RÉFORME DE LA LOI SUR L'ACCÈS
(PROTECTION DES RENSEIGNEMENTS PERSONNELS)

GUIDE D'APPLICATION POUR LES MUNICIPALITÉS

MESURES ENTRANT EN VIGUEUR
AUX 22 SEPTEMBRE 2023 ET 2024

UMQ

La voix des GOUVERNEMENTS de proximité

Guide préparé par :
Fasken
Me Antoine Aylwin
Me Iara Griffith
Me Soleica Monnier
Me Julie Uzan-Naulin

Représentants de l'Union des municipalités du Québec :
Me Joanne Loyer
Me Jason Prévost
Me Noémie Ladouceur-Fournelle

Crédits photos :
Shutterstock

Conception et infographie :
Robert Devost Graphiste Inc

Avertissement:
Ce document ne remplace ni ne synthétise la législation et la réglementation adoptées ni la littérature dans ce domaine.

TABLE DES MATIÈRES

INTRODUCTION

Depuis plus de cent ans, l'Union des municipalités du Québec (« UMQ ») représente des municipalités de toute taille partout au Québec. L'UMQ travaille fort pour s'assurer que ses membres soient les mieux informés quant aux changements qui touchent le milieu municipal. C'est pourquoi elle a préparé le deuxième volet de ce Guide.

Alors que le progrès technologique sous-tend des risques accrus en matière de cybersécurité et de vie privée, la protection des renseignements personnels suscite un intérêt croissant. En 2018, l'Union européenne a adopté le Règlement général sur la protection des données (le « RGPD »), lequel encadre d'une main de fer le traitement des données à caractère personnel des résidents européens et a initié une vague de réformes à l'échelle internationale. Suivant cette tendance, le Québec – première province canadienne à le faire – a adopté le projet de loi n° 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, devenu la Loi 25[1]. Celle-ci apporte notamment d'importantes modifications à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (la « Loi sur l'accès[2] ») et à la Loi sur la protection des renseignements personnels dans le secteur privé .

Entrant progressivement en vigueur entre 2022 et 2024, la Loi 25 définit le rôle et les fonctions du responsable de la protection des renseignements personnels au sein d'un organisme public, comme une municipalité. Cette loi vise à offrir un meilleur contrôle aux citoyens quant à leurs renseignements personnels et à responsabiliser davantage les organisations dans leur gestion de ces renseignements. Elle impose aussi le signalement de certains incidents de confidentialité, la tenue d'évaluation des facteurs relatifs à la vie privée, la mise en place de pratiques de gouvernance et de politiques de confidentialité en langage clair, des droits accrus pour les particuliers et d'importantes sanctions en cas de non-respect de ses dispositions par les organismes publics. En somme, elle modernise le cadre législatif pour l'adapter à la réalité technologique d'aujourd'hui.

Ce Guide fait suite au précédent volet présentant les dispositions entrées en vigueur le 22 septembre 2022. Le premier volet s'attache plus particulièrement à expliquer les nouvelles fonctions du Responsable de la protection des renseignements personnels, le rôle du Comité sur l'accès à l'information et la protection des renseignements personnels, les obligations en matière d'incidents de confidentialité ainsi que les communications de ces renseignements, sans le consentement, à des fins de recherche, d'étude ou de production de statistiques.

Ce second volet présente, quant à lui, les obligations entrant en vigueur les 22 septembre 2023 et 2024.

Les changements annoncés comportent leur lot de défis et l'UMQ tient à accompagner les municipalités dans leur mise en application.

2021 À 2024

2021

Adoption et sanction du PL 64

2022

- Rôle et responsabilités de la personne ayant la plus haute autorité et fonctions de responsable.
- Mise en place d'un comité sur l'accès à l'information et la protection des renseignements personnels.
- Principe de responsabilité d'un organisme public.
- Signalement de certains incidents de confidentialité.
- Communication à des fins d'étude, de recherche ou de production de statistiques.
- Pouvoirs accrus de la Commission d'accès à l'information.

2023

- Adoption et diffusion des règles de gouvernance de la municipalité.
- Diffusion d'une politique de confidentialité en langage clair.
- Devoir d'assistance du responsable de la protection des renseignements personnels.
- Informations à fournir aux particuliers dans le cadre de la collecte de renseignements personnels et de décisions fondées sur un traitement automatisé.
- Critères de validité du consentement, notamment eu égard aux renseignements personnels sensibles.
- Acquisition, développement et refonte de système d'information ou de prestation électronique de services (Protection de la vie privée dès la conception).
- Protection par défaut pour les produits ou services technologiques offerts au public disposant de paramètres de confidentialité.
- Exigences de transparence dans le cadre de l'utilisation de technologies comprenant des fonctions d'identification, de localisation et de profilage.
- Collecte en collaboration avec un autre organisme.
- Utilisation des renseignements dépersonnalisés.
- Exigences pour une communication conforme à l'article 68 de la Loi sur l'accès.
- Exigences pour une communication à l'extérieur du Québec.
- Nouvelles exigences dans le cadre d'un mandat ou d'un contrat de services.
- Sanctions pénales.

2024

- Droit à la « portabilité ».

GLOSSAIRE

DES ABRÉVIATIONS UTILISÉES DANS LE GUIDE

CAI :	Commission d'accès à l'information du Québec
Comité :	Comité sur l'accès à l'information et la protection des renseignements personnels
ÉFVP :	Évaluation des facteurs relatifs à la vie privée
Loi sur l'accès :	*Loi concernant le cadre juridique des technologies de l'information*, RLRQ, c. C-1.1
Loi 25 :	*Projet de loi no 64 sanctionné, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (L.Q. 2021, c. 25)*
RAD :	Responsable de l'accès aux documents
RPRP :	Responsable de la protection des renseignements personnels
SRIDAIL :	Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité
UMQ :	Union des municipalités du Québec

Portée - Modification à la définition de « renseignement personnel »

Le présent Guide vise à fournir des lignes directrices pour outiller les municipalités dans leur conformité à la Loi 25 au regard des renseignements personnels qu'elles détiennent, que leur conservation soit assurée par elles-mêmes ou par un tiers, pour son compte (ex. un fournisseur de services).

La définition de « renseignement personnel », ainsi que les règles de protection qui s'y appliquent, seront changées à partir de septembre 2023. En effet,

> **le « renseignement personnel » visera expressément tout « renseignement qui concerne une personne physique et permet, directement ou indirectement, de l'identifier[4] ».**

Le législateur clarifie donc que certains renseignements peuvent être visés par la Loi sur l'accès même s'ils ne permettent pas directement d'identifier une personne, par exemple, si le nom et les renseignements identificatoires d'une personne ont été remplacés par un code unique, tel un numéro d'employé[5]. Ainsi, dans les procès-verbaux des municipalités, si les décisions prises en regard d'un employé font référence à un numéro d'employé, ce numéro demeure un renseignement personnel. Les nouvelles possibilités de réidentification des personnes rendues possibles par les nouvelles technologies, comme le croisement de données, sont appréhendées par la réforme de la Loi 25.

DISPOSITIONS ENTRANT EN VIGUEUR EN SEPTEMBRE 2023

1. ADOPTION ET DIFFUSION DES RÈGLES DE GOUVERNANCE DE LA MUNICIPALITÉ

1.1. Contenu des règles

D'ici le 22 septembre 2023, les municipalités[1] devront établir des règles encadrant leur gouvernance à l'égard des renseignements personnels qu'elles détiennent. Ces règles :

- **Devront avoir été approuvées par le Comité[2]**
- **Devront notamment prévoir :**
  - Les rôles et responsabilités des membres du personnel tout au long du cycle de vie des renseignements personnels;
  - Un processus de traitement des plaintes relatives à la protection des renseignements personnels;
  - Une description des activités de formation et de sensibilisation à la protection des renseignements personnels offerts par l'organisme à son personnel;
  - Des mesures de protection particulières à l'égard des renseignements personnels recueillis ou utilisés dans le cadre d'un sondage, dont :
    - une évaluation de la nécessité de recourir au sondage ;
    - l'aspect éthique du sondage compte tenu, notamment, de la sensibilité des renseignements personnels recueillis et la finalité de leur utilisation.

Le gouvernement pourrait prévoir le contenu et les modalités de ces règles par règlement[2].

1.2. Forme et diffusion des règles

Les règles pourront prendre la forme d'une politique, d'une directive ou d'un guide. Les municipalités devront diffuser les règles elles-mêmes sur leur site Internet. La notion de politique-cadre de laquelle découlent des directives ou guides offre plus de flexibilité dans la mise à jour de tels documents. Un modèle de Politique-cadre sur la gouvernance se trouve à l'**Annexe 1-A**.

[1] *Pour les fins du présent Guide, le terme « municipalité » englobe tous les organismes municipaux visés à l'art. 5 de la Loi sur l'accès, notamment, les régies intermunicipales, les mandataires ou agents d'une municipalité selon la loi, et tout organisme dont le conseil d'administration est formé d'au moins un élu municipal siégeant à ce titre et dont une municipalité ou une communauté métropolitaine adopte ou approuve le budget ou contribue à plus de la moitié du financement.*

[2] *En vertu d'un Règlement publié le 17 mai 2023 dans la Gazette officielle du Québec, les organismes publics qui, lors de l'année civile précédente, employaient 50 salariés ou moins sont exemptés de l'obligation de former un Comité. Le nombre de 50 salariés est établi en fonction de la moyenne des salariés au cours de l'année civile précédente. Dans le cas d'une municipalité, les fonctions confiées au Comité sont exercées par le directeur général, suivant l'art. 4. Pour plus d'information sur le mandat et les responsabilités du Comité, veuillez consulter le Guide, volet 1, p. 17.*

Annexe 1-A

MODÈLE DE POLITIQUE-CADRE SUR LA GOUVERNANCE

(PROTECTION DES RENSEIGNEMENTS PERSONNELS)

TABLE DES MATIÈRES

1. PRÉAMBULE

Dans le cadre de ses activités et de sa mission, la municipalité de [**Nom de la municipalité**] (la « **Municipalité** ») traite des Renseignements personnels, notamment ceux des visiteurs de son site web, de citoyens et de ses employés. À ce titre, elle reconnait l'importance de respecter la vie privée et de protéger les Renseignements personnels qu'elle détient.

Afin de s'acquitter de ses obligations en la matière, la Municipalité s'est dotée de la présente Politique. Celle-ci énonce les principes-cadres applicables à la protection des Renseignements personnels que la Municipalité détient tout au long du Cycle de vie de ceux-ci et aux droits des Personnes concernées.

La protection des Renseignements personnels détenus par la Municipalité incombe à toute personne qui traite ces renseignements. Celle-ci doit comprendre et respecter les principes de protection des Renseignements personnels inhérents à l'exercice de ses fonctions ou qui découlent de sa relation avec la Municipalité.

2. OBJET

La présente Politique :

- énonce les principes encadrant la gouvernance de la Municipalité à l'égard des Renseignements personnels tout au long de leur Cycle de vie et de l'exercice des droits des Personnes concernées ;
- prévoit le processus de traitement des plaintes relatives à la protection des Renseignements personnels ;
- définit les rôles et responsabilités en matière de protection des Renseignements personnels à la Municipalité ;
- décrit les activités de formation et de sensibilisation que la Municipalité offre à son personnel.

3. CADRE NORMATIF

La présente Politique s'inscrit dans un contexte régi notamment par la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, c. A-2-1.). Conformément à cette Loi, la présente Politique est accessible via le site Internet de la Municipalité **[Insérer l'hyperlien de la politique]**.

4. DÉFINITIONS

Aux fins de la présente Politique, les termes suivants désignent :

« **CAI** » la Commission d'accès à l'information du Québec.

« **Comité** » le Comité sur l'accès à l'information et la protection des renseignements personnels de la Municipalité.

« **Cycle de vie** » l'ensemble des étapes visant le traitement d'un Renseignement personnel soit la collecte, l'utilisation, la communication, la conservation et la destruction de celui-ci.

« **Évaluation des facteurs relatifs à la vie privée** » ou « **ÉFVP** » la démarche préventive qui vise à mieux protéger les Renseignements personnels et à respecter la vie privée des personnes physiques. Elle consiste à considérer tous les facteurs qui auraient des conséquences positives et négatives sur le respect de la vie privée des Personnes concernées.

« **Incident de confidentialité** » désigne toute consultation, utilisation ou communication non autorisées par la loi d'un Renseignement personnel, ou toute perte ou autre atteinte à la protection de ce renseignement.

« **Loi** » désigne la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, c. A-2.1.

« **Personne concernée** » désigne une personne physique à qui se rapportent les Renseignements personnels.

« **Renseignement personnel** » désigne toute information qui concerne une personne physique et qui permet de l'identifier directement — soit par le recours à cette seule information — ou indirectement — soit par combinaison avec d'autres informations.

« **Responsable de l'accès aux documents** » ou RAD désigne la personne qui, au sein de la Municipalité, exerce cette fonction et qui doit répondre aux demandes d'accès aux documents selon la Loi.

« **Renseignement personnel sensible** » désigne tout Renseignement personnel qui — de par sa nature, notamment médicale, biométrique ou autrement intime, ou en raison de la manière dont il est utilisé ou communiqué — suscite un haut degré d'attente raisonnable en matière de vie privée.

« **Responsable de la protection des renseignements personnels** » ou « **RPRP** » désigne la personne qui, au sein de la Municipalité, exerce cette fonction et veille à y assurer le respect et la mise en oeuvre de la Loi concernant la protection des Renseignements personnels.

5. CHAMP D'APPLICATION

La présente Politique s'applique aux Renseignements personnels détenus par la Municipalité et à toute personne qui traite des Renseignements personnels que la Municipalité détient.

6. TRAITEMENT DES RENSEIGNEMENTS PERSONNELS

La protection des Renseignements personnels est assurée tout au long de leur Cycle de vie dans le respect des principes suivants, sauf exception prévue par la Loi.

6.1. Collecte

6.1.1. La Municipalité ne recueille que les Renseignements personnels nécessaires à la réalisation de sa mission et de ses activités. Avant de recueillir des Renseignements personnels, la Municipalité détermine les fins de leur traitement. La Municipalité ne recueille que les Renseignements personnels strictement nécessaires aux fins indiquées.

6.1.2. La collecte de Renseignements personnels se fait auprès de la Personne concernée.

6.1.3. Au moment de la collecte, et par la suite sur demande, la Municipalité informe les Personnes concernées, notamment, des fins et des modalités de traitement de leurs Renseignements personnels et de leurs droits quant à ces renseignements, par exemple, au moyen d'une Politique de confidentialité ou d'un avis « juste-à-temps ».

6.1.4. Lorsque la Loi exige l'obtention d'un consentement, celui-ci doit être manifeste, libre, éclairé et donné à des fins spécifiques. Il est demandé à chacune de ces fins, en termes simples et clairs. Ce consentement ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé.

6.2. Utilisation

6.2.1. La Municipalité n'utilise les Renseignements personnels qu'aux fins pour lesquelles ces renseignements ont été recueillis. Cependant, la Municipalité peut modifier ces fins si la Personne concernée y consent préalablement.

6.2.2. Elle peut également les utiliser à des fins secondaires sans le consentement de la Personne concernée, dans l'un ou l'autre des cas suivants :

- lorsque l'utilisation est à des fins compatibles avec celles pour lesquelles les renseignements ont été recueillis ;
- lorsque l'utilisation est manifestement au bénéfice de la Personne concernée ;
- lorsque l'utilisation est nécessaire à l'application d'une loi au Québec, que cette utilisation soit ou non prévue expressément par la loi ;
- lorsque l'utilisation est nécessaire à des fins d'étude, de recherche ou de production de statistiques et que les renseignements sont dépersonnalisés.

6.2.3. Lorsqu'elle utilise les Renseignements personnels à des fins secondaires dans l'un des trois premiers cas de figure énumérés à l'article 6.2.2 ci-dessus, elle doit consigner une telle utilisation au registre prévu à cet effet, tel que décrit à l'article 7.1.3.

6.2.4. Lorsque la Loi le prévoit expressément ou lorsqu'un traitement de Renseignements personnels est jugé plus à risque pour les Personnes concernées, la Municipalité entreprend une ÉFVP en vertu de l'article 8 des présentes afin de mitiger les risques identifiés.

6.2.5. La Municipalité établit et tient à jour un inventaire des fichiers de Renseignements personnels qu'elle recueille, utilise et communique. Cet inventaire contient minimalement :

- les catégories de renseignements qu'il contient, les fins pour lesquelles les renseignements sont conservés et le mode de gestion de chaque fichier ;
- la provenance des renseignements versés à chaque fichier ;
- les catégories de Personnes concernées par les renseignements versés à chaque fichier ;
- les catégories de personnes qui ont accès à chaque fichier dans l'exercice de leurs fonctions ;
- les mesures de sécurité prises pour assurer la protection des Renseignements personnels.

6.2.6. Toute personne qui en fait la demande a droit d'accès à cet inventaire, sauf à l'égard des renseignements dont la confirmation de l'existence peut être refusée en vertu des dispositions de la Loi.

6.3. Communication

6.3.1. Sous réserve des exceptions prévues par la Loi, la Municipalité ne peut communiquer des Renseignements personnels sans le consentement de la Personne concernée. Le consentement doit être donné expressément lorsque des Renseignements personnels sensibles sont en cause.

6.3.2. Lorsque des Renseignements personnels sont communiqués à un mandataire ou un fournisseur de services dans le cadre d'un mandat ou d'un contrat de services ou pour l'exécution d'un mandat, la Municipalité doit conclure une entente avec le fournisseur de services ou le mandataire qui comprend les dispositions contractuelles types de la Municipalité.

6.3.3. Lorsque les Renseignements personnels sont communiqués à des tiers hors Québec, la Municipalité procède à une ÉFVP conformément à l'article 8 des présentes. Une communication à des tiers est consignée au registre à prévu cet effet.

