefois, comme le démontre le présent rapport, la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (LQ 2021, c. 25) a ajouté de nombreuses responsabilités à la Ville de Sherbrooke. Au-delà de l'adoption de différentes politiques, procédures et guides, une gestion continue de ce dossier devra être réalisée. Qu'on parle de la gestion des incidents de confidentialité, de la réalisation d'évaluations des facteurs relatifs à la vie privée, de la mise en place d'une formation adéquate ou encore de la gestion des plaintes, il est indéniable que des ressources supplémentaires doivent être affectées au dossier de la protection des renseignements personnels. En effet, le Service du greffe ne possède actuellement pas les ressources nécessaires pour mettre en œuvre l'ensemble des recommandations du vérificateur général.

Pour mener à bien ce dossier, il est nécessaire de retenir les services d'une personne qui verra à s'assurer de la mise en place des principes de conformité, de gouvernance, des politiques et des procédures reliées à la protection des renseignements personnels. Elle devra veiller à leur mise en œuvre, à leur coordination et à leur amélioration continue, tout en s'assurant du respect des obligations légales et des orientations retenues par la Ville.

La Ville intégrera donc les recommandations du vérificateur général dans son plan d'action visant l'amélioration continue de la protection des renseignements personnels afin que l'ensemble des renseignements personnels en sa possession soit bien protégé. Sa mise en œuvre et son succès dépendront des ressources que la Ville y consacrera.

ANNEXE 1
Exigences légales et réglementaires auxquelles la Ville est assujettie

Ci-après les lois (liste non exhaustive) qui contiennent des particularités en matière de protection des RP.

- *Loi sur la protection des renseignements personnels dans le secteur privé*, qui s'applique aux organisations du secteur privé (entreprises et organismes à but non lucratif)
- *Code civil* (RLRQ, c. CCQ-1991)
- *Loi sur les archives* (RLRQ, c. A-21.1) ;
- *Loi concernant le cadre juridique des technologies de l'information* (RLRQ, c. C-1.1)
- *Code des professions* (RLRQ, c. C-26)
- *Loi sur l'administration fiscale* (RLRQ, c. A-6.002)
- *Code de la sécurité routière* (RLRQ, c. C-24.2)
- *Loi sur la protection de la jeunesse* (RLRQ, c. P-34.1) ;
- *Loi sur les services de santé et les services sociaux* (RLRQ, c. S-4.2)
- *Loi sur l'assurance maladie* (RLRQ, c. A-29)
- *Loi sur le ministère de la Santé et des Services sociaux* (RLRQ, c. M-19.2)
- *Loi sur l'Institut de la statistique du Québec* (RLRQ, c. I-13.011)
- *Loi sur la santé publique* (RLRQ, c. S-2.2)
- *Loi sur la santé et de la sécurité du travail* (RLRQ, c. S-2.1)
- *Loi sur la Société de l'assurance automobile du Québec* (RLRQ, c. S-11.011)
- *Charte des droits et libertés de la personne* (RLRQ, c. C-12)
- *Loi sur la Régie du logement* (RLRQ, c. R-8.1)
- *Loi sur l'enseignement privé* (RLRQ, c. E-9.1)
- *Loi sur la sécurité privée* (RLRQ, c. S-3.5)
- *Loi sur le Barreau* (RLRQ, c. B-1)
- *Loi sur le notariat* (RLRQ, c. N-3)
- *Loi sur les assureurs* (RLRQ, c. A-32.1)

ANNEXE 2
Objectifs de l'audit et critères d'évaluation

Objectif 1

La Ville a pris, en temps opportun, les mesures nécessaires pour respecter les exigences de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.*

Critères d'évaluation

1. Un ou une responsable de la protection des renseignements personnels (RPRP) a été nommé.
    - Son rôle et ses responsabilités sont définis;
    - Les employés et employées de la Ville savent qu'ils peuvent s'y référer au besoin;
    - La Commission d'accès à l'information (CAI) est avisée par écrit de son identité et dispose de ses coordonnées, de sa date d'entrée en fonction et de tout changement concernant ce ou cette responsable.