6.4. Conservation

6.4.1. La Municipalité prend toutes les mesures raisonnables afin que les Renseignements personnels qu'elle détient soient à jour, exacts et complets pour servir aux fins pour lesquelles ils sont recueillis ou utilisés.

6.4.2. La Municipalité conserve les Renseignements personnels aussi longtemps que nécessaire pour mener ses activités, sous réserve de délais prévus à son calendrier de conservation.

6.5. Destruction et anonymisation

6.5.1. Lorsque sont atteintes les finalités pour lesquelles les Renseignements personnels ont été collectés, ces renseignements sont détruits ou anonymisés, sous réserve de la Loi sur les archives, RLRQ, c. A- 21.1, et suivant les délais prévus au calendrier de conservation et aux règles de gestion des documents de la Municipalité.

7. REGISTRES

7.1. Conformément à la Loi, la Municipalité tient à jour les registres suivants :

7.1.1. Registre des communications de Renseignements personnels sans le consentement d'une Personne concernée dans les cas suivants :

- lorsque la Municipalité communique l'identité d'une Personne concernée à une personne ou à un organisme privé afin de recueillir des renseignements déjà colligés par ces derniers ;
- lorsque la Municipalité communique des Renseignements personnels nécessaires à l'application d'une loi au Québec, que cette communication soit ou non expressément prévue par la loi ;
- lorsque la Municipalité communique des Renseignements personnels nécessaires à l'application d'une convention collective, d'un décret, d'une ordonnance, d'une directive ou d'un règlement qui établit les conditions de travail ;
- lorsque la Municipalité communique des Renseignements personnels à un mandataire ou à un fournisseur de services dans le cadre d'un mandat ou d'un contrat de services ;
- lorsque la Municipalité communique des Renseignements personnels à des fins d'étude, de recherche ou de statistique ;
- après avoir effectué une ÉFVP, lorsque la Municipalité communique des Renseignements personnels dans les cas visés par l'article 68.

7.1.2. Dans les cas visés au paragraphe 7.1.1, le registre comprend :

- la nature ou le type de renseignement communiqué ;
- la personne ou l'organisme qui reçoit cette communication ;
- la fin pour laquelle ce renseignement est communiqué et l'indication, le cas échéant, qu'il s'agit d'une communication de Renseignements personnels à l'extérieur du Québec ;
- la raison justifiant cette communication.

7.1.3. Registre des ententes de collecte conclues aux fins de l'exercice des fonctions ou de la mise en oeuvre d'un programme d'un organisme public avec lequel la Municipalité collabore pour la prestation de services ou la réalisation d'une mission commune. Un tel registre comprend :

- le nom de l'organisme pour lequel les renseignements sont recueillis ;
- l'identification du programme ou de l'attribution pour lequel les renseignements sont nécessaires ;
- la nature ou le type de la prestation de service ou de la mission ;
- la nature ou le type de renseignements recueillis ;
- la fin pour laquelle ces renseignements sont recueillis ;
- la catégorie de personnes, au sein de l'organisme qui recueille les renseignements et au sein de l'organisme receveur, qui a accès aux renseignements.

7.1.4. Registre des utilisations de Renseignements personnels au sein de la Municipalité à d'autres fins et sans le consentement de la Personne concernée lorsque cette utilisation est compatible avec les fins pour lesquelles ils ont été recueillis, qu'elle est clairement à l'avantage de la Personne concernée ou qu'elle est nécessaire à l'application d'une loi au Québec. Un tel registre comprend :

- la mention du paragraphe du deuxième alinéa de l'article 65.1 de la Loi permettant l'utilisation, c'est-à-dire la base juridique applicable ;
- dans le cas visé au paragraphe 3° du deuxième alinéa de l'article 65.1 de la Loi, la disposition législative qui rend nécessaire l'utilisation du renseignement ;
- la catégorie de personnes qui a accès au renseignement aux fins de l'utilisation indiquée.

7.1.5. Registre des communications d'information concernant un Incident de confidentialité à une personne ou à un organisme susceptible de réduire le risque de préjudice grave associé à un Incident de confidentialité ;

7.1.6. Registre des incidents de confidentialité[3]. Un tel registre comprend :

- une description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description ;
- une brève description des circonstances de l'incident ;
- la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période ;
- la date ou la période au cours de laquelle l'organisation a pris connaissance de l'incident ;
- le nombre de Personnes concernées par l'incident ou, s'il n'est pas connu, une approximation de ce nombre ;
- une description des éléments qui amènent l'organisation à conclure qu'il existe ou non un risque qu'un préjudice sérieux soit causé aux Personnes concernées, tels que la sensibilité des renseignements personnels concernés, les utilisations malveillantes possibles de ces renseignements, les conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables ;
- si l'incident présente un risque qu'un préjudice sérieux soit causé, les dates de transmission des avis à la CAI et aux Personnes concernées, en application du deuxième alinéa de l'article 63.8 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels ou du deuxième alinéa de l'article 3.5 de la Loi sur la protection des renseignements personnels dans le secteur privé, de même qu'une mention indiquant si des avis publics ont été donnés par l'organisation et la raison pour laquelle ils l'ont été, le cas échéant ;
- une brève description des mesures prises par l'organisation, à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé.

[3] À cet effet, voir le modèle du Guide Volet 1 ou veuillez communiquer avec nous au besoin.

8. ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE

8.1. La Municipalité réalise une ÉFVP, notamment dans le contexte des traitements suivants de Renseignements personnels :

- avant d'entreprendre un projet d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services qui implique des Renseignements personnels ;
- avant de recueillir des Renseignements personnels nécessaires à l'exercice des attributions ou à la mise en oeuvre d'un programme d'un organisme public avec lequel elle collabore pour la prestation de services ou pour la réalisation d'une mission commune ;
- avant de communiquer des Renseignements personnels sans le consentement des Personnes concernées à une personne ou à un organisme qui souhaite utiliser ces renseignements à des fins d'étude, de recherche ou de production de statistiques ;
- lorsqu'elle entend communiquer des Renseignements personnels, sans consentement des Personnes concernées, conformément à l'article 68 de la Loi sur l'accès ;
- lorsqu'elle entend communiquer des Renseignements personnels à l'extérieur du Québec ou confier à une personne ou à un organisme à l'extérieur du Québec le soin de recueillir, d'utiliser, de communiquer ou de conserver de tels renseignements pour son compte.

8.2. En effectuant une ÉFVP, la Municipalité tient compte de la sensibilité des Renseignements personnels à être traités, des fins de leur utilisation, de leur quantité, de leur distribution et de leur support, ainsi que de la proportionnalité des mesures proposées pour protéger les Renseignements personnels.

8.3. De plus, lorsque les Renseignements personnels sont communiqués à l'extérieur du Québec, la Municipalité s'assure que ceux-ci bénéficient d'une protection adéquate, notamment au regard des principes de protection des Renseignements personnels généralement reconnus.

8.4. La réalisation d'une ÉFVP sert à démontrer que la Municipalité a respecté toutes les obligations en matière de protection des Renseignements personnels et que toutes les mesures ont été prises afin de protéger efficacement ces renseignements.

9. ACTIVITÉS DE RECHERCHE ET ACCÈS AUX RENSEIGNEMENTS PERSONNELS

9.1. Des chercheurs peuvent demander l'accès à des Renseignements personnels à des fins de recherche. Une telle demande doit être soumise au [RPRP de la Municipalité] ;

9.2. Lorsque l'ÉFVP conclut que des Renseignements personnels peuvent être communiqués à cette fin, la Municipalité doit conclure une entente avec les chercheurs qui contient les dispositions contractuelles types de la Municipalité et toute mesure supplémentaire identifiée dans l'ÉFVP.

10. SONDAGES

Toute personne, organisme ou autre organisation qui souhaite effectuer un sondage auprès de Personnes concernées au moyen de Renseignements personnels que détient la Municipalité doit le faire conformément à la **Politique de la Municipalité sur les sondages**.

11. DROITS DES PERSONNES CONCERNÉES

11.1. Sous réserve de ce que prévoient les lois applicables, toute Personne concernée dont les Renseignements personnels sont détenus par la Municipalité dispose notamment des droits suivants :

- le droit d'accéder aux Renseignements personnels détenus par la Municipalité et d'en obtenir une copie, que ce soit en format électronique ou non électronique ;

  - à moins que cela ne soulève des difficultés pratiques sérieuses, un Renseignement personnel informatisé recueilli auprès d'une Personne concernée, et non pas créé ou inféré à partir d'un Renseignement personnel la concernant, lui est communiqué dans un format technologique structuré et couramment utilisé, à sa demande. Ce renseignement est aussi communiqué, à sa demande, à toute personne ou à tout organisme autorisé par la loi à recueillir un tel renseignement.

- le droit de faire rectifier tout Renseignement personnel incomplet ou inexact détenu par la Municipalité ;

- le droit d'être informée, le cas échéant, que des Renseignements personnels sont utilisés pour prendre une décision fondée sur un traitement automatisé.

11.2. Bien que le droit d'accès puisse être exercé en tout temps, l'accès aux documents contenant ces renseignements est assujetti à certaines exceptions identifiées dans la Loi.

11.3. Les documents contenant des Renseignements personnels peuvent être consultés sur place ou être accessibles d'une autre manière, avec ou sans paiement de frais. Le cas échéant, la Municipalité informe la Personne concernée de l'obligation de payer des frais avant de traiter sa demande.

11.4. Les demandes d'accès aux Renseignements personnels par les Personnes concernées peuvent être faites verbalement ou par écrit. Les demandes verbales seront traitées de manière informelle et peuvent ne pas recevoir de réponse écrite.

11.5. Les demandes d'accès aux Renseignements personnels sensibles doivent être faites par écrit et recevront une réponse écrite.

11.6. Les demandes d'accès aux Renseignements personnels doivent être suffisamment précises pour permettre au RPRP de localiser lesdits Renseignements personnels. Le droit d'accès ne s'applique qu'aux Renseignements personnels existants.

12. TRAITEMENT DES PLAINTES

Toute plainte relative aux pratiques de protection des Renseignements personnels de la Municipalité ou de sa conformité aux exigences de la Loi qui concernent les Renseignements personnels doit être transmise au RPRP, lequel doit y répondre dans un délai de [•] jours [***Note : la Loi ne prévoit pas de délai de réponse, mais un délai de 20 jours serait adéquat***].

13. SÉCURITÉ DES RENSEIGNEMENTS PERSONNELS

13.1. La Municipalité met en place des mesures de sécurité raisonnables afin d'assurer la confidentialité, l'intégrité et la disponibilité des Renseignements personnels recueillis, utilisés, communiqués, conservés ou détruits. Ces mesures tiennent notamment en compte du degré de sensibilité des Renseignements personnels, de la finalité de leur collecte, de leur quantité, de leur localisation et de leur support.

13.2. La Municipalité gère les droits d'accès des membres de son personnel afin que seuls ceux soumis à un engagement de confidentialité et ayant besoin d'y accéder dans le cadre de leurs fonctions aient accès aux Renseignements personnels.

14. INCIDENTS DE CONFIDENTIALITÉ

14.1. Tout Incident de confidentialité est pris en charge conformément au [Note : nommer le plan de réponse aux incidents] de la Municipalité. La Municipalité prend alors les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent. Elle met à jour son programme de protection des Renseignements personnels, le cas échéant.

14.2. Tout Incident de confidentialité est signalé au RPRP et est consigné au registre des Incidents de confidentialité, conformément à l'article 7.1.6 de la présente Politique.

14.3. Si l'Incident de confidentialité présente un risque de préjudice sérieux pour les Personnes concernées, la Municipalité avise celles-ci avec diligence ainsi que la CAI.

15. RÔLES ET RESPONSABILITÉS

15.1. La protection des Renseignements personnels que la Municipalité détient repose sur l'engagement de tous ceux qui traitent ces renseignements et plus particulièrement des suivants :

15.2. Le RPRP :

- s'assure de la protection des Renseignements personnels tout au long de leur Cycle de vie, de la collecte à la destruction ;
- siège au Comité ;
- se conforme aux exigences liées aux demandes d'accès ou de rectification, sous réserve des responsabilités dévolues au RAD, y compris :
  - donner au requérant un avis de la date de réception de sa demande ;
  - aviser le requérant des délais et de son droit à la révision ;
  - répondre à la demande dans un délai de 20 jours, ou si le traitement de la demande ne paraît pas possible sans nuire au déroulement normal des activités de la Municipalité, dans un délai de 10 jours supplémentaires, après avoir avisé le requérant par écrit ;
  - prêter assistance au requérant pour identifier le document susceptible de contenir les renseignements recherchés lorsque sa demande est imprécise ;
  - motiver tout refus d'acquiescer à une demande d'accès ;
  - à la demande du requérant, lui prêter assistance pour l'aider à comprendre la décision le concernant ;
  - rendre sa décision par écrit et en transmettre une copie au requérant. Elle doit être accompagnée du texte de la disposition sur laquelle le refus s'appuie, le cas échéant, et d'un avis l'informant du recours en révision et indiquant notamment le délai dans lequel il peut être exercé.
  - veiller à ce que le renseignement faisant l'objet de la demande soit conservé le temps requis pour permettre au requérant d'épuiser les recours prévus à la Loi.
- supervise la tenue des registres énumérés à l'article 7 de la présente Politique.
- participe à l'évaluation du risque de préjudice sérieux lié à un Incident de confidentialité, notamment eu égard à la sensibilité des renseignements visés, aux conséquences anticipées de leur utilisation et à la probabilité que ces renseignements soient utilisés à des fins malveillantes ;
- le cas échéant, effectue des vérifications des obligations de confidentialité en lien avec la communication de Renseignements personnels dans le cadre de mandats ou de contrats de services confiés à des tiers conformément à l'article 6.3.2 de la présente Politique.

15.3. Le Comité :

- veille à la mise en place de mesures visant la sensibilisation et la formation des membres du personnel et des membres de la direction de la Municipalité sur les obligations et les pratiques en matière d'accès à l'information et de protection des Renseignements personnels ;
- élabore les principes de diffusion de l'information ;
- approuve la présente Politique-cadre sur la gouvernance en matière de protection des Renseignements personnels ;
- émet des directives sur l'utilisation d'outils informatiques marketing impliquant la communication de données ou le profilage ;
- identifie les principaux risques en matière de protection de Renseignements personnels et en avise la direction afin que des mesures correctives soient proposées ;
- approuve toute dérogation aux principes généraux de protection des renseignements personnels qui auront été établis ;
- émet des directives pour la protection des Renseignements personnels, notamment pour la conservation de ceux-ci par des tiers et à l'extérieur du Québec ;
- est consulté, dès le début d'un projet et aux fins de l'ÉFVP, pour tous les projets d'acquisition, de développement et de refonte des systèmes d'information ou de prestation électronique de services impliquant des renseignements personnels :
  - veille à ce que la réalisation de l'ÉFVP soit proportionnée à la sensibilité des renseignements concernés, aux fins auxquelles ils sont utilisés, à la quantité et à la distribution des Renseignements et au support sur lequel ils seront hébergés ;
  - le cas échéant, s'assure que le projet permet de communiquer à la Personne concernée les Renseignements personnels informatisés recueillis auprès d'elle dans un format technologique structuré et couramment utilisé ;
- escalade les recommandations qui ne sont pas suivies [au RPRP] ;
- doit être avisé de tout Incident de confidentialité impliquant les Renseignements personnels et conseiller la Municipalité quant aux suites à y donner ;
- revoit le [**Plan de réponse aux incidents de confidentialité**] dans l'éventualité d'un Incident de confidentialité ;
- revoit les règles pour la collecte et la conservation des Renseignements personnels provenant de sondages, y compris dans le cadre de la [**Politique de la Municipalité sur les sondages**] ;
- revoit toute question d'intérêt touchant la protection des Renseignements personnels ;
- revoit les mesures relatives à la vidéosurveillance et s'assure du respect de la vie privée dans le cadre de son utilisation.

15.4. Toute personne qui traite des Renseignements personnels que la Municipalité détient :

- agit avec précaution et intègre les principes énoncés à la présente Politique à ses activités ;
- n'accède qu'aux renseignements nécessaires à l'exercice de ses fonctions ;
- n'intègre et ne conserve des renseignements que dans les dossiers destinés à l'accomplissement de ses fonctions ;
- conserve ces dossiers de manière à ce que seules les personnes autorisées y aient accès ;
- protège l'accès aux Renseignements personnels en sa possession ou auxquels elle a accès par un mot de passe ;
- s'abstient de communiquer les Renseignements personnels dont elle prend connaissance dans l'exercice de ses fonctions, à moins d'être dûment autorisée à le faire ;
- s'abstient de conserver, à la fin de son emploi ou de son contrat, les Renseignements personnels obtenus ou recueillis dans le cadre de ses fonctions et maintient ses obligation de confidentialité ;
- détruit tout Renseignement personnel conformément à la procédure de **[ajouter le nom de la procédure de la municipalité.]** de la Municipalité ;
- participe aux activités de sensibilisation et de formation en matière de protection des Renseignements personnels qui lui sont destinées ;
- signale tout manquement, Incident de confidentialité ou toute autre situation ou irrégularité qui pourrait compromettre de quelque façon que ce soit la sécurité, l'intégrité ou la confidentialité de Renseignements personnels conformément à la procédure établie par la Municipalité.

16. ACTIVITÉS DE SENSIBILISATION

La Municipalité offre des activités de formation et de sensibilisation à son personnel en matière de protection des Renseignements personnels. Notamment, elle [***Note : à compléter***].

17. SANCTIONS

Toute personne qui enfreint la présente Politique est passible de sanctions selon le cadre normatif applicable.

18. MISE À JOUR

De manière à suivre l'évolution du cadre normatif applicable en matière de protection des Renseignements personnels et à améliorer le programme de protection des Renseignements personnels de la Municipalité, la présente Politique pourra être mise à jour au besoin. Veuillez vous rendre à la version sur le site Web de la Municipalité pour consulter la version la plus récente.

19. ENTRÉE EN VIGUEUR

La présente Politique entre en vigueur lors de son adoption par le Conseil de la Municipalité.

Annexe 1-B

MODÈLE DE RÉSOLUTION EXCLUANT LA MUNICIPALITÉ DE L'OBLIGATION DE FORMER UN COMITÉ SUR L'ACCÈS À L'INFORMATION ET LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

[Nom de la municipalité]

(la « Municipalité »)

RÉSOLUTION DU CONSEIL MUNICIPAL

DISSOLUTION DU COMITÉ SUR L'ACCÈS À L'INFORMATION ET LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

CONSIDÉRANT que le **[Préciser la date]** aux termes de la résolution **[Indiquer le numéro de la résolution]**, la municipalité a procédé à la nomination des membres du Comité sur l'accès à l'information et la protection des renseignements personnels (le « Comité ») conformément à l'article 8.1 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (la « Loi sur l'accès ») ;

CONSIDÉRANT l'entrée en vigueur du Règlement excluant certains organismes publics de l'obligation de former un comité sur l'accès à l'information et la protection des renseignements personnels (le « Règlement ») ;

CONSIDÉRANT que la municipalité souhaite se prévaloir de l'exclusion et être dispensée de l'obligation de former le Comité en raison du nombre de salariés à son emploi ;

CONSIDÉRANT que le Règlement prévoit que les fonctions qui étaient confiées au Comité sont confiées au directeur général ;

IL EST RÉSOLU que le conseil municipal procède à la dissolution du Comité, abroge la résolution **[Préciser le numéro de la résolution]** adoptée le **[jour]** du **[Préciser le mois] [Préciser l'année]** relative à la nomination des membres, et confie au directeur général les fonctions du Comité.

SIGNÉ le **[Préciser le jour]**e jour du mois de **[Préciser le mois]** 2023.

Annexe 1-C

MODÈLE DE RÉSOLUTION POUR L'ADOPTION DE LA POLITIQUE-CADRE SUR LA GOUVERNANCE

[Nom de la municipalité]

(la **« Municipalité »)**

RÉSOLUTION DU CONSEIL MUNICIPAL

ADOPTION DE LA POLITIQUE-CADRE SUR LA GOUVERNANCE

CONSIDÉRANT l'importance pour la Municipalité d'assurer la protection des renseignements personnels qu'elle détient en toute transparence ;

CONSIDÉRANT que l'article 63.3 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (la « Loi sur l'accès ») prévoit l'obligation pour les Municipalités de publier sur son site internet des règles encadrant sa gouvernance à l'égard des renseignements personnels ;

CONSIDÉRANT qu'afin de s'acquitter de ses obligations en la matière, la Municipalité a élaboré la présente Politique-cadre sur la gouvernance énonçant notamment les principes applicables à la protection des renseignements personnels que la Municipalité détient tout au long du cycle de vie de ceux-ci et aux droits des personnes concernées ;

CONSIDÉRANT que la présente Politique a été approuvée par le Comité sur l'accès à l'information et la protection des renseignements personnels **(**le **« Comité »)** le **[jour]** du **[Préciser le mois et l'année]** ;

IL EST RÉSOLU que le conseil municipal adopte la Politique-cadre sur la gouvernance et demande qu'elle soit publiée sur le site internet de la Municipalité.

SIGNÉ le **[Préciser le jour]**e jour du mois de **[Préciser le mois]** 2023.

2. TRANSPARENCE ET CONSENTEMENT

Le cycle de vie du renseignement personnel tel que présenté sur le site de la CAI s'exprime comme suit :

Il importe de connaitre ce cycle car les obligations applicables dépendront de l'étape du cycle de vie du renseignement personnel. Par exemple, les obligations en matière de consentement lors de la collecte de renseignements personnels (2.1) diffèreront de celles applicables à la communication de ces mêmes renseignements (2.3).

2.1. Collecte

La collecte de renseignements personnels est soumise à diverses obligations. D'une part, une municipalité ne peut recueillir que les renseignements personnels nécessaires à l'exercice de ses attributions ou à la mise en oeuvre d'un programme dont elle a la gestion[6]. D'autre part, la finalité de la collecte doit être proportionnelle à l'atteinte au droit à la vie privée qu'elle présente pour la personne concernée[7]. Enfin, la municipalité devra fournir l'information obligatoire à la personne afin que celle-ci puisse prendre une décision éclairée quant à la collecte de ses renseignements personnels.

Attention, la collecte de renseignements personnels de mineurs est soumise à des règles particulières[8]. En effet, lorsqu'une municipalité recueille des renseignements personnels auprès d'un mineur de moins de 14 ans, elle doit obtenir le consentement du titulaire de l'autorité parentale ou de son tuteur (dans la plupart des cas, ses parents). À partir de 14 ans, le mineur devient apte à consentir, en plus du tuteur et des parents.

2.1.1. Informations à fournir aux personnes concernées au moment de la collecte

Contrairement à l'utilisation ou à la communication, pour lesquelles la Loi sur l'accès exige un consentement de façon précise, la collecte de renseignements personnels ne jouit pas du même traitement[9]. En effet, le législateur ne semble pas avoir cru bon d'ajouter une obligation d'obtenir un consentement particulier[10] au moment de la collecte, comme c'est le cas sous le régime fédéral[11]. La Loi renvoie plutôt à une obligation de transparence, en ce qu'elle énumère les informations à fournir à la personne concernée lors de la collecte[12].

Le nouvel article 65 exigera en effet que chaque municipalité fournisse l'information suivante à la personne concernée au moment de la collecte :

- le nom de la municipalité au nom de qui la collecte est faite ;
- les fins auxquelles les renseignements sont recueillis ;
- les moyens par lesquels les renseignements sont recueillis ;
- le caractère obligatoire ou facultatif de la demande ;
- les conséquences pour la personne concernée ou, selon le cas, pour le tiers, d'un refus de répondre à la demande ou, le cas échéant, d'un retrait de son consentement à la communication ou à l'utilisation des renseignements recueillis suivant une demande facultative ;
- les droits d'accès et de rectification prévus par la Loi sur l'accès ;
- le cas échéant, le nom du tiers qui recueille les renseignements au nom de l'organisme public ;
- le cas échéant, le nom des tiers ou des catégories de tiers (par exemple, des fournisseurs de service) à qui il est nécessaire de communiquer les renseignements aux fins énumérées (voir la section 5 pour plus d'informations sur les obligations en matière de contrats de service) ;
- le cas échéant, la possibilité que les renseignements soient communiqués à l'extérieur du Québec.

À la demande de la personne concernée, la municipalité devra aussi informer la personne concernée :

- des renseignements personnels recueillis auprès d'elle ;
- des catégories de personnes qui ont accès à ces renseignements au sein de l'organisme public et de la durée de conservation de ces renseignements ;
- des coordonnées du responsable de la protection des renseignements personnels[13].

2.1.2. Informations à fournir avant de recueillir des renseignements à des fins de d'identification, de localisation et de profilage

Si elle recueille des renseignements personnels auprès de la personne concernée en ayant recours à une technologie comprenant des fonctions permettant de l'identifier, de la localiser ou d'effectuer un profilage, elle devra au préalable, l'informer :

- du recours à une telle technologie ;
- des moyens offerts pour activer les fonctions permettant d'identifier, de localiser ou d'effectuer un profilage[14].

Le profilage s'entend de la collecte et de l'utilisation de renseignements personnels afin d'évaluer certaines caractéristiques d'une personne physique, notamment à des fins d'analyse du rendement au travail, de la situation économique, de la santé, des préférences personnelles, des intérêts ou du comportement de cette personne.

Cette nouvelle exigence renforce le principe de confidentialité par défaut selon lequel la Municipalité qui recueille des renseignements personnels en offrant au public un produit ou un service technologique disposant de paramètres de confidentialité doit s'assurer que, par défaut, ces paramètres assurent le plus haut niveau de confidentialité, sans aucune intervention de la personne concernée[15].

2.1.2.1. La notion de « technologie »

Le législateur a choisi la désactivation par défaut de certaines technologies, laquelle demande un geste d'activation positif pour l'activation – équivalent d'un consentement exprès. Il s'agit d'un virage important introduit par la Loi 25.

Ni la Loi sur l'accès ni son pendant du secteur privé ne définissent expressément l'expression « technologie »[16].

La **LCCJTI**[17] assimile aux « technologies de l'information » celles qui sont « électroniques, magnétiques, optiques, sans fil ou autres ou faisant appel à une combinaison de technologies[18] ».

À titre d'exemple, la CAI mentionne que la vidéosurveillance, la biométrie ainsi que la géolocalisation et l'identification par radiofréquence font partie de ces « technologies[19] ».

La CAI poursuit en précisant que « ces technologies sont présentes, entre autres, dans certains passeports et permis de conduire, dans les cartes d'accès des employés, dans les cartes de plusieurs sociétés de transport au Québec, dans la téléphonie cellulaire ou encore dans certains véhicules professionnels[20] ».

Comme mentionné, une municipalité qui recueille des renseignements personnels en ayant recours à une technologie permettant d'identifier, de localiser ou d'effectuer le profilage d'un individu doit d'abord informer l'individu du recours à une telle technologie et des moyens offerts pour l'activer [21].

2.1.2.2. La notion de « localisation »

Selon les commentaires du SRIDAIL, une technologie qui comprend une fonction de localisation indique où la personne se trouve à un moment donné, par exemple un GPS peut être un instrument de localisation. Le degré de localisation est variable. La localisation peut viser, notamment, une adresse précise, un lieu approximatif, un quartier ou une ville. À compter du 22 septembre 2023, une municipalité devra donc demander aux utilisateurs d'activer les fonctionnalités qui lui permettent de les localiser au moyen d'un opt-in.

De plus, rappelons que la LCCJTI énonce :

> **À moins que la loi le prévoie expressément en vue de protéger la santé des personnes ou la sécurité publique, nul ne peut exiger qu'une personne soit liée à un dispositif qui permet de savoir où elle se trouve[22].**

Par conséquent, certaines technologies de géolocalisation devraient faire l'objet d'un consentement exprès, et ce, depuis l'entrée en vigueur de la LCCJTI en 2001.

2.1.2.3. La notion d' « identification »

Selon les commentaires du SRIDAIL, une technologie qui comprend une fonction d'identification d'une personne est présente lorsqu'elle est en mesure de distinguer celle-ci par rapport à une autre.

En présence d'un système biométrique (par exemple, la reconnaissance faciale ou d'empreintes digitales, de la cornée, etc.), un régime particulier situé dans la LCCJTI trouvera également application[23]. Voici un sommaire des obligations applicables en fonction du cycle de vie des renseignements biométriques.

Avant la collecte

- Réaliser une ÉFVP avant d'utiliser un système biométrique[24] et la mettre à jour pendant le projet, au besoin (voir section 4.1).
- Évaluer la nécessité de la collecte : c'est-à-dire pourquoi recueille-t-on les renseignements biométriques? Y'a-t-il un objectif important, légitime et réel?
- Divulguer le système biométrique à la CAI « avec diligence, dans les 60 jours avant sa mise en service »[25].
- Pour ce faire, utiliser le Formulaire de déclaration d'une banque de caractéristiques ou de mesures biométriques.
- Minimiser la collecte de renseignements biométriques : seuls ceux minimaux pour identifier ou authentifier une personne devraient être saisis[26].
- Par exemple, il ne faudrait pas recueillir l'empreinte des dix doigts d'une personne si seule l'empreinte de l'index droit est nécessaire.

Lors de la collecte

- Obtenir un consentement exprès, c'est-à-dire que la personne doit poser un geste actif (et non passif)[27].
- Exemple de modèle de consentement de Formulaire de la Commission d'accès à l'information.
- Prévoir une autre solution en cas de refus[28].
- S'assurer de déclarer le contenu obligatoire selon la loi au moment de la collecte, si le formulaire ci-dessus n'est pas utilisé[29].

Suivant la collecte

- Respecter les finalités annoncées lors de la collecte pour toute communication ou utilisation subséquente des renseignements personnels. Autrement, le consentement exprès devra être obtenu pour toute nouvelle finalité non déclarée au moment de la collecte[30].
- Interdiction stricte de toute forme de réutilisation de renseignements « découverts » à partir des données biométriques saisies (par exemple, la reconnaissance faciale peut donner des indications sur l'état émotionnel d'une personne au moment de la capture, il est strictement interdit d'en faire quoi que ce soit)[31].
- Implanter des mesures de sécurité appropriées pour protéger les renseignements biométriques, en tant que renseignements personnels sensibles[32].
- En matière biométrique, la CAI recommande fortement de conserver une base de données décentralisée et dépersonnalisée[33].

Destruction

- La destruction doit être sécurisée et irréversible. Les notes concernant les renseignements biométriques d'une personne (par exemple, les métadonnées) doivent également être détruites – pas de possibilité d'anonymisation des renseignements biométriques tel que prévu dans la Loi sur l'accès[34].
- La CAI a des pouvoirs d'ordonnance particuliers pour faire cesser l'utilisation de systèmes biométriques et obliger la destruction des renseignements biométriques[35].

Pour en savoir plus, consulter le guide sur la biométrie rendu disponible en ligne par la CAI.

2.1.2.4. La notion de « profilage »

Le profilage vise à évaluer certaines caractéristiques en vue de porter un jugement ou de tirer des conclusions sur cette personne. Il ne comprend pas les traitements purement statistiques qui visent une vue d'ensemble sur un groupe[36].

Par exemple : le fait d'offrir une navigation personnalisée sur le site d'une municipalité en fonction des champs d'intérêt et des préférences d'une personne (notamment à l'aide de témoins de connexion) est considéré comme du profilage[37]. De même, une technologie qui effectuerait un profilage à partir des informations fournies par une personne candidate pour lui refuser automatiquement un emploi dans une municipalité constituerait du profilage[38]. Dans ce dernier cas, les règles quant aux décisions fondées exclusivement sur un traitement automatisé de renseignements personnels s'appliqueraient également[39].

2.1.3. Diffusion d'une politique de confidentialité en langage clair

Les municipalités qui recueillent des renseignements personnels par un moyen technologique doivent publier sur leur site Internet et diffuser par tout moyen propre à atteindre les personnes concernées une politique de confidentialité rédigée en termes simples et clairs. Toute modification à une telle politique doit faire l'objet d'un avis[40].

Le gouvernement peut prendre un règlement pour déterminer le contenu et les modalités de cette politique et de cet avis. **Voir note complémentaire ci-dessous.**

L'Annexe 2-A à la page suivante propose un squelette afin de développer une politique de confidentialité, sous réserve d'un règlement que le gouvernement pourrait adopter en ce sens. Elle contient des pictogrammes afin de satisfaire aux exigences de langage clair, mais les municipalités sont libres de n'en retenir que le texte. Si votre organisation utilise des technologies permettant d'identifier, de localiser, profiler, ou encore, de prendre des décisions exclusivement fondées sur un traitement automatisé[41], n'oubliez pas de consulter les sections 2.1.2 et 2.2.4 afin d'intégrer les éléments prévus par la loi.

Note complémentaire :

Le 12 juillet 2023, le gouvernement du Québec a publié un Projet de règlement sur les politiques de confidentialité des organismes publics recueillant des renseignements personnels par moyen technologique. Il s'agit d'un règlement qui est actuellement au stade de la consultation publique jusqu'au 18 août prochain et qui entrera en vigueur le 1er janvier 2024.

L'entrée en vigueur de ce Règlement ne vient pas reporter l'obligation pour les municipalités d'adopter ladite politique au plus tard le 22 septembre 2023.

Lorsque le Règlement sera adopté et publié nous apporterons les modifications à l'Annexe 2-A.

Annexe 2-A

Lorsque le Règlement sur les politiques de confidentialité sera adopté et publié, nous apporterons les modifications à l'Annexe 2-A.

MODÈLE DE POLITIQUE DE CONFIDENTIALITÉ

Dernière mise à jour : [•] 2023

La municipalité de [•] s'engage à protéger la confidentialité et la sécurité de vos renseignements personnels.

Cette politique vous concerne. Elle décrit la manière dont nous recueillons, utilisons et communiquons vos renseignements personnels. Elle explique aussi comment vous pouvez demander accès à ces renseignements ou les faire rectifier, lorsque cela est nécessaire.

Lorsque vous nous fournissez des renseignements personnels via notre site Web ou une de nos applications mobiles après avoir pris connaissance de cette politique, vous consentez à ce que nous les utilisions et communiquions de la manière décrite.

EN BREF

COMMENT :
Lorsque vous naviguez sur notre site Web, téléchargez une de nos applications mobiles ou communiquez avec nous, nous recueillons certains renseignements qui vous concernent et qui nous permettent de vous identifier.

QUOI :
Nous recueillons des renseignements qui permettent de vous identifier, des renseignements d'achat et des renseignements concernant votre utilisation de nos services.

POURQUOI :
Pour mieux vous servir, répondre à vos questions, traiter vos demandes et administrer notre site Web ou nos applications. Qui d'autre : des fournisseurs qui nous aident à traiter des paiements ou à communiquer avec vous auront accès à certains renseignements.

OÙ :
Nous sommes situés au Québec, mais certains de nos fournisseurs peuvent avoir accès à vos renseignements à l'extérieur du Québec.

VOS DROITS :
Vous avez le droit de demander l'accès ou la rectification de ces renseignements en nous écrivant.

VOTRE CONSENTEMENT :
Vous avez le droit de retirer votre consentement en tout temps, mais cela peut nous empêcher de continuer à vous servir.

Qu'entend-on par « renseignement personnel »?

Un « renseignement personnel » peut, à lui seul ou avec d'autres informations, permettre de vous identifier, de vous localiser ou d'entrer en contact avec vous.

Comment recueillons-nous vos renseignements personnels?

Nous recueillons vos renseignements personnels lorsque vous :

- [•]

Quels renseignements recueillons-nous et pourquoi?