2. Un comité sur la protection des renseignements personnels a été formé.
    - Le mandat du comité a été défini et approuvé par les autorités compétentes.
    - Le comité est minimalement composé :
        - du ou de la RPRP ou de la personne responsable de l'accès aux documents (RAD) (si applicable) et du ou de la responsable de la protection des RP;
        - du ou de la responsable de la sécurité de l'information, le cas échéant;
        - du ou de la responsable de la gestion documentaire, le cas échéant;
        - de toute personne dont l'expertise est requise.
    - Un calendrier de rencontres est établi et respecté.
    - Un ordre du jour standard a été établi et comprend minimalement les points suivants :
        - Statut sur l'inventaire et/ou la cartographie des RP;
        - Incidents de confidentialité;
        - Évaluation des facteurs relatifs à la vie privée;
        - Projets d'acquisition de logiciels et de systèmes impliquant des RP;
        - Traitement automatisé induisant des RP;
        - Données biométriques utilisant des RP;
        - Règles (modifications, ajouts, retraits, etc.) relatives aux RP;
        - Communication des RP;
        - Protection de la vie privée dès la conception.
    - Des comptes rendus/procès-verbaux sont rédigés, approuvés par les autorités compétentes et conservés par la personne désignée à cet effet.

3. Un processus et/ou une procédure encadrant la gestion des incidents de confidentialité ont été formellement définis. Ce document inclut l'obligation d'aviser la CAI et la personne concernée de

tout incident de confidentialité impliquant un renseignement personnel et qui présente un risque sérieux de préjudice. Un registre des incidents est également créé et tenu à jour.

4. Un encadrement formel a été mis en place (et est mis à jour), au besoin, en ce qui concerne la communication de RP sans le consentement de la personne concernée.

5. Si la Ville utilise, ou prévoit utiliser, une banque de caractéristiques ou de mesures biométriques, elle a présenté le tout à la CAI au moins 60 jours avant sa mise en service. Si la Ville utilise, vérifie ou confirme l'identité d'une intervenante ou d'un intervenant au moyen de caractéristiques ou de mesures biométriques, les mesures d'encadrement ont été divulguées à la CAI.

6. Les politiques, directives et pratiques encadrant la gouvernance des RP ont été développées, approuvées par les autorités compétentes et sont publiées sur le site Web de la Ville, lorsque c'était requis. Ces documents traitent, sans s'y limiter, la gestion des plaintes, la confidentialité, la désindexation, le deuil, le droit à la portabilité, le sondage et la sécurité des TI.

7. La Ville a développé la documentation portant sur l'évaluation des facteurs relatifs à la vie privée (EFVP).

8. La Ville a créé les libellés de consentement requis, les critères de nécessité et de validité, et en fait usage.

9. De la formation et/ou des activités de sensibilisation à la PRP ont été offertes par la Ville à son personnel.

10. Les actions et activités de la Ville en ce qui a trait au respect de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* font l'objet d'une reddition de comptes régulière et pertinente, et favorisent la prise de décision en temps opportun.

11. La Ville a développé des ententes de communication des RP lorsqu'elle en recueille pour le compte d'un autre organisme public avec qui elle collabore ou lorsqu'elle communique des RP sans le consentement des personnes concernées, par exemple à des fins de recherche.

12. La Ville a élaboré et mis en œuvre des règles de gouvernance encadrant la destruction ou l'anonymisation des RP après leur utilisation.

Objectif 2

La Ville a pris les mesures nécessaires pour identifier et documenter les RP qu'elle détient ou est amenée à détenir, et elle s'appuie sur une analyse des risques et des coûts pour déterminer les mesures de protection à mettre en place.