Nous ne recueillons que les renseignements personnels dont nous avons besoin pour offrir nos services municipaux. Ainsi, nous pouvons recueillir les renseignements suivants :

Renseignements sur votre identité

Lesquels?	**Pourquoi?**
• [•]	• [•]

Renseignements d'utilisation

Lesquels?	**Pourquoi?**
• [•]	• [•]

Documents liés aux services municipaux en ligne [ex. : payer un constat d'infraction, obtenir une licence, soumettre une demande de permis de rénovation, de construction, s'abonner à la bibliothèque, à un service de loisir, s'inscrire au camp de jour]

Lesquels?	**Pourquoi?**
• [•]	• [•]

De manière générale…

Nous devons parfois utiliser vos renseignements personnels pour :

- Respecter nos obligations légales ;
- Prévenir les cybermenaces et les fraudes ;
- Répondre aux demandes, mandats et ordonnances des tribunaux et autres organismes ;
- Protéger vos droits et intérêts ainsi que les nôtres ;
- Collaborer dans le cadre de poursuites judiciaires ou d'enquêtes.

À qui communiquons-nous vos renseignements personnels?

Dans certaines circonstances, nous faisons appel à des fournisseurs pour nous aider à vous servir. Avant de leur communiquer vos renseignements personnels, nous prenons des mesures raisonnables pour que ceux-ci s'engagent à respecter cette politique.

Catégorie de tiers	**Ce qu'ils font pour nous**
Gestion de relation avec le citoyen	• [•]
Services de paiement	• [•]

Où vos renseignements sont-ils hébergés?

Nous hébergeons et traitons vos renseignements personnels au Québec. Dans certaines circonstances, ils peuvent être hébergés à l'extérieur du Québec, là où nous engageons des fournisseurs de services tiers, notamment en **[Note : à préciser]**.

Vos renseignements personnels pourraient être communiqués dans des pays autres que votre pays de résidence, lesquels peuvent avoir des règles de protection des renseignements personnels différentes. Ils sont soumis aux lois du pays dans lequel ils se trouvent et peuvent faire l'objet d'une communication aux gouvernements, aux tribunaux ou aux organismes d'application de la loi ou de la réglementation du pays en question.

Toutefois, nos pratiques concernant vos renseignements personnels demeurent en tout temps régies par cette politique et les lois québécoises applicables en matière de protection des renseignements personnels.

Combien de temps conservons-nous vos renseignements personnels?

Nous conserverons vos renseignements personnels aussi longtemps que nécessaire aux fins décrites dans cette politique, pour nous conformer à nos obligations légales, régler les différends et conclure des ententes avec nos clients ou partenaires.

Nous supprimons les renseignements personnels obsolètes ou inutiles, par exemple, si vous nous indiquez que vous cessez d'utiliser définitivement nos services. Vous pouvez en tout temps demander la rectification ou la suppression de renseignements, en apprendre plus ici [Note : ajouter un lien vers la section « Quels sont vos droits? »].

Comment protégeons-nous vos renseignements personnels?

Mesures

Nous avons mis en place des mesures de protection physiques, administratives et techniques pour protéger la confidentialité et la sécurité des renseignements personnels que nous détenons, notamment pour prévenir les accès non autorisés.

Nos serveurs sont également gérés par un tiers spécialisé.

En cas d'incident impliquant des renseignements personnels, nous avons un plan. Il prévoit que nous aviserons les autorités et les personnes concernées lorsqu'un tel incident présente un risque de préjudice sérieux et que nous mettrons en place des mesures pour limiter les conséquences négatives. [Note : confirmer que vous en avez un].

Limitation des accès

Seul le personnel autorisé et qualifié ayant besoin de consulter vos renseignements personnels dans l'exercice de ses fonctions y a accès. De plus, les comptes employés et l'accès aux serveurs sont soumis à la double authentification.

Avertissement

Toutefois, aucune mesure de sécurité n'est absolue ou entièrement garantie. Si vous avez des raisons de croire que votre interaction avec nous n'est plus sécurisée (par exemple, si vous pensez que la sécurité des renseignements que vous nous avez fournis a été compromise), veuillez nous contacter immédiatement à l'adresse indiquée dans la section « Comment nous contacter? » [Note : ajouter hyperlien] ci-dessous.

Quand est-ce que cette politique ne s'applique pas?

Cette politique ne s'applique pas aux sites Web exploités par des tiers sur lesquels nous n'avons aucun contrôle. Si vous suivez un lien vers un site tiers (par exemple, pour vous inscrire à un événement), la politique de confidentialité de ce site tiers s'appliquera. Nous ne sommes pas responsables de leurs politiques, procédures ou pratiques en matière de protection des renseignements personnels. Nous vous invitons à prendre connaissance de ces politiques avant de soumettre des renseignements personnels à ces sites tiers.

Quels sont vos droits concernant les renseignements personnels?

Accès, suppression et rectification

Vous pouvez accéder aux renseignements personnels que nous détenons à votre sujet et, s'il y a lieu, demander des rectifications, selon ce que la loi permet ou exige. Vous pouvez aussi demander la suppression d'un renseignement périmé ou non justifié, ou formuler par écrit des commentaires.

Toutefois, pour que les renseignements personnels que nous détenons à votre sujet soient exacts et à jour, veuillez nous informer sans tarder de tout changement.

À votre demande, et à moins que cela ne soulève des difficultés pratiques sérieuses, nous pouvons vous communiquer un renseignement personnel informatisé dans un format technologique structuré et couramment utilisé. Nous communiquerons aussi, si vous le souhaitez, ce renseignement à toute personne ou à tout organisme autorisé par la loi à recueillir un tel renseignement. [Note : ce droit entre en vigueur en 2024, divulgation non obligatoire dans la politique]

Retrait de votre consentement

Vous pouvez également retirer votre consentement à l'utilisation et à la communication des renseignements personnels recueillis. Par contre, il se pourrait que nous ne soyons plus en mesure de vous offrir certains services.

[Vous pourriez aussi demander de l'information quant à notre utilisation de tout système de décision automatisée et sur l'impact qu'il peut avoir sur vous] [Note : vous n'êtes pas obligé de faire mention de ce droit dans la politique.]

Pour exercer vos droits, écrivez-nous à l'adresse [Indiquer l'adresse courriel] (voir la section « Comment nous contacter » [Note : ajouter un lien] pour d'autres options). Nous pourrions vous demander une pièce d'identité pour s'assurer qu'il s'agit bien de vous.

Pour en savoir plus sur les droits que vous confèrent les lois québécoises qui protègent votre vie privée, consultez les liens suivants : Québec.

Comment nous contacter?

Pour toute question ou tout commentaire au sujet de cette politique ou de la protection de vos renseignements personnels, veuillez communiquer avec notre Responsable de la protection des renseignements personnels aux coordonnées suivantes :

Responsable de la protection des renseignements personnels

- [•]

Notre Responsable de la protection des renseignements personnels s'occupe de répondre aux demandes d'accès ou de rectification, d'information et à toute plainte que vous pourriez avoir relativement à nos pratiques à l'égard de vos renseignements personnels.

Allons-nous mettre à jour cette politique?

Si nous apportons des changements importants à cette politique, par exemple, pour nous conformer aux nouvelles exigences de la loi, nous vous aviserons un mois à l'avance afin que vous puissiez faire un choix éclairé quant à votre utilisation de nos services. Nous mettrons la nouvelle version à votre disposition sur le site Web, en indiquant la date de la dernière mise à jour. Si vous nous avez fourni vos coordonnées, nous vous transmettrons un avis de modification.

Annexe 2-B

MODÈLE DE RÉSOLUTION POUR L'ADOPTION DE LA POLITIQUE DE CONFIDENTIALITÉ

[Nom de la municipalité]

(la **« Municipalité »)**

RÉSOLUTION DU CONSEIL MUNICIPAL

ADOPTION DE LA POLITIQUE DE CONFIDENTIALITÉ

CONSIDÉRANT l'importance pour la Municipalité d'assurer la protection des renseignements personnels qu'elle détient en toute transparence ;

CONSIDÉRANT que l'article 63.4 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (la « Loi sur l'accès ») prévoit l'obligation pour les municipalités de publier sur son site Internet et de diffuser par tout moyen propre à atteindre les personnes concernées une politique de confidentialité rédigée en termes simples et clairs ;

CONSIDÉRANT qu'afin de s'acquitter de ses obligations en la matière, la Municipalité a élaboré la présente Politique de confidentialité énonçant notamment les principes applicables à la protection des renseignements personnels que la Municipalité recueille par un moyen technologique.

IL EST RÉSOLU que le conseil municipal adopte la Politique de confidentialité et demande qu'elle soit publiée sur le site internet de la Municipalité et diffusée par tout moyen propre à atteindre les personnes concernées

SIGNÉ le **[Préciser le jour]**e jour du mois de **[Préciser le mois]** 2023.

2.2. Utilisation

2.2.1. Forme et validité du consentement

De manière générale, lorsque la Loi sur l'accès prévoit l'obtention d'un consentement, celui-ci doit avoir les attributs suivants[42] pour être valide :

MANIFESTE	Évident, certain et indiscutable et qu'il ne doit laisser aucun doute quant à la volonté qui y est exprimée.
LIBRE	Donné sans contrainte. Ce critère ne serait pas satisfait si, par exemple, le consentement résultait d'une pression exercée sur la personne concernée.
ÉCLAIRÉ	Qui permet à la personne concernée de donner son consentement en toute connaissance de cause.
DONNÉ À DES FINS SPÉCIFIQUES	Demandé à des fins précises; il ne peut donc pas être général. La personne concernée doit être en mesure de choisir si elle consent ou non à chaque fin spécifique, par exemple en cochant des cases dans un formulaire électronique.
D'UNE DURÉE NÉCESSAIRE À LA RÉALISATION DES FINS AUXQUELLES IL A ÉTÉ DEMANDÉ	Le consentement ne doit être donné que pour la durée nécessaire à la réalisation des fins auxquelles il a été demandé. Cette durée peut être un nombre de jours, de mois ou d'années, ou alors faire référence à un événement déterminé ou à une situation précise.

Par ailleurs, la demande de consentement doit :

- viser chaque fin séparément ;
- être rédigée en termes simples et clairs ;
- lorsque faite par écrit, être présentée distinctement de toute autre information communiquée à la personne concernée ;
- offrir de prêter assistance à la personne concernée afin de l'aider à comprendre la portée du consentement demandé.

Enfin, le consentement ne vaut que pour la durée nécessaire à la réalisation des fins auxquelles il a été demandé[43]. Un consentement qui n'est pas donné conformément à la Loi sur l'accès est sans effet[44]. Afin de s'assurer de la mise en oeuvre de ces exigences à travers votre municipalité, il est possible d'adopter une politique sur l'obtention du consentement et de la porter à la connaissance de votre personnel.

2.2.2. Présomption de consentement à l'utilisation et à la communication

Lors de la collecte, la nouvelle mouture de la Loi sur l'accès crée une présomption selon laquelle la personne qui fournit ses renseignements personnels après avoir reçu l'information obligatoire (décrite à la section 2.1.1) consent à leur utilisation et à leur communication aux fins déclarées au moment de la collecte[45]. Ainsi, sauf dans les cas où la Loi sur l'accès autorise l'utilisation (et la communication) sans consentement[46], la Loi sur l'accès exige d'obtenir un consentement distinct à l'utilisation et à la communication de renseignements personnels aux fins qui ne seraient pas déclarées au moment de la collecte.

2.2.3. Utilisation à des fins secondaires

Une utilisation qui n'est pas déclarée au moment de la collecte est une « utilisation à des fins secondaires ». Elle est permise par la Loi sur l'accès dans deux cas :

1) Elle constitue un cas de figure prévu par la loi

Une municipalité pourrait utiliser un renseignement personnel sans avoir obtenu le consentement lors de la collecte dans les cas suivants :

- son utilisation est à des fins compatibles avec celles pour lesquelles il a été recueilli

Pour qu'une fin soit « compatible », il doit y avoir un lien direct et pertinent avec les fins pour lesquelles le renseignement a été recueilli[47].

- son utilisation est manifestement au bénéfice des personnes concernées ;
- son utilisation est nécessaire à l'application d'une loi ;
- son utilisation est nécessaire à des fins d'étude, de recherche ou de production de statistiques et il est dépersonnalisé[48].

Un renseignement personnel est « dépersonnalisé » lorsqu'il ne permet plus d'identifier directement la personne concernée[49]. Cette notion de « dépersonnalisation » est à distinguer de celle d' « anonymisation » abordée à la section 8. Le processus de dépersonnalisation au sein d'une municipalité entraîne également l'obligation de mettre en place les moyens raisonnables pour limiter les risques de réidentification des personnes concernées[50]. Si votre municipalité compte recourir à de la dépersonnalisation, assurez-vous d'adopter des directives claires à cet effet et de les diffuser à travers les membres de votre personnel, par exemple sous la forme d'une politique.

Ne pas oublier de consigner ces utilisations à des fins secondaires dans le registre prévu à cet effet, lorsque requis par la loi [51].

2) Le consentement des personnes concernées a été obtenu

Si votre municipalité souhaite utiliser un renseignement personnel à une finalité qui n'a pas été déclarée au moment de la collecte et qui n'est pas prévue par la Loi sur l'accès, le consentement de(s) personne(s) concernée(s) devra être obtenu[52]. Le consentement devra être obtenu conformément aux règles générales sur le consentement prévues à la section 2.2.1.

Si le renseignement personnel est un renseignement personnel sensible, un consentement exprès doit être obtenu[53]. Également, les attentes raisonnables de la personne concernée pourraient exiger l'obtention d'un consentement exprès.

Un « renseignement personnel sensible » désigne tout Renseignement personnel qui — de par sa nature, notamment médicale, biométrique ou autrement intime, ou en raison de la manière dont il est utilisé ou communiqué — suscite un haut degré d'attente raisonnable en matière de vie privée[54].

2.2.4. Obligation d'information liée à une décision fondée sur un traitement automatisé

La nouvelle Loi prévoit une obligation de transparence pour les municipalités qui prennent une décision fondée exclusivement sur un traitement automatisé des renseignements personnels d'une personne[55]. On pourrait penser, par exemple, au cas où une municipalité aurait recours à une technologie permettant d'accorder ou de refuser une vignette ou un permis de construction selon l'analyse automatisée de pièces justificatives d'un citoyen.

Une telle décision doit permettre à la municipalité de prendre position sur une personne et avoir des conséquences, notamment juridiques, sur celle-ci.

Une décision fondée exclusivement sur un traitement automatisé est celle qui a été prise sans aucune intervention humaine, ou du moins, sans qu'une personne physique n'ait exercé de contrôle important dans la décision.

En présence d'une telle pratique, les municipalités devront informer les personnes concernées du fait que leurs renseignements personnels sont utilisés pour prendre une décision fondée exclusivement sur un traitement automatisé, au plus tard au moment où la personne est informée de la décision elle-même. Les organismes utilisant des technologies pour prendre des décisions basées exclusivement sur le traitement automatisé de renseignements personnels devraient en outre mentionner cette utilisation dans leur politique de confidentialité (voir l'**Annexe 2-A** pour un modèle de Politique de confidentialité) et réaliser une ÉFVP (voir section 4.2.).

À la demande de la personne visée par une décision automatisée, la municipalité l'informe quant aux éléments suivants :

- les renseignements personnels utilisés pour rendre la décision ;
- les raisons et principaux facteurs et paramètres ayant mené à la décision ;
- le droit de faire rectifier les renseignements personnels utilisés pour rendre la décision.

2.3. Communication

Selon la CAI, la communication est la période où le renseignement personnel est communiqué.

Par exemple :

- lorsque qu'un citoyen achète un titre de stationnement grâce à un système de prestation électronique de services ;
- lorsqu'un citoyen transmet des commentaires par courriel au sujet d'une piste cyclable.

Une telle décision doit permettre à la municipalité de prendre position sur une personne et avoir des conséquences, notamment juridiques, sur celle-ci.

Une décision fondée exclusivement sur un traitement automatisé est celle qui a été prise sans aucune intervention humaine, ou du moins, sans qu'une personne physique n'ait exercé de contrôle important dans la décision :

- lorsqu'il s'adresse au service à la clientèle de sa bibliothèque de quartier ;
- lorsqu'il s'adresse à la direction des travaux publics ;
- lorsqu'un citoyen remplit un formulaire sur un site Web.

2.3.1. Communication de renseignements personnels

La règle générale en matière de consentement à la communication de renseignements personnels demeure inchangée : un consentement distinct doit être obtenu si la communication envisagée par la municipalité n'a pas été déclarée lors de la collecte conformément à la section 2.1 de ce guide, par exemple par le biais d'un formulaire ou d'une politique de confidentialité. Comme pour l'utilisation, le consentement doit être exprès si le renseignement personnel visé est sensible (voir la section 2.2.3).

2.3.2. Exceptions à l'obligation d'obtenir un consentement

Il existe plusieurs cas de figure où le consentement des personnes n'est pas requis pour communiquer leurs renseignements personnels, car permis par la loi. Ces derniers étaient déjà présents avant la Loi 25. Cela dit, les conditions d'existence des exceptions ont été renforcées, par exemple en raison de la nécessité de conclure une ÉFVP (voir section 4).

Également, plusieurs communications de renseignements personnels faisant l'objet d'une exception au consentement doivent être consignées dans les registres prévus par la Loi sur l'accès et décrits à la section 7.

Enfin, les règles applicables à l'impartition (ex. communication à des fournisseurs ou mandataires d'une municipalité sans consentement) ont été modifiées et se trouvent à la section 5.

3. Droits des personnes concernées

La Loi 25 n'a pas apporté de changements significatifs aux droits des personnes concernées à l'égard de leurs renseignements personnels.

3.1. Accès

Pour rappel, toute personne a le droit d'être informée de l'existence de renseignements personnels la concernant et d'en recevoir communication, sous réserve des restrictions au droit d'accès prévues par la Loi[56].

3.1.1. Droit à la « portabilité »

Au-delà du droit d'obtenir copie de ses renseignements personnels, à partir du 22 septembre 2024, toute personne pourra obtenir, dans un format technologique structuré et couramment utilisé[4], un renseignement personnel informatisé qu'elle a fourni, ou demander que celui-ci soit transmis à une autre personne ou à un organisme dans ce même format[57].

Le droit à la portabilité se limite aux renseignements personnels informatisés recueillis auprès d'une personne, c'est-à-dire ceux que la personne a fourni directement à une municipalité, par exemple, les renseignements d'identité déposés en ligne au soutien d'une demande de permis. Ainsi, ce droit ne vise pas les renseignements personnels recueillis en format papier ni les renseignements qu'une municipalité aurait créés ou inférés à partir des renseignements personnels de la personne concernée recueillis.

Lorsque le requérant demande à la municipalité de communiquer ses renseignements personnels à un tiers, il incombe à la municipalité de vérifier que le tiers est en droit de recueillir de tels renseignements personnels, en tenant compte, selon le cas, de la notion d'intérêt sérieux et légitime, du critère de nécessité et, s'il s'agit d'un organisme public, des attributions de cet organisme ou des programmes dont il a la gestion[58].

La municipalité n'est pas tenue d'évaluer la qualité des renseignements personnels avant de donner suite à chaque demande. Toutefois, elle doit veiller à ce que les renseignements personnels soient à jour, exacts et complets pour servir aux fins pour lesquelles ils sont recueillis ou utilisés[59].

Selon le SRIDAIL, « un organisme public doit privilégier des formats adaptés aux renseignements demandés, ouverts et interopérables. [...] En revanche, un format difficile à traiter, comme une image, un PDF ou un format dont l'utilisation implique l'acquisition d'un logiciel ou d'une licence payante, n'est pas considéré comme étant un format technologique structuré et couramment utilisé. »

Le droit à la portabilité peut s'exercer à condition qu'il ne soulève pas de difficultés pratiques sérieuses, par exemple, si la demande représente des coûts importants ou est trop complexe. Si elle refuse d'acquiescer à une demande pour ce motif, la municipalité devrait être en mesure d'appuyer sa position lors d'une demande de révision devant la CAI.

[4] Selon le SRIDAIL, un format est dit « structuré et couramment utilisé » lorsque des applications logicielles d'usage courant peuvent facilement reconnaître et extraire les informations qui y sont contenues.

Nouveauté de septembre 2023 : les municipalités peuvent communiquer au conjoint ou à un proche parent d'une personne décédée un renseignement personnel qu'elles détiennent concernant cette personne, si la connaissance de ce renseignement est susceptible d'aider le requérant dans son processus de deuil et que la personne décédée n'a pas consigné par écrit son refus d'accorder ce droit d'accès[60].

Lorsqu'elle souhaite mettre en oeuvre un projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services qui implique des renseignements personnels, la municipalité doit, en plus des obligations d'ÉFVP décrites à la section 4.1, permettre qu'un renseignement personnel informatisé recueilli auprès de la personne concernée soit communiqué à cette dernière dans un format technologique structuré et couramment utilisé.

3.2. Rectification et suppression

Par ailleurs, toute personne dont l'existence de renseignements personnels a été confirmée peut demander la rectification de tels renseignements s'ils sont inexacts, incomplets, équivoques, ou si leur collecte, leur communication ou leur conservation ne sont pas autorisées par la loi[61].

L'art. 40 du Code civil ajoute que « toute personne peut faire supprimer, dans un dossier qui la concerne, un renseignement périmé ou non justifié par l'objet du dossier. »

Le RPRP d'une municipalité doit donner suite à une demande d'accès ou de rectification avec diligence, au plus tard dans les 20 jours après la date de la réception[62]. Lorsqu'il refuse l'accès, ce dernier doit en expliquer les raisons à la personne concernée et indiquer la disposition de la Loi sur laquelle ce refus s'appuie[63].

3.3. Retrait du consentement

La Loi sur l'accès prévoit aussi qu'une personne peut retirer son consentement à l'utilisation et à la communication des renseignements personnels recueillis, si ceux-ci sont recueillis lors d'une demande facultative[64]. Il faudra attendre des lignes directrices de la CAI ou du SRIDAIL quant à la manière dont ce droit sera mis en oeuvre, notamment à savoir s'il se rattachera au droit à la suppression.

Notons que les droits d'accès, de rectification et de retrait du consentement font partie des informations à fournir aux personnes concernées au moment de la collecte de renseignements personnels, comme expliqué à la section 2.1.1.

3.4. Devoir d'assistance

Dans le cadre d'une demande d'accès, une personne pourra solliciter l'assistance du RAD ou du RPRP pour comprendre la teneur de la décision reçue. Rappelons que la décision refusant l'accès à un renseignement ou à un document doit être motivée et indiquer la disposition légale sur laquelle le refus s'appuie[65]. Cette motivation doit permettre au requérant de comprendre le refus pour chacun des renseignements ou des documents visés[66].

Le devoir d'assistance implique de vulgariser la décision en fournissant les raisons pour lesquelles la communication est refusée, et non de fournir un argumentaire juridique. Le RPRP ou le RAD doit agir d'une manière diligente et raisonnable.

4. Évaluation des facteurs relatifs à la vie privée

Une ÉFVP est une démarche **préventive** visant à mieux protéger les renseignements personnels et à respecter davantage la vie privée des personnes concernées. Elle consiste à tenir compte des facteurs qui auraient des conséquences positives et négatives sur le respect de la vie privée des personnes concernées[67]. Ces facteurs impliquent :

- de vérifier que le projet est conforme au droit applicable et aux principes qui en découlent ;
- de déterminer les risques d'atteinte à la vie privée qu'il présente et d'évaluer leurs conséquences ;
- de mettre en place des stratégies pour éviter ces risques ou les mitiger efficacement.

Le processus d'ÉFVP vise d'abord à protéger les personnes physiques concernées, et non les intérêts de la municipalité. Il vise aussi la mise en place de mesures adéquates pour respecter toutes les obligations applicables en matière de protection des renseignements personnels. Ainsi, l'ÉFVP vise à anticiper les problèmes que causerait une gestion inadéquate des renseignements personnels par la municipalité (plaintes, incidents de sécurité, poursuites judiciaires, atteinte à l'image, etc.).

Par ailleurs, une ÉFVP est **évolutive**. Elle n'est efficace que si elle est mise à jour de façon continue. Elle doit être revue au besoin, tout au long de la vie du projet.

Pour permettre la détection et le signalement des situations qui requièrent une ÉFVP, les municipalités doivent sensibiliser leur personnel et peuvent même désigner des responsables dans chaque ligne d'affaires, selon la taille de la municipalité. Ces personnes devraient être en contact direct avec le RPRP et le Comité.

Pour en savoir plus sur les ÉFVP, consulter le Guide sur la réalisation des ÉFVP publié par la CAI en mars 2021, qu'elle doit mettre à jour d'ici le 22 septembre 2023 pour se conformer à l'entrée en vigueur des nouvelles obligations introduites par la Loi 25. Dans l'attente de la mise à jour, le guide devrait tout de même servir de base aux municipalités pour compléter les différentes ÉFVP obligatoires à partir de septembre 2023.

Le devoir d'assistance implique de vulgariser la décision en fournissant les raisons pour lesquelles la communication est refusée, et non de fournir un argumentaire juridique. Le RPRP ou le RAD doit agir d'une manière diligente et raisonnable.

4.1. Acquisition, développement et refonte de système d'information ou de prestation électronique de services

Avant d'acquérir, développer ou refondre un système d'information ou de prestation électronique de service (« PES ») qui demanderait de recueillir, utiliser, communiquer, conserver ou détruire des renseignements personnels, les municipalités devront procéder à une ÉFVP[68].

En principe, l'obligation de faire une ÉFVP ne s'étend pas à la mise à jour d'un système d'information ou d'une prestation électronique de services, sauf si cette mise à jour est susceptible d'avoir des conséquences importantes sur la protection des renseignements personnels.

Dès le début d'un projet, le Comité doit être consulté. À toute étape d'un projet visé, le Comité peut suggérer :

- de nommer une personne pour mettre en oeuvre des mesures de protection des renseignements personnels ;
- des mesures de protection dans tout document, tels un cahier des charges ou un contrat ;
- de décrire des responsabilités des personnes participantes, en matière de protection des renseignements personnels ;
- la tenue d'activités de formation sur la protection des renseignements personnels pour les personnes participantes.

Un organisme public doit prévoir qu'une personne pourra exercer son droit à la portabilité, à la condition que ce droit ne soulève pas des difficultés pratiques sérieuses (voir la section 3.1.1).

Un modèle pour réaliser cette analyse suit à l'**Annexe 4-A**.

ANNEXE 4-A

MODÈLE D'ÉFVP POUR UN PROJET D'ACQUISITION, DÉVELOPPEMENT ET REFONTE DE SYSTÈME D'INFORMATION OU DE PRESTATION ÉLECTRONIQUE DE SERVICES

Introduction

Ce formulaire s'adresse à une personne ou à un département souhaitant réaliser un projet d'acquisition, de développement ou de refonte de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels (un « **Projet** »), en application de la Loi sur l'accès aux documents des organismes publics et la protection des renseignements sur l'accès (la « **Loi sur l'accès** »).

Par « renseignement personnel », on entend un renseignement qui concerne une personne physique et permet, directement ou indirectement, de l'identifier. Ceci peut comprendre son nom, son numéro d'assurance sociale (NAS), son adresse postale, son numéro de téléphone, son adresse électronique, son numéro de télécopieur, son état de santé, sa situation financière, les renseignements relatifs à sa carte de crédit et son historique de crédit. Les renseignements personnels concernent un individu (personne physique), par opposition à une entreprise (personne morale). Les renseignements dépersonnalisés sont des renseignements personnels.

Description du processus permettant d'obtenir l'approbation d'un Projet

Dès la réception de votre document, notre Responsable de la protection des renseignements personnels (notre « **RPRP** ») procédera à l'évaluation des facteurs qui pourraient avoir des conséquences positives ou négatives sur le respect de la vie privée des personnes dont les renseignements personnels seraient visés par un Projet (l'« **ÉFVP** »).

Veuillez noter que le délai de traitement variera notamment en fonction de l'étendue du Projet, de la quantité et de la nature des renseignements personnels qu'il concerne.

Le RPRP pourrait vous demander de l'information additionnelle avant de vous faire part de sa décision. Si l'ÉFVP est approuvée, le RPRP autorisera la mise en oeuvre du Projet, y compris des mesures de mitigation, contractuelles ou autres, permettant de limiter les risques relatifs à la vie privée.

Le formulaire signé doit être transmis au **RPRP** au début du Projet, mais doit être mis à jour tout au long de l'évolution de ce dernier, par exemple :

- lors de la survenance d'enjeux en matière de protection des renseignements personnels qui pourraient nécessiter une expertise ;
- ponctuellement, à votre demande pour obtenir un avis quant aux répercussions considérables de l'évolution du Projet sur l'ÉFVP.

Instructions

Veuillez compléter les sections 1 à 3 du formulaire qui suit. La dernière section est réservée à notre RPRP. Voici quelques instructions avant de débuter :

• Vous ne devez répondre aux questions que dans le cadre de votre rôle et de vos responsabilités et au meilleur de vos connaissances. Par conséquent, si vous ne connaissez pas la réponse, ou pensez qu'elle relève d'un autre département, veuillez l'indiquer.

• Au contraire, si vous pensez que la réponse relève d'une personne au sein de votre équipe/département, n'hésitez pas à lui transmettre la question pour qu'elle puisse y répondre. La réalisation d'une ÉFVP est un travail d'équipe.

• Veuillez joindre tout document pertinent pour compléter votre réponse et en faire mention à même ce formulaire, à la section 3.

• Si vous pensez que votre Projet implique une communication de renseignements personnels hors du Québec, complétez en parallèle la procédure d'ÉFVP « Communication hors Québec » et n'oubliez pas de documenter la communication dans notre [Registre des communications].

Pour toute question ou pour acheminer votre formulaire d'ÉFVP rempli, veuillez communiquer avec notre Responsable de la protection des renseignements personnels **[Ajouter lien hypertexte].**

DEMANDE D'ÉFVP – PROJET TECHNOLOGIQUE

1. Identification du département et du responsable du Projet

Département responsable :

Personne responsable du Projet :

Demande d'ÉFVP préparée par :

Fonction au sein de la municipalité :

Date de soumission au RPRP :

Responsable TI impliqué :

Autre(s) partie(s) prenante(s) impliquée(s) (ou que vous songez à impliquer) :

2. Sommaire du Projet

Objectif :

Contexte :

Dates de début et de fin (ou dates envisagées) ; précisez les différentes phases, le cas échéant :

*Joindre tout document pertinent à la section 3.

3. Présence de renseignements personnels

Répondez au meilleur de vos connaissances.		**Oui**	**Non**
a)	Je suis certain(e) que le Projet implique des renseignements personnels.	☐	☐
b)	Les renseignements personnels ne sont pas exclusivement à caractère public (voir **Appendice 1**).	☐	☐
c)	Le Projet implique des modifications/mises à jour d'un système qui comprend des renseignements personnels.	☐	☐
d)	Le Projet implique l'ajout/modification d'un système qui a des liens (est connecté) avec un autre système qui comprend des renseignements personnels.	☐	☐

Si vous avez répondu « **NON** » à toutes les questions :

- vous n'avez pas à communiquer votre demande d'ÉFVP au RPRP ;
- Vous devez conserver ce document dans le dossier du Projet.

Si vous avez répondu « **OUI** » à l'une des questions, veuillez répondre aux questions suivantes.

4. Sélectionnez le type de Projet envisagé.

☐ Acquisition d'un système d'information ou d'une prestation électronique de services (« PES »)

☐ Développement d'un système d'information ou d'une PES

☐ Refonte d'un système d'information ou d'une PES

Nom du système ou de la PES :

Description détaillée du Projet (description des objectifs, des finalités, du cadre juridique, de la valeur ajoutée, etc.) :

Joindre tout document pertinent à la section 3.

5. Inventaire des renseignements personnels visés par le Projet

Personnes visées	Sélectionnez tout ce qui s'applique :	Commentaires
Renseignements visant des clients	☐	
Renseignements visant des employés	☑	
Renseignements visant des internautes	☑	
Autres (renseignements sur des étudiants ou stagiaires, des cadres, des membres du conseil d'administration, coordonnées professionnelles de fournisseurs ou partenaires, etc.)	☐	**Préciser :**

Type	Sélectionnez tout ce qui s'applique	Pourquoi ce renseignement est-il nécessaire au Projet?
Prénom	☑	
Nom de famille	☐	
Nom d'utilisateur	☐	
Adresse courriel	☐	
Adresse postale	☐	
Adresse IP	☐	
Numéro de téléphone personnel	☐	
Numéro d'assurance sociale	☐	

Type	Sélectionnez tout ce qui s'applique	Pourquoi ce renseignement est-il nécessaire au Projet?
Renseignements démographiques (âge, origine ethnique, etc.)	☐	**Préciser :**
Historique d'achat	☐	
Profil de consommateur et préférences	☐	**Préciser :**
Renseignements sensibles - voir **Appendice 1**	☐	**Préciser :**
Renseignements créés ou inférés à partir de renseignements personnels [NTD : ajouter un exemple pour contexte]	☐	**Préciser :**
Renseignements dépersonnalisés (code d'employé, de participant, de client, etc.) – voir **Appendice 1**	☐	**Préciser :**
Renseignements à caractère public voir **Appendice 1**	☐	**Préciser :**
Autre	☐	**Préciser :**

6. Contexte de l'utilisation des renseignements personnels

a) Objectifs de l'utilisation des renseignements personnels

b) Façon dont les renseignements personnels seront utilisés

c) Personnes qui auront accès aux renseignements personnels :

Administrateurs informatiques ☐

Préciser le groupe de personnes ayant accès et le nombre approximatif d'individus (p. ex. : service aux citoyens/50 personnes)

Fournisseur de services externe ☐

Préciser le groupe de personnes ayant accès et le nombre approximatif d'individus (p. ex. : service aux citoyens/50 personnes)

Préciser si un fournisseur infonuagique pourrait avoir accès aux données

Préciser le groupe de personnes ayant accès et le nombre approximatif d'individus (p. ex. : service aux citoyens/50 personnes)

Autre
Préciser le groupe de personnes ayant accès et le nombre approximatif d'individus (p. ex. : service aux citoyens/50 personnes)

d) Support sur lequel les renseignements seront hébergés

Veuillez sélectionner ce qui s'applique

- ☐ Les renseignements personnels seront hébergés sur un support analogique (papier, magnétique, etc.)
- ☐ Les renseignements personnels seront hébergés sur un serveur interne
- ☐ Les renseignements personnels seront hébergés sur une plateforme infonuagique dont les accès sont contrôlés par notre équipe
- ☐ Les renseignements personnels seront hébergés sur une plateforme infonuagique à laquelle certains membres du fournisseur de service ont accès
- ☐ Les renseignements personnels seront hébergés sur les serveurs d'un tiers ou dans l'infonuagique sous le contrôle d'un tiers
- ☐ Autre

e) Répartition des renseignements personnels (préciser si les renseignements personnels sont répartis dans plusieurs bases de données à plusieurs emplacements ou s'ils sont, au contraire, conservés dans une base de données centralisée)

f) Nombre de personnes concernées (approx.)

g) Quantité de renseignements personnels visés (approx.)

Quels sont, selon vous, les risques sur la vie privée pour les personnes concernées par le Projet ? (préciser par ex. les risques en cas d'incident, de réidentification des personnes, les risques réputationnels de la divulgation non autorisée, etc.)

7. Mesures de contrôle d'accès

Veuillez sélectionner les mesures que vous mettrez en oeuvre afin d'assurer la protection des renseignements personnels impliqués dans le Projet.