Critères d'évaluation

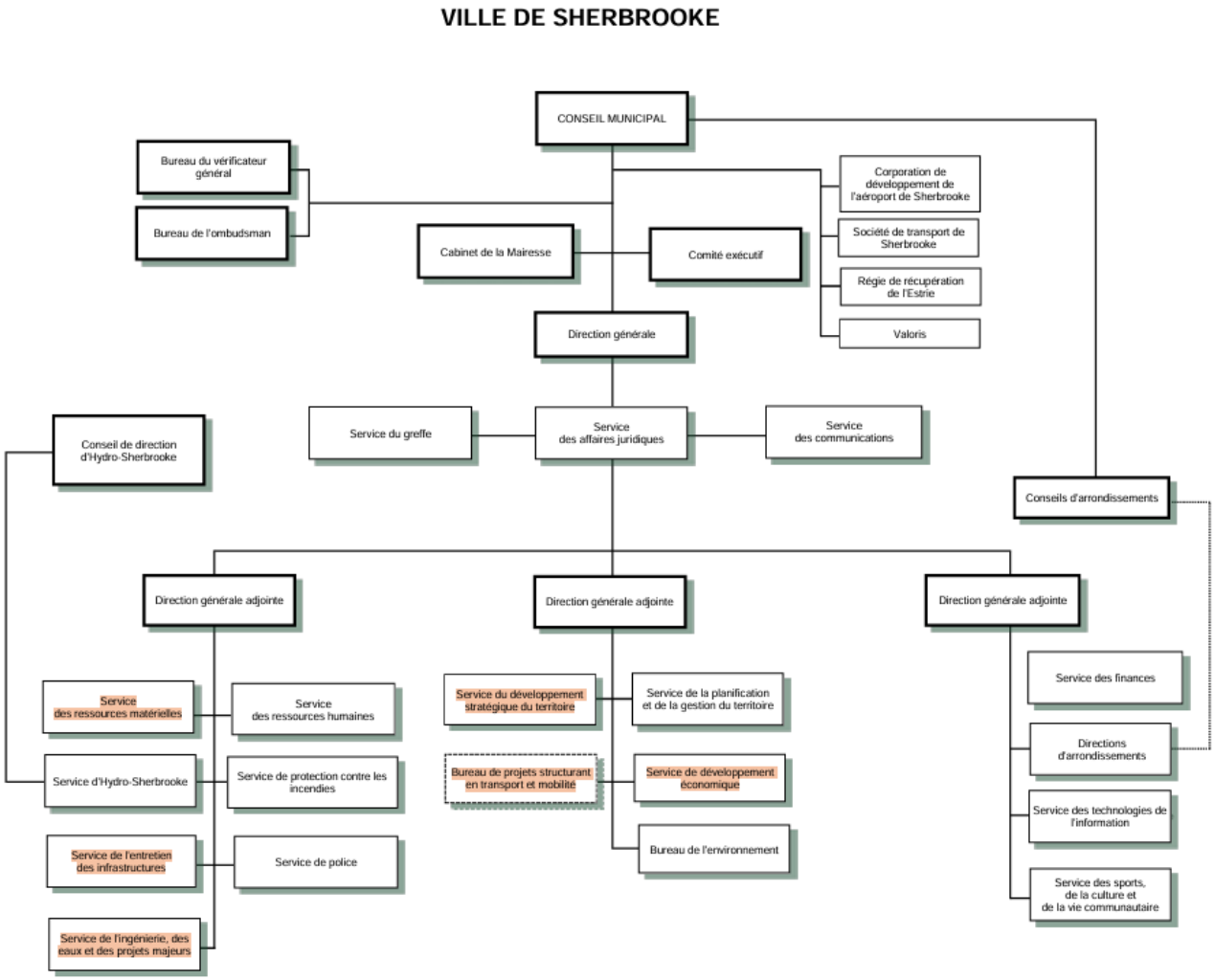
1. La Ville a dressé l'inventaire des RP (sur support numérique ou papier) et des différentes sources d'information incluant ce qui est imparti (s'assurer d'identifier tous les systèmes dans lesquels sont collectés/stockés des RP), ainsi :
   a. tous les RP collectés, utilisés et stockés ont été identifiés et consignés dans un registre prévu à cette fin;
   b. l'usage qui est fait de tous les RP est connu et consigné dans un registre prévu à cette fin;

c. les supports de stockage des RP sont connus et consignés dans un registre prévu à cette fin;
d. les détenteurs de RP sont identifiés et consignés dans un registre prévu à cette fin.

2. La Ville a déterminé les contrôles en place et les mesures raisonnables de protection à mettre en place sur les RP collectés, utilisés, communiqués, stockés ou détruits afin de mitiger les risques identifiés compte tenu de la sensibilité des RP, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support.

3. En prenant en compte les exigences légales et réglementaires, la Ville a effectué et documenté une analyse des risques et des coûts, et les a listés afin de déterminer et de prioriser les mesures de protection à mettre en place pour gérer les RP.