- ☐ Gestion et contrôle des accès basés strictement sur le besoin de la municipalité (catégories d'utilisateurs)
- ☐ Authentification multifacteurs pour accéder aux données ou aux systèmes sous-jacents (p. ex., double facteur)
- ☐ Cycle de vie des systèmes et gestion des vulnérabilités (mise à jour logicielle)
- ☐ Configuration dans le respect du principe de vie privée par défaut (Privacy by Design)
- ☐ Segmentation du système
- ☐ Protection des données au repos
- ☐ Protection des données lors de la communication
- ☐ Traçabilité des accès
- ☐ Dépersonnalisation (p. ex., chiffrement, retrait de tous identifiants directs)
- ☐ Surveillance (suivi des accès, rapport d'activité anormale)
- ☐ Autre : **Cliquez ou appuyez ici pour entrer du texte.**

8. Mesures de sécurité informatique

	Oui	Non
L'équipe de la sécurité informatique a revu le Projet. Le cas échéant, joindre tout document pertinent dans la section 3.	☐	☐
L'ensemble des recommandations de l'équipe de la sécurité informatique ont été suivies.	☐	☐

Si vous avez répondu « **Non** » à la précédente question, veuillez lister les recommandations non implantées et les motifs.

9. Conservation et destruction selon le calendrier de conservation

	Oui	Non
Un délai d'archivage a été fixé pour les renseignements inactifs.	☐	☐
Un délai de conservation a été déterminé pour les différentes catégories de renseignements personnels.	☐	☐
Le système permet une destruction des renseignements personnels de façon automatique après l'expiration du délai de conservation (p. ex., destruction des séquences vidéo après 30 jours).	☐	☐
Le système permet la correction des renseignements personnels.	☐	☐
Les copies de sauvegarde pourraient contenir des renseignements personnels qui devraient être détruits.	☐	☐

10. Technologies utilisées pour le traitement des renseignements personnels

	Oui	Non
Les renseignements personnels seront recueillis directement auprès de la personne concernée par un outil informatique (p. ex., formulaire disponible en ligne).	☐	☐

Nom de la technologie :

Fournisseur de la technologie (le cas échéant, joindre le contrat) :

Si la réponse à la question est « **Oui** », les paramètres de sécurité par défaut du système ou de la prestation électronique de services assureront le plus haut niveau de sécurité par défaut (p. ex., ils n'autorisent pas l'utilisation de la caméra de l'appareil ou une autre fonctionnalité de façon automatique).

Est-ce qu'une décision exclusivement automatisée sera mise en place ? Est-ce qu'une technologie permettant l'identification (p. ex., la biométrie), la localisation (p. ex., fonction « localisez-moi ») ou le profilage (p. ex., établir un profil consommateur) sera utilisée ?

☐ **Non** ☐ **Oui** (préciser, le cas échéant)

11. Droits des personnes concernées

Mon Projet permet qu'un renseignement personnel informatisé recueilli directement auprès de la personne concernée soit communiqué à cette dernière dans un format technologique structuré et couramment utilisé (p. ex., en format PDF)

☐ **Non** ☐ **Oui** (préciser, le cas échéant)

Commentaires :

Signature du responsable du Projet

Date

12. Renseignements supplémentaires et documents joints

Liste des documents joints (tels que les politiques, les procédures, l'aperçu du Projet, schéma, études d'opportunité, de préfaisabilité ou de faisabilité, dossier d'affaires, toute certification obtenue, etc.), des demandes additionnelles d'information réalisées auprès du fournisseur (le cas échéant) ou de tout autre renseignement additionnel.

SECTION RÉSERVÉE AU RPRP

ANALYSE ET DÉCISION DU RPRP

Identification des risques

Identifier les risques et lacunes du Projet mis en lumière par le formulaire d'ÉFVP. Les risques peuvent, par exemple, inclure : - Conservation de renseignements lorsque leur utilité n'est plus démontrée - Vol de renseignements personnels - Collecte excessive de renseignements - Divulgation non autorisée de renseignements personnels - Réidentification de renseignements préalablement anonymisés - Manque d'informations fournies aux individus lors de la collecte - Création excessive ou non justifiée d'informations - Objectif du Projet pas suffisamment important ou non légitime - Intrusion dans la vie privée disproportionnée	[Pour chaque risque identifié, veuillez évaluer son niveau à l'aide de la grille fournie en **Appendice 2**]

Mitigation des risques

Si applicable, veuillez identifier toutes les mesures de mitigation des risques nécessaires. Les mesures peuvent, par exemple, inclure : - Des mesures de protection des renseignements personnels dans tout document relatif au Projet - La nomination d'une personne chargée de la mise en oeuvre et du suivi des mesures de protection des renseignements personnels - La planification d'activités de formation ou de sensibilisation pour les participants au Projet - Une reddition de compte périodique - Des mesures contractuelles	[La première étape consiste à identifier les causes. Les causes potentielles peuvent inclure : • un processus déficient • des erreurs dans la manipulation des renseignements • un manque de connaissances ou de formation • des mécanismes de surveillance insuffisants ou inexistants • une distribution inadéquate des responsabilités • des comportements malveillants • une collecte excessive de renseignements • des technologies défaillantes ou désuètes • l'utilisation non justifiée ou non nécessaire de renseignements sensibles • l'absence de consentement • l'existence d'un moyen moins intrusif et suffisamment efficace pour atteindre l'objectif visé Ensuite, il faut identifier les mesures de mitigations nécessaires (voir colonne de gauche). Pour chaque mesure identifiée, veuillez préciser le délai dans lequel elle serait exigée, s'il y a lieu.]

Décision ÉFVP

Responsable de la protection des renseignements personnels

☐ Le Projet est approuvé sans recommandation
☐ Le Projet est approuvé, sous réserve de l'implantation des recommandations
☐ Le Projet est refusé

Date: [JJ-MM-AAA] [Si le Projet est refusé, préciser pourquoi]

Appendice 1
Classification de la sensibilité des renseignements personnels

	CLASSE 1	CLASSE 2	CLASSE 3	CLASSE 4
Description	Renseignements personnels à **caractère public.**	Renseignements personnels **dépersonnalisés** utilisés à l'interne dans le cadre des opérations quotidiennes.	Renseignements **confidentiels** ou qui, en raison du contexte de leur utilisation ou de leur communication, suscitent un degré d'attente raisonnable en matière de vie privée.	Renseignements personnels **sensibles** qui, de par leur nature, notamment médicale, biométrique ou autrement intime, suscitent un haut degré d'attente raisonnable en matière de vie privée ou dont l'utilisation ou la communication nécessitent des procédures particulières.
Exemples	Coordonnées d'affaires, renseignements publiés au tableau de l'ordre des avocats, notaires, etc.	Renseignements qui ne permettent pas d'identifier directement une personne comme le numéro d'employé, de client ou des statistiques démographiques.	Date de naissance, adresse postale personnelle, numéro de téléphone personnel, noms des enfants, coordonnées des contacts d'urgence, etc.	Numéro d'assurance sociale, renseignements biométriques, convictions politiques, religieuses, dossier médical, orientation sexuelle ou identité de genre.
Conséquences	Aucune	Conséquences limitées pour la municipalité et les personnes concernées.	Conséquences négatives importantes, y compris des risques juridiques, économiques et réputationnels.	Conséquences négatives graves, y compris des risques juridiques, économiques et réputationnels.
Restriction d'accès	Aucune	Accès restreint à l'interne.	Accès accordés seulement aux personnes ayant besoin de connaître les renseignements (principe du moindre privilège).	Accès limité à des personnes autorisées identifiées, selon une liste régulièrement mise à jour.

Appendice 2
Classification de la sensibilité des renseignements personnels

ÉVALUATION DU NIVEAU DE RISQUE

	Risque minime 1	Risque faible 2	Risque modéré 3	Risque élevé à inacceptable 4
Risques pour les personnes concernées	Aucun impact n'est envisagé pour les personnes concernées.	Les risques n'outrepassent pas la simple incommodité temporaire, disparaissent à court terme et ne sont pas de nature à affecter les droits et libertés des personnes concernées. Les renseignements personnels visés par le traitement ne sont pas sensibles.	Les personnes concernées sont susceptibles de subir un stress émotionnel, des pertes financières limitées ou couvertes par les assurances ou un sentiment d'intrusion. Les personnes concernées pourraient avoir à entreprendre des démarches relatives à la surveillance de leur dossier de crédit, par exemple.	Les risques visent le moyen et long terme. Ils peuvent inclure le vol d'identité, des pertes financières importantes, des effets négatifs sur les cotes de crédit, des pertes d'emplois, des dommages ou pertes de biens, la discrimination, l'extorsion, des menaces à l'intégrité de la personne et menacer la santé physique ou psychologique des personnes concernées. Les personnes concernées sont généralement informées des impacts, de même que les autorités réglementaires.
Impact de la réalisation du risque	L'impact est très faible voire inexistant. Il n'engendre aucune conséquence pour les personnes, ou des conséquences très mineures pour une seule personne. Par exemple, si seuls des coordonnées professionnelles ou des renseignements à caractère public sont visés.	L'impact engendre des conséquences mineures pour une personne ou pour un petit nombre de personnes. Par exemple, si peu de renseignements personnels dépersonnalisés sont touchés.	L'impact engendre des conséquences importantes pour une personne ou des conséquences mineures pour un grand nombre de personnes. Par exemple, si les personnes touchées sont des mineurs, des personnes ayant un handicap ou autre.	Le risque engendre des conséquences majeures pour une personne ou des conséquences importantes pour un grand nombre de personnes; si inacceptable, le risque engendre des conséquences trop importantes et/ou implique une non-conformité aux lois. Par exemple, si le risque engendre des impacts sévères sur la vie personnelle ou professionnelle ou sur les finances des personnes touchées; ou encore si elles mettent en danger la vie d'une personne.
Probabilité de réalisation du risque	Le risque n'a aucune chance de se concrétiser.	Le risque a peu de chance de se concrétiser ou un événement similaire ne s'est jamais produit.	Le risque a de bonnes chances de se réaliser ou un événement similaire s'est déjà produit à une ou quelques reprises.	Le risque a de très grandes chances de se concrétiser ou un événement similaire s'est produit à plusieurs reprises.

4.2. Communication hors Québec (Article 70.1)

Les municipalités doivent réaliser une ÉFVP distincte de celle qui précède si elles prévoient la communication de renseignements personnels ou la réalisation d'un mandat lié au cycle de gestion de la protection de renseignements personnels à l'extérieur du Québec, y compris lorsque les copies de sauvegarde de leurs serveurs sont hébergées à l'extérieur du Québec. Les municipalités devront notamment vérifier, à travers cette ÉFVP, que les renseignements personnels bénéficieront d'une protection adéquate, au regard des principes de protection des renseignements personnels généralement reconnus. Selon le SRIDAIL, ces principes sont ceux de l'Organisation de coopération et de développement économiques (OCDE) dans ses lignes directrices sur la protection de la vie privée[69].

Une municipalité ne peut communiquer des renseignements personnels à l'extérieur du Québec que si elle conclut :

- que les renseignements personnels bénéficieront d'une protection adéquate ;
- que l'État adhère à un programme de certification ou à une norme ISO reconnue ;
- que l'ajout de clauses contractuelles comblerait le respect des principales exigences de la Loi sur l'accès afin de limiter les risques liés au fait que la législation de l'État ne se conforme pas à tous les principes de protection des renseignements personnels généralement reconnus[70].

La communication ou la réalisation d'un mandat doit faire l'objet d'une entente écrite qui tient compte, notamment, des résultats de l'évaluation des facteurs relatifs à la vie privée et, le cas échéant, des modalités convenues dans le but d'atténuer les risques identifiés dans le cadre de cette évaluation. Il est donc recommandé que les municipalités prévoient des clauses contractuelles types à cet égard dans leurs modèles d'ententes qui impliquent le partage de renseignements personnels.

Un modèle pour réaliser cette analyse suit.

ANNEXE 4-B

MODÈLE D'ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE POUR UNE COMMUNICATION DE RENSEIGNEMENTS PERSONNELS À L'EXTÉRIEUR DU QUÉBEC

Introduction

La Loi sur l'accès requiert de réaliser une évaluation des facteurs relatifs à la vie privée (« ÉFVP ») avant de communiquer des renseignements personnels à l'extérieur du Québec. Elle exige que nous consignions les résultats de l'ÉFVP dans l'entente de communication ainsi que, le cas échéant, les modalités convenues dans le but d'atténuer les risques identifiés par l'ÉFVP.
Selon la Loi sur l'accès, l'ÉFVP doit notamment tenir compte de :

- **la sensibilité des renseignements communiqués ;**
- **la finalité de leur utilisation ;**
- **les mesures de protection, y compris celles qui sont contractuelles, dont les renseignements bénéficieraient ;**
- **le régime juridique applicable dans l'État où ce renseignement serait communiqué, notamment les principes de protection des renseignements personnels qui y sont applicables.**

La réalisation d'une ÉFVP permet de mettre en place les contrôles nécessaires à l'étape de l'élaboration de l'initiative afin de réduire les risques identifiés et de nous assurer de traiter les renseignements personnels conformément au droit applicable.
La réalisation de l'ÉFVP est proportionnée à la sensibilité des renseignements personnels visés, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support.

- **Une ÉFVP n'est pas nécessaire dans les cas suivants :**
  - communication à un tiers en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de la personne concernée[71] ;
  - communication à un organisme public ou à un organisme d'un autre gouvernement, lorsque la communication est manifestement au bénéfice des personnes concernées[72] ;
  - Communication faite dans le cadre d'un engagement international ou d'une autre entente visée[73].

Instructions

Veuillez compléter les sections A. et B. de la procédure qui suit. Les sections C. et D. sont réservées à notre Responsable de la protection des renseignements personnels (notre « RPRP »). Voici quelques instructions avant de débuter :
Pour toute question ou pour acheminer votre ÉFVP complétée, veuillez communiquer avec notre RPRP [ajouter hyperlien].

a) **Vous ne devez répondre aux questions que dans le cadre de votre rôle et de vos responsabilités et au meilleur de vos connaissances. Par conséquent, si vous ne connaissez pas la réponse, ou pensez qu'elle relève d'un autre département, veuillez l'indiquer.**
b) **Au contraire, si vous pensez que la réponse relève d'une personne au sein de votre équipe/département, n'hésitez pas à lui transmettre la question pour qu'elle puisse y répondre. La réalisation d'une ÉFVP est un travail d'équipe.**
c) **Veuillez joindre tout document pertinent pour compléter votre réponse et en faire mention à même la présente procédure, dans la section « 2. Renseignements supplémentaires et documents joints pertinents en soutien aux Sections A et B ».**
d) **Si la communication visée par la présente ÉFVP s'inscrit dans un projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services, complétez en parallèle la procédure d'ÉFVP pour les projets technologiques.**

ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE – COMMUNICATION HORS QUÉBEC

SECTION A

Nom du ou des tiers à qui les renseignements seraient communiqués :

ÉFVP préparée par :

Responsable de la communication :

Date de soumission au RPRP :

Date de la dernière mise à jour :

Contexte de la communication hors Québec envisagée :

Date de début de la communication (ou date envisagée) :

Une entente est-elle déjà signée ?

☐ Oui

☐ Non (préciser si elle est en cours de signature et joindre tout document pertinent dans la section B.)

Préciser si la communication envisagée est ponctuelle ou continue :

☐ Ponctuelle

☐ Continue

Situation sous-jacente :

☐ Je veux communiquer des renseignements personnels à un tiers situé hors du Québec

☐ Je veux confier le mandat de recueillir, d'utiliser, de communiquer ou de conserver des renseignements personnels pour le compte de la municipalité à un tiers situé à l'extérieur du Québec (p. ex., recruteur, expert informatique, service d'hébergement, service de gestion et de traitement, tel un service infonuagique, consultant)

Catégorie de personnes concernées (employés, résident, autre) :

☐ Résidents de la municipalité ☐ Employés ☐ Visiteurs du site internet ☐ Fournisseurs ☐ Autre (préciser)

Nombre de personnes concernées (approximation) :

Lieu(x) où seront communiqués les renseignements personnels hors du Québec :

SECTION B

1 - Renseignements sur la communication envisagée

Qui est la personne-ressource chez le ou les tiers ?

[Fournir le nom, le titre et l'adresse courriel du RPRP du ou des tiers à qui sont communiqués les renseignements personnels]

Quel est l'objectif de la communication ?

[Expliquer les objectifs de la communication, ainsi que le type de besoin d'affaires auquel la communication cherche à répondre. Le cas échéant, expliquer quels seront les avantages pour votre municipalité, pour certaines unités commerciales ou pour les personnes concernées (employés ou clients de votre municipalité).]

Quels sont les renseignements personnels communiqués et pourquoi est-il nécessaire de les communiquer ?
Insérez le type de renseignements personnels communiqués, p. ex. : nom, prénom, adresse, salaire, date de naissance, langue, information bancaire, date d'embauche, citoyenneté, numéro d'employé, numéro de téléphone personnel ou professionnel, contact en cas d'urgence, signature :

[Expliquez pourquoi chaque renseignement est nécessaire dans le cadre de la communication envisagée.]

Cochez ici si des renseignements personnels sensibles seraient communiqués :

- ☐ Renseignements révélant l'origine ethnique ou nationale
- ☐ Opinions politiques, croyances religieuses ou philosophiques
- ☐ Données génétiques ou biométriques
- ☐ Données relatives à santé
- ☐ Données concernant la vie sexuelle ou l'orientation sexuelle
- ☐ Information financière ou de paiement
- ☐ Identifiant unique (NAS, numéro de permis de conduire, numéro de passeport, etc.)
- ☐ Information de localisation (GPS, réseau Wi-Fi, cartes d'accès, etc.)
- ☐ Données susceptibles de révéler des choix de mode de vie, des intérêts personnels ou toute autre information énumérée ci-dessus (c'est-à-dire des informations de navigation, les habitudes de visionnement, etc.)
- ☐ Autre type de renseignements personnels sensibles (par ex. : identité autochtone, identité ou expression de genre, lieu de naissance et handicap)
  Veuillez préciser.

[Veuillez indiquer le niveau de sensibilité des renseignements personnels communiqués. Pour ce faire, se référer à l'**Appendice 2**. Indiquer ci-dessous la classe des renseignements personnels communiqués]

Indiquer les personnes à l'interne impliquées
[Par ex., le directeur des affaires juridiques, responsable organisationnel de la gestion de risque, toute personne chargée de la sécurité des systèmes d'information, de l'éthique, de la gestion documentaire, etc.]
Veuillez préciser.

Sécurité (du ou des tiers)

- ☐ Pratiques conformes à une norme de l'industrie comme ISO 27001
- ☐ Vérification périodique par des tiers indépendants qualifiés de type SOC 2 ou un audit équivalent
- ☐ Gestion des accès selon le principe du moindre privilège
- ☐ Double authentification aux renseignements personnels
- ☐ Dépersonnalisation
- ☐ Évaluation périodique de la sécurité / test d'intrusion (pen test)
- ☐ Autoévaluation périodique de tout contrôle important
- ☐ Interface d'authentification unique
- ☐ Droit d'audit
- ☐ Avis du fournisseur en cas d'incident de confidentialité ou de sécurité
- ☐ Traçabilité ou journalisation des accès
- ☐ Le fournisseur est responsable de ses sous-traitants
- ☐ Les sous-traitants offrent un niveau de protection équivalent à celui du tiers
- ☐ Formations sur des sujets de sécurité ou de protection des renseignements personnels obligatoires pour le personnel
- ☐ Autre (préciser) : **Cliquez ou appuyez ici pour entrer du texte**

[Les mesures de sécurité doivent être appropriées eu égard notamment à la finalité de l'utilisation des renseignements personnels une fois communiqués hors du Québec et de leur sensibilité (voir **Appendice 2**). Fournir ici plus de détails ou spécifier toute autre mesure qui sera implantée (au besoin).]

Sécurité en cours de transmission

[Quelles sont les mesures de sécurité, organisationnelles, techniques ou autres, qui seront mises en place pour protéger les renseignements personnels en cours de transmission. Si pertinent, préciser l'outil de transmission utilisé]

La communication au(x) tiers nécessite-t-elle un consentement ? Dans l'affirmative, quelle est la forme exigée ?

- ☐ Oui, consentement exprès
- ☐ Oui, consentement implicite
- ☐ La communication a été portée à la connaissance des intéressé(s) au moment de la collecte à l'aide d'une politique (joindre tout document pertinent)
- ☐ Non, une exception permet la communication des renseignements personnels sans le consentement des personnes concernées
- ☐ Je ne sais pas

[Si vous avez répondu non, veuillez préciser quelle exception permet la communication sans leur consentement et si la communication a été enregistrée au [registre des communications/inventaire des traitements]

Quel sera la durée de conservation des renseignements personnels communiqués ?

- ☐ Selon le calendrier de conservation de la municipalité
- ☐ Une durée précise (veuillez préciser) : Cliquez ou appuyez ici pour entrer du texte.
- ☐ Aucune durée de conservation exigée
- ☐ Je ne sais pas

[Précisez ce qu'il adviendra des renseignements après leur conservation (destruction – et la façon dont ils seront détruits –, ou anonymisation – dans ce cas, précisez l'intérêt sérieux et légitime justifiant l'anonymisation). Précisez également si des renseignements seront conservés sur des copies de sauvegarde.]

2 - Renseignements supplémentaires et documents joints pertinents en soutien aux Sections A et B.

Liste des documents joints (tels que les politiques, les procédures, l'aperçu du projet de communication ou du projet d'entente, etc.), des demandes additionnelles d'information réalisées auprès du tiers ou des tiers, ou de tout autre renseignement additionnel.

SECTION C

ANALYSE DU RÉGIME JURIDIQUE APPLICABLE DANS L'ÉTAT OÙ LES RENSEIGNEMENTS SONT COMMUNIQUÉS

L'ÉFVP doit établir que les renseignements personnels communiqués à l'extérieur du Québec y bénéficieront d'une protection adéquate, notamment à la lumière des principes de protection des renseignements personnels généralement reconnus[5]. Pour ce faire, l'ÉFVP doit évaluer le régime juridique applicable dans l' « État » (y compris les autres provinces canadiennes) où les renseignements seront communiqués. La municipalité doit prendre en considération si la législation de l'État reconnaît un droit à la vie privée et si elle contient des dispositions inconciliables avec le régime juridique québécois en matière de protection de la vie privée. Par exemple, des dispositions qui empêcheraient l'exécution de clauses contractuelles obligatoires selon cette ÉFVP seraient incompatibles avec le régime québécois en matière de protection de la vie privée. Si plusieurs États sont évalués, compléter une fiche par État évalué.

La communication (ou la réalisation d'un mandat pour le compte de votre municipalité) hors du Québec doit faire l'objet d'une entente écrite qui tient compte, notamment, des résultats de cette section et, le cas échéant, des modalités convenues dans le but d'atténuer les risques identifiés dans le cadre de cette évaluation.

[5] Selon le site Québec.ca, les « principes généralement reconnus » sont ceux de l'OCDE tels que publiés dans les Lignes directrices de l'OCDE régissant la protection de la vie privée, en ligne.

Principe :	Conformité :	Commentaires :
Limitation en matière de collecte La collecte des renseignements personnels doit être limitée uniquement à ceux qui sont nécessaires et proportionnels par rapport aux finalités en vue desquelles ils sont recueillis. Les renseignements personnels sont recueillis par des moyens licites et, le cas échéant, après en avoir informé les personnes concernées ou avec leurs consentements.	☐ Oui ☐ Non ☐ En partie	[Cette colonne permet d'inscrire les constatations faites lors de l'analyse de chacun des principes de protection des renseignements personnels, notamment ce qui est présent ou non dans la législation applicable à l'État où les renseignements personnels seraient communiqués.]
Qualité des renseignements Les renseignements personnels, dans la mesure où les finalités en vue desquelles ils doivent être utilisés l'exigent, doivent être exacts, complets et tenus à jour.	☐ Oui ☐ Non ☐ En partie	
Description des finalités Les finalités en vue desquelles les renseignements personnels sont recueillis doivent être déterminées au plus tard au moment de la collecte. Les renseignements personnels ne doivent être utilisés par la suite que pour atteindre ces finalités ou d'autres qui ne soient pas incompatibles avec les précédentes.	☐ Oui ☐ Non ☐ En partie	

Principe :	Conformité :	Commentaires :
Limitation de l'utilisation et de la communication Les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles pour lesquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne le permette. On ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins déterminées.	☐ Oui ☐ Non ☐ En partie	
Garanties de sécurité Les renseignements personnels doivent être protégés, grâce à des garanties de sécurité raisonnables, contre des risques tels que la perte des renseignements ou le vol ainsi que leur accès, utilisation, modification, communication, conservation ou destruction autorisés ou non autorisés. Les renseignements personnels doivent être protégés, quelle que soit la forme sous laquelle ils sont conservés, et ce, au moyen de mesures de sécurité correspondant à leur degré de sensibilité.	☐ Oui ☐ Non ☐ En partie	
Transparence Les politiques et les pratiques sur la gestion des renseignements personnels doivent être facilement accessibles à toute personne, sans effort déraisonnable. Ces renseignements doivent être fournis sous une forme généralement compréhensible. Il devrait être possible de se procurer aisément les moyens de déterminer l'existence et la nature des renseignements personnels et les finalités principales de leur utilisation, de même que l'organisme détenteur et le siège habituel de ses activités.	☐ Oui ☐ Non ☐ En partie	
Participation individuelle Toute personne physique doit avoir le droit d'obtenir la confirmation du fait qu'une organisation détient ou non des renseignements personnels la concernant. Elle devrait également avoir le droit de se faire communiquer les renseignements la concernant dans un délai raisonnable, selon des modalités raisonnables et sous une forme qui lui soit aisément intelligible.Dans ce contexte, une organisation peut exiger des frais raisonnables. Toute personne doit avoir le droit d'être informée des raisons pour lesquelles une demande d'accès à ses renseignements personnels est rejetée. Elle doit également être informée de son droit de contester un tel refus. La personne doit aussi être informée de son droit de faire rectifier, compléter, corriger ou effacer ses renseignements.	☐ Oui ☐ Non ☐ En partie	

Principe :	Conformité :	Commentaires :
Responsabilité Le droit interne prévoit que l'organisation détentrice des renseignements personnels est responsable du respect des mesures donnant effet aux principes énoncés ci-dessus. L'organisation détentrice ne devrait pas être relevée de cette obligation pour la simple raison que le traitement des renseignements personnels est effectué par un tiers. Il doit également être possible de connaître l'identité de la personne désignée pour assurer le respect des principes sur la protection des renseignements personnels (p. ex. : le responsable de la protection des renseignements personnels).	☐ Oui ☐ Non ☐ En partie	
Les renseignements personnels bénéficieront d'une protection adéquate	☐ Oui ☐ Non ☐ En partie	[Si la réponse est « Non » ou « En partie », veuillez détailler les mesures contractuelles qui peuvent être prises pour atténuer ces lacunes dans l'Appendice 1. Au contraire, indiquer si le régime juridique de l'État évalué est incompatible avec le régime juridique québécois en matière de protection de la vie privée. Par exemple, des dispositions qui empêcheraient l'exécution de clauses contractuelles obligatoires selon cette ÉFVP seraient incompatibles avec le régime québécois en matière de protection de la vie privée].
Autorisation/refus de la communication à l'extérieur du Québec	☐ Oui ☐ Non	

SECTION D

RÉSERVÉE AU RPRP, EN COLLABORATION AVEC DES CONSEILLERS JURIDIQUES EXTERNES

Décision quant à la communication

RECOMMANDATIONS :
Si applicable, veuillez identifier toutes les mesures, notamment contractuelles, nécessaires afin de remédier aux différentes lacunes mises en lumière par l'ÉFVP.

[Pour chaque mesure, veuillez préciser le délai dans lequel elle serait exigée pour sa mise en oeuvre, s'il y a lieu.]

Approbation ÉFVP
Responsable de la protection des renseignements personnels

- ☐ La communication hors Québec est approuvée sans recommandation.
- ☐ La communication est approuvée, sous réserve de la signature d'une entente comportant les mesures identifiées dans les recommandations.
- ☐ La communication est refusée.

Date:_____

[Si la communication est refusée, préciser pour quelles raisons.]

Appendice 1

Mesures contractuelles nécessaires pour l'autorisation de la communication hors-Québec

Liste des clauses à ajouter à l'entente de communication pour autoriser l'ÉFVP. Possibilité de se référer au catalogue de clauses-types de votre municipalité [NTD : à confirmer]

[Selon les résultats de l'ÉFVP, les clauses de protection des renseignements personnels peuvent inclure :

ANNEXE A l'interdiction d'utiliser à d'autres fins ou de communiquer les renseignements personnels ;

ANNEXE B des mesures de sécurité précises ;

ANNEXE C des règles relatives à l'accès aux renseignements personnels par les membres du personnel de votre municipalité ;

ANNEXE D l'obligation d'aviser votre municipalité en cas d'incident de confidentialité ou de toute autre violation ou tentative de violation de l'une ou l'autre des obligations relatives à la confidentialité des renseignements personnels communiqués ;

ANNEXE E des règles relatives à la conservation et à la destruction des renseignements personnels au terme de l'entente ou en cas de résiliation ;

ANNEXE F la conformité à une norme comme ISO, NIST, etc., reconnue par l'industrie.

Appendice 2
Classification de la sensibilité des renseignements personnels

	Classe 1	Classe 2	Classe 3	Classe 4
Description	Renseignements personnels à caractère public et pouvant être communiqués à l'extérieur de la municipalité.	Renseignements personnels dépersonnalisés utilisés à l'interne dans le cadre des opérations quotidiennes.	Renseignements confidentiels ou qui, en raison du contexte de leur utilisation ou de leur communication, suscitent un degré d'attente raisonnable en matière de vie privée.	Renseignements personnels sensibles qui, de par leur nature, notamment médicale, biométrique ou autrement intime, suscitent un haut degré d'attente raisonnable en matière de vie privée ou dont l'utilisation ou la communication nécessitent des procédures spéciales.
Exemples	Coordonnées d'affaires, renseignements publiés au tableau de l'ordre des avocats, etc.	Renseignements qui ne permettent pas d'identifier directement une personne comme le numéro d'employé, de résident ou des statistiques démographiques.	Date de naissance, adresse postale personnelle, numéro de téléphone personnel, noms des enfants, coordonnées des contacts d'urgence, etc.	Numéro d'assurance sociale, renseignements biométriques, convictions politiques, religieuses, dossier médical, orientation sexuelle ou identité de genre.
Conséquences d'une divulgation non autorisée	Aucune	Conséquences limitées pour votre municipalité et les personnes concernées.	Conséquences négatives importantes, y compris des risques juridiques, économiques et réputationnels.	Conséquences négatives graves, y compris des risques juridiques, économiques et réputationnels.
Restriction d'accès	Aucune	Accès restreint à l'interne.	Accès accordés seulement aux personnes ayant besoin de connaître les renseignements (principe du moindre privilège).	Accès limité à des personnes autorisées identifiées, selon une liste régulièrement mise à jour.

4.3. Communication à des fins d'étude, de recherche ou de production de statistiques (Article 67.2.1)

Ces dispositions étant entrées en vigueur en septembre 2022[74], nous vous référons au Guide de conformité pour les municipalités, volume 1, section « 4. La communication de renseignements personnels sans le consentement de la personne concernée à des fins d'étude, de recherche ou de production de statistiques ». Celle-ci contient notamment un modèle d'ÉFVP que les municipalités peuvent utiliser.

4.4. Communication à des finalités autorisées (Article 68)

La Loi sur l'accès prévoit qu'à partir de septembre 2023, les exceptions à l'exigence d'obtenir un consentement pour les communications suivantes doivent faire l'objet d'une ÉFVP :

- à un organisme public ou à un organisme d'un autre gouvernement lorsque cette communication est nécessaire à l'exercice des attributions de l'organisme receveur ou à la mise en oeuvre d'un programme dont cet organisme a la gestion ;
- à un organisme public ou à un organisme d'un autre gouvernement lorsque la communication est manifestement au bénéfice de la personne concernée ;
- 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[75].

La communication ne peut alors être autorisée que si l'ÉFVP conclut que[76] :

1. L'objectif visé ne peut être atteint que si le renseignement est communiqué sous une forme permettant d'identifier la personne concernée.

> **Un renseignement personnel dépersonnalisé permet l'identification de la personne concernée (voir section 2.2.3). Ainsi, ce critère revient à se demander s'il est possible, pour atteindre l'objectif visé, de communiquer les renseignements sous une forme anonymisée (voir section 8).**

2. Il est déraisonnable d'exiger l'obtention du consentement de la personne concernée.

> La **municipalité doit démontrer que l'obtention du consentement de la personne concernée est déraisonnable dans les circonstances. Il peut s'agir, par exemple, de la difficulté de joindre un nombre élevé de personnes pour obtenir leur consentement ou encore d'entrer en contact avec les personnes concernées, notamment parce que les coordonnées de celles-ci ne sont pas connues.**

3. L'objectif pour lequel la communication est requise l'emporte, eu égard à l'intérêt public, sur l'impact de la communication et de l'utilisation du renseignement sur la vie privée de la personne concernée.

> **Ce critère de proportionnalité implique d'évaluer les bienfaits appréhendés de la communication des renseignements personnels par rapport au niveau de risque que cela pourrait engendrer sur la vie privée des personnes concernées.**

4. Le renseignement personnel est utilisé de manière à en assurer la confidentialité.

> **La personne ou l'organisme qui reçoit les renseignements personnels doit être en mesure de démontrer qu'il met en place toutes les mesures de protection et de sécurité nécessaires pour en assurer la confidentialité. Il doit également accepter de mettre en place les mesures souhaitées par l'organisme public qui communique les renseignements personnels. D'ailleurs, les mesures de sécurité propres à assurer la protection des renseignements personnels doivent être prévues dans l'entente écrite.**

Une entente doit encadrer cette communication, dont le contenu statutaire est prévu dans la Loi sur l'accès[77].

- Pour en savoir plus, consulter le site internet du SRIDAIL.
- Si vous souhaitez consulter un modèle plus détaillé, vous pouvez vous référer au premier volume du guide (Annexe 4-A), étant donné la similarité des critères des ÉFVP prévus par la Loi sur l'accès, avec les adaptations nécessaires.

4.5. Collecte en collaboration avec un autre organisme public

Les municipalités devront également réaliser une ÉFVP si elles recueillent des renseignements personnels nécessaires à l'exercice de leurs attributions ou à la mise en oeuvre d'un programme d'un organisme avec lequel ils collaborent pour la prestation de services ou pour la réalisation d'une mission commune[78]. [NTD : confirmer si ce cas de figure pourrait s'appliquer aux municipalités] Une telle collecte doit faire l'objet d'une entente écrite transmise à la CAI[79]. L'entente entre en vigueur 30 jours après sa réception par la CAI. La Loi sur l'accès prévoit le contenu obligatoire de l'entente :

- L'identification de la municipalité qui recueille le renseignement et celle de l'organisme public pour lequel la collecte est effectuée ;
- Les fins auxquelles le renseignement est recueilli ;
- La nature ou le type de renseignement recueilli ;
- Les moyens par lesquels le renseignement est recueilli ;
- Les mesures propres à assurer la protection du renseignement personnel ;
- La périodicité de la collecte ;
- La durée de l'entente[80].

Les municipalités devront donc s'assurer que leurs modèles d'entente prévoient ce contenu obligatoire (et non dans les annexes).

5. Impartition

Contrairement à son pendant du secteur privé, la Loi sur l'accès autorisait déjà les organismes publics à communiquer des renseignements personnels à un tiers sans le consentement de la personne concernée dans le cadre d'un mandat ou d'un contrat de services ou d'entreprise[81]. Cette exception au consentement demeure avec la Loi 25, mais elle est assujettie à une obligation de transparence au moment de la collecte (discutée à la section 2.1.1).