ANNEXE 3
Organigramme de la Ville de Sherbrooke



Note : Les services en surbrillance ont été créés ou restructurés en 2024.

ANNEXE 4
Situations d'EFVP obligatoires

Extrait du site Web de la CAI[10], qui définit les cinq situations prévues par la Loi sur l'accès *dans lesquelles les EFVP sont obligatoires.*

1. Communication de renseignements personnels sans consentement à un tiers à des fins d'étude, de recherche ou de production de statistiques

La communication de renseignements personnels sans le consentement des personnes concernées à une personne ou à un organisme souhaitant utiliser ces renseignements à des fins d'étude, de recherche ou de production de statistiques est permise seulement si une EFVP conclut au respect de certains critères.

La communication doit être faite dans le cadre d'une entente écrite, transmise à la Commission. Cette entente entre en vigueur dans les 30 jours suivant sa réception.

2. Projet d'acquisition, de développement ou de refonte de système d'information ou de prestation électronique de services

Une EFVP est requise pour tout projet lié à un système d'information ou de prestation électronique de services impliquant des renseignements personnels. Il peut s'agir d'un projet d'acquisition, de développement ou de refonte. Dès le début d'un tel projet, aux fins de l'EFVP, l'organisme doit consulter son comité sur l'accès à l'information et la protection des renseignements personnels.

Un système d'information peut revêtir de multiples formes. Il n'est pas nécessairement informatisé, quoique cela soit fréquent. Il peut s'agir entre autres d'un :

- Système informatique de traitement des dossiers;
- Logiciel de vidéoconférence ou de collaboration;
- Système biométrique;
- Système d'intelligence artificielle;
- Système de cartes à puce/RFID;
- Système de vidéosurveillance;
- Système statistique;
- Système de gestion de la paie.

Un système de prestation électronique de services peut notamment prendre la forme :

- D'une borne libre-service;
- D'un service de paiement par RFID/NFC;
- D'une zone membre d'un site Web;
- D'un dossier électronique;
- D'une application mobile.

[10] Commission d'accès à l'information du Québec. (2024). *Guide d'accompagnement à la démarche et à sa documentation : Réaliser une évaluation des facteurs relatifs à la vie privée*, p. 12. https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_GU_EFVP.pdf

3. Communication d'un renseignement personnel à l'extérieur du Québec

Votre organisme doit procéder à une EFVP avant de :

- Communiquer un renseignement personnel à une entité située à l'extérieur du Québec;
- Confier à une personne ou à un organisme à l'extérieur du Québec la tâche de recueillir, d'utiliser, de communiquer ou de conserver, pour votre compte, un tel renseignement.

4. Collecte pour le compte d'un autre organisme

Un organisme public peut recueillir des renseignements personnels nécessaires à l'exercice des attributions d'un autre organisme public. Il peut également le faire en vue de la mise en œuvre d'un programme d'un organisme public avec lequel il collabore pour la prestation de services ou pour la réalisation d'une mission commune.

- Par exemple, un organisme peut recueillir un renseignement personnel afin de vérifier l'admissibilité de personnes à un programme qu'il administre.

Les organismes qui collaborent doivent conclure une entente et la transmettre à la Commission.

5. Autres communications de renseignements personnels sans consentement dans le cadre d'une entente

Plus précisément, une EFVP doit aussi être réalisée avant de communiquer un renseignement personnel sans consentement :

- À un organisme public ou à un organisme d'un autre gouvernement lorsque la communication est manifestement au bénéfice de la personne concernée;
- À un organisme public ou à un organisme d'un autre gouvernement pour l'exercice de ses attributions ou la mise en œuvre d'un programme dont il a la gestion;
- À une personne ou à un organisme lorsque des circonstances exceptionnelles le justifient;
- À une personne ou à un organisme si cette communication est nécessaire dans le cadre de la prestation d'un service à rendre à la personne concernée par un organisme public, notamment aux fins de l'identification de cette personne.

La communication doit être faite dans le cadre d'une entente écrite transmise à la Commission. Cette entente entre en vigueur dans les 30 jours suivant sa réception. 4. Audit – Rémunération des él