En effet, cette exception permet aux municipalités de transmettre des renseignements personnels à des mandataires et fournisseurs de services sans obtenir de consentement particulier à cet effet.

Comme mentionné dans la section 4.1, lorsque les services d'un fournisseur sont retenus dans le cadre de l'acquisition, le développement ou la refonte d'un système d'information ou d'une prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels, la municipalité doit, avant toute chose, procéder à une ÉFVP[82]. Si la responsabilité de réaliser l'ÉFVP relève de la municipalité, le fournisseur devrait toutefois y collaborer.

5.1. Conditions de mise en oeuvre

De plus, la municipalité doit conclure une entente écrite avec son mandataire ou fournisseur de services[83] prévoyant :

- Les dispositions de la Loi sur l'accès que l'autre partie s'engage à respecter ;
- Des mesures de sécurité (physiques, organisationnelles et techniques) permettant d'assurer la protection du caractère confidentiel des renseignements personnels communiqués ;
- Que l'autre partie ne peut utiliser les renseignements que dans le cadre de l'exécution de son mandat ou du contrat. L'entente devrait donc interdire à l'autre partie d'utiliser des renseignements personnels à ses fins propres ou pour les fins d'un tiers ;
- Que l'autre partie ne peut conserver les renseignements après l'expiration de l'entente.

L'autre partie doit aussi fournir un engagement de confidentialité signé par toute personne à qui les renseignements pourraient être communiqués, à moins que le RPRP estime que cela n'est pas nécessaire. Elle devra aviser sans délai le RPRP de « toute violation ou tentative de violation par toute personne de l'une ou l'autre des obligations relatives à la confidentialité du renseignement communiqué », et non simplement des incidents de confidentialité. Enfin, le RPRP de la municipalité peut effectuer toute vérification relative aux obligations de confidentialité du fournisseur, c'est-à-dire de demander tout document et effectuer toute vérification additionnelle[84].

ATTENTION d'inscrire la communication de renseignements personnels à un fournisseur de services sans le consentement dans votre registre des communications (voir la section 7).

6. Protection par défaut pour les produits ou services technologiques offerts au public disposant de paramètres de confidentialité

6.1. Protection des renseignements personnels par défaut (Privacy by Default)

Le principe de protection par défaut implique que les renseignements personnels soient automatiquement protégés sans qu'aucune action supplémentaire ne soit requise de la part d'une personne[85]. Ce principe est inspiré du principe du même nom que l'on retrouve dans le Règlement général sur la protection des données (RGPD) en Europe[86].

Par exemple, lors du téléchargement d'une application, il peut arriver qu'un message apparait pour demander l'accès aux contacts, aux photographies ou au microphone. Il s'agit alors d'une application du principe de protection par défaut, dans la mesure où la collecte des renseignements personnels est soumise à l'autorisation préalable de l'utilisatrice ou de l'utilisateur, et nécessite un opt-in[87].

Selon le texte de la Loi sur l'accès[88], l'obligation s'applique uniquement aux produits et aux services offerts au public, et non à ceux utilisés à l'interne par le personnel ou qui sont destinés à d'autres municipalités, organismes publics ou entreprises.

La protection par défaut ne s'applique pas aux paramètres de confidentialité d'un témoin de connexion (cookie)[89].

6.2. Différence avec la protection des renseignements personnels dès la conception (Privacy by Design)

Le principe de protection des renseignements personnels dès la conception implique qu'un système d'information ou une PES soit, dès la conception, respectueuse de la vie privée des utilisateurs[90]. De même que le précédent, ce principe s'inspire du principe du même nom en Europe[91].

Le SRIDAIL a mis en ligne un outil de type « aide-mémoire » pour s'assurer du respect des exigences de la Loi sur l'accès. Cela dit, le modèle d'ÉFVP fourni à la section 4 de ce guide permettra aussi de s'assurer du respect de ce principe dans le cadre d'un projet technologique.

7. Tenue de registres

En plus du registre des incidents abordé dans le volet 1, la Loi sur l'accès exige des municipalités qu'elles tiennent les registres suivants :

Type de registre	Contenu du registre
Registre des communications de renseignements personnels sans le consentement	
1. Lorsque la municipalité communique l'identité d'une Personne concernée à une personne ou à un organisme privé afin de recueillir des renseignements déjà colligés par ces derniers. **2. Lorsque la Municipalité communique des Renseignements personnels nécessaires à l'application d'une loi au Québec, que cette communication soit ou non expressément prévue par la loi.** **3. Lorsque la municipalité communique des renseignements personnels nécessaires à l'application d'une convention collective, d'un décret, d'une ordonnance, d'une directive ou d'un règlement qui établit les conditions de travail.** **4. Lorsque la municipalité communique des renseignements personnels à un mandataire ou à un fournisseur de services dans le cadre d'un mandat ou d'un contrat de services.** **5. Lorsque la municipalité communique des renseignements personnels à des fins d'étude, de recherche ou de statistique.** **6. Après avoir effectué une ÉFVP, lorsque la municipalité communique des renseignements personnels dans les cas visés par l'article 68.**	• La nature ou le type de renseignement communiqué. • La personne ou l'organisme qui reçoit cette communication. • La fin pour laquelle ce renseignement est communiqué et l'indication, le cas échéant, qu'il s'agit d'une communication de renseignements personnels à l'extérieur du Québec. • La raison justifiant cette communication.
Registre des ententes de collecte conclues avec un autre organisme public[92]	
	• Le nom de l'organisme pour lequel les renseignements sont recueillis. • L'identification du programme ou de l'attribution pour lequel les renseignements sont nécessaires. • La nature ou le type de la prestation de service ou de la mission. • La nature ou le type de renseignements recueillis. • La fin pour laquelle ces renseignements sont recueillis. • La catégorie de personnes, au sein de l'organisme qui recueille les renseignements et au sein de l'organisme receveur, qui a accès aux renseignements.
Registre des utilisations de renseignements personnels à des fins secondaires[93]	
	• La mention du paragraphe du deuxième alinéa de l'art. 65.1 de la Loi permettant l'utilisation, c'est-à-dire la base juridique applicable. • Dans le cas visé à l'art. 65.1 al. 2(3) de la Loi, la disposition législative qui rend nécessaire l'utilisation du renseignement. • La catégorie de personnes qui a accès aux renseignements aux fins de l'utilisation indiquée.

8. Destruction et anonymisation

Lorsque les fins pour lesquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, les municipalités devront le détruire ou l'anonymiser pour l'utiliser à des fins d'intérêt public, sous réserve de la *Loi sur les archives*[94].

Selon la *Loi sur les archives* :

> Tout organisme public doit établir et tenir à jour un calendrier de conservation qui détermine les périodes d'utilisation et les supports de conservation de ses documents actifs et semi-actifs et qui indique quels documents inactifs sont conservés de manière permanente et lesquels sont éliminés[95].

La conservation, l'archivage et la destruction doivent donc être réalisées selon le calendrier de conservation que la municipalité propose et soumet à Bibliothèque et Archives nationales du Québec (« **BAnQ** ») [96]. BAnQ a publié en 2022 un Recueil des règles de conservation du secteur municipal et plan de classification pour guider les municipalités dans l'élaboration de leur calendrier de conservation, pour remplacer celui de 2014. Par ailleurs, les municipalités devraient déjà avoir une politique de gestion des documents actifs et semi-actifs[97], ainsi qu'une politique sur les documents inactifs[98].

> Ainsi, les municipalités pourraient devoir mettre à jour leurs politiques et calendrier de conservation afin de se mettre en conformité avec la Loi sur l'accès[99] – tout en gardant en tête que la Loi sur les archives a préséance sur la Loi sur l'accès en matière de conservation et destruction[100]. En effet, rappelons notamment que l'aliénation ou l'élimination de documents actifs ou semi-actifs d'une municipalité ne peut être réalisée que si le calendrier de conservation le permet[101]. Si le calendrier ne prévoit rien, un document actif ou semi-actif devrait donc être conservé en l'état.

Quant à la possibilité d'anonymiser un renseignement prévue à l'article 73, lorsqu'elle serait permise selon la Loi sur les archives, encore faut-il qu'elle soit réalisée à des fins d' « intérêt public », c'est-à-dire à l'avantage de l'ensemble de la population et qui profite à la société en général. Si ces deux conditions préliminaires sont remplies, les techniques utilisées doivent alors permettre de respecter les critères prévus à l'article 73, qui tournent autour de l'irréversibilité de la technique utilisée, un seuil difficile à atteindre :

Un renseignement sera anonymisé lorsqu'il est, en tout temps, raisonnable de prévoir dans les circonstances qu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement cette personne.

Les renseignements anonymisés en vertu de la Loi sur l'accès doivent l'être selon les meilleures pratiques généralement reconnues et selon les critères et modalités déterminés par règlement.

Dans l'attente du règlement visant à préciser les critères qu'un procédé d'anonymisation doit suivre, le SRIDAIL reprend les trois critères repris du mémoire de la CAI sur la Loi 25[102]. Ainsi, le processus d'anonymisation choisi devrait notamment respecter les trois critères suivants[103] :

Individualisation	**Il ne doit pas être possible d'isoler une personne ni de l'identifier directement ou indirectement.**
Corrélation	**Il ne doit pas être possible de relier des ensembles de données distincts qui concernent une même personne.**
Inférence	**Il ne doit pas être possible de déduire de nouvelles informations sur une personne.**

De plus, les mesures doivent être constamment revues à la lumière de l'évolution des technologies actuelles et raisonnablement prévisibles, pour s'assurer qu'elles continuent d'être irréversibles à travers le temps. Ainsi, si une technique d'anonymisation permet aujourd'hui d'atteindre le seuil d'anonymisation fixé par la loi, des tests réguliers devraient être réalisés afin d'évaluer les risques de réidentification des personnes concernées à travers le temps[104].

Un renseignement anonymisé n'est plus considéré un renseignement personnel et n'est donc plus soumis aux obligations de protection des renseignements personnels prévues par la Loi sur l'accès.

Pour en savoir plus, consulter la page informative du SRIDAIL sur l'anonymisation.

Un renseignement sera anonymisé lorsqu'il est, en tout temps, raisonnable de prévoir dans les circonstances qu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement cette personne.

Les renseignements anonymisés en vertu de la Loi sur l'accès doivent l'être selon les meilleures pratiques généralement reconnues et selon les critères et modalités déterminés par règlement.

9. Conséquences en cas de non-conformité

La Loi 25 crée deux catégories de sanctions en cas de non-conformité :

Infractions moins graves (art. 158)	Infractions plus graves (art. 159)
• Jusqu'à 10 000 $ dans le cas d'une personne physique	• Jusqu'à 100 000 $ dans le cas d'une personne physique
• Jusqu'à 30 000 $ dans les autres cas	• Jusqu'à 150 000 $ dans les autres cas

En cas de récidive, les amendes seront portées au double[105]. Enfin, la CAI devra intenter toute poursuite pénale dans un délai de cinq ans suivant la perpétration de l'infraction[106]. **Afin de déterminer le montant à imposer, le juge devra tenir compte des facteurs suivants :**

- La nature, la gravité, le caractère répétitif et la durée de l'infraction ;
- La sensibilité des renseignements personnels concernés par l'infraction ;
- Le fait que le contrevenant ait agi intentionnellement ou ait fait preuve de négligence ou d'insouciance ;
- Le caractère prévisible de l'infraction ou le défaut d'avoir donné suite aux recommandations ou aux avertissements visant à la prévenir ;
- Les tentatives du contrevenant de dissimuler l'infraction ou son défaut de tenter d'en atténuer les conséquences ;
- Le fait que le contrevenant ait omis de prendre des mesures raisonnables pour empêcher la perpétration de l'infraction ;
- Le fait que le contrevenant, en commettant l'infraction ou en omettant de prendre des mesures pour empêcher sa perpétration, ait accru ses revenus ou ait réduit ses dépenses, ou avait l'intention de le faire ;
- Le nombre de personnes concernées par l'infraction et le risque de préjudice auquel ces personnes sont exposées[107].

Notons que l'adverbe « sciemment » a été retiré des art. 158 et 159. Désormais, le poursuivant n'aura plus à prouver qu'un contrevenant avait l'intention de commettre une infraction.

Infractions et manquements	art. 158	art. 159
Refuser ou entraver l'accès à un document ou à un renseignement accessible en vertu de la loi, notamment en détruisant, modifiant ou cachant le document ou en retardant indûment sa communication.	●	
Refuser ou entraver l'accès à un document ou à un renseignement accessible en vertu de la loi, notamment en détruisant, modifiant ou cachant le document ou en retardant indûment sa communication.	●	
Donner accès à un document dont la loi ne permet pas l'accès ou auquel un organisme public, conformément à la loi, refuse de donner accès.	●	
Informer une personne de l'existence d'un renseignement dont elle n'a pas le droit d'être informée en vertu de la loi.	●	
Entraver l'exercice des fonctions du responsable de l'accès aux documents ou de la protection des renseignements personnels.	●	
Recueillir, utiliser, conserver ou détruire des renseignements personnels en contravention à la loi.	●	
Omettre de déclarer, s'il est tenu de le faire, un incident de confidentialité à la Commission ou aux personnes concernées.	●	
Communiquer des renseignements personnels en contravention à la loi.		●
Entraver le déroulement d'une enquête, d'une inspection ou l'instruction d'une demande par la CAI.		●
Procéder ou tenter de procéder à l'identification d'une personne physique à partir de renseignements dépersonnalisés sans l'autorisation de l'organisme public qui les détient, ou à partir de renseignements anonymisés.		●
Refuser ou négliger de se conformer, dans le délai fixé, à une demande de production de documents émise par la CAI.		●
Contrevenir à une ordonnance de la CAI.		●
Ne pas prendre les mesures de sécurité propres à assurer la protection des renseignements personnels conformément à l'article 63.1 de la Loi sur l'accès.		●

[1] L.Q. 2021, c. 25.
[2] RLRQ, c. A-2.1.
[3] RLRQ, c. P-39.1.
[4] Loi sur l'accès, préc., note 2, art. 54.
[5] Le concept sera abordé dans la section 2.2.3.
[6] Id., art. 64.
[7] SRIDAIL, « Informations à transmettre lors d'une collecte de renseignements personnels par un organisme public ». Il doit exister un lien rationnel avec la collecte du renseignement, l'atteinte à la vie privée doit être minimisée (il n'existe pas d'autre moyen efficace moins intrusif pour répondre à la finalité), la divulgation du renseignement personnel serait nettement plus utile à la municipalité que préjudiciable à la personne concernée.
[8] Loi sur l'accès, art. 53.1 al. 2 et 64.1. Ceci est un enjeu d'actualité puisque la CAI a publié en décembre 2022 un rapport sur la protection des renseignements personnels des jeunes dans l'environnement numérique, en ligne.
[9] Loi sur l'accès, préc., note 2, art. 65 (version courante et version modifiée).
[10] Nous verrons cependant que l'exigence d'activation des fonctions permettant l'identification, la localisation ou le profilage est une forme de consentement à la collecte, cela dit.
[11] Loi sur la protection des renseignements personnels et les documents électroniques, LC 2000, c. 5 [LPRPDE].
[12] Loi sur l'accès, préc., note 2, art. 65 (version courante et version modifiée).
[13] Cependant, la municipalité est tenue d'aviser dès que possible la Commission d'accès à l'information du titre, des coordonnées et de la date d'entrée en fonction de la personne qui exerce la fonction de responsable de l'accès aux documents et ceux de la personne qui exerce la fonction de responsable de la protection des renseignements personnels, en vertu de l'art. 8 al. 4.
[14] Loi sur l'accès, préc., note 2, art. 65.0.1.
[15] Id., art. 63.7, voir l'exception pour les témoins de connexion.
[16] Id., art. 65.0.1 ; Loi sur le privé, préc., note 3, art. 8.
[17] RLRQ c. C-1.1.
[18] Id., art. 1.
[19] Id.
[20] Id.
[21] Loi sur l'accès, préc., note 2, art. 65.0.1.
[22] LCCJTI, préc., note 17, art. 43 al. 2.
[23] LCCJTI, préc., note 17, art. 44 et 45.
[24] Loi sur l'accès, préc., note 2, art. 63.5.
[25] LCCJTI, préc., note 23, art. 45 al. 1.
[26] Id., art. 44 al. 1.
[27] Id., art. 44 al. 1.
[28] Voir Plainte à l'endroit du « Marché d'alimentation Marcanio et fils inc. », dossier n°1013956-S, 14 janvier 2021 (CAI)).
[29] Loi sur l'accès, préc., note 2, art. 65 et 65.0.2. L'art. art. 53.1 s'appliquera également au système biométrique en cause.
[30] Id., art. 65.1.
[31] Id., art. 44 al. 2.
[32] Loi sur l'accès, préc., note 2, art. 63.1.
[33] CAI, Rapport Rétablir l'équilibre de 2016
[34] Loi sur l'accès, préc., note 2, art. 73.
[35] (voir Enquête à l'égard de Héritage Ébénisterie Architecturale inc.).
[36] (quebec.ca).
[37] (quebec.ca).
[38] Id.
[39] Loi sur l'accès, préc., note 2, art. 65.2 ; quebec.ca).
[40] Id., art. 63.4.
[41] Loi sur l'accès, préc., note 2, art. 65.2.
[42] Loi sur l'accès, préc., note 2, art. 53.1.
[43] Id., art. 53.1 al. 4.
[44] Id., art. 53.1 al. 1.
[45] Id., art. 65.0.1. Une municipalité peut s'appuyer sur le consentement présumé à l'utilisation et à la communication des renseignements dans la mesure où elle respecte les obligations de transparence, art. 65 Loi sur l'accès.
[46] Voir, par ex., art. 65.1.
[47] Id., art. 65.1 al. 3.
[48] Id., art. 65.1. al. 2.
[49] Id., art. 65.1. al. 5.
[50] Id., art. 65.1 al. 6.
[51] Id., art. 65.1 al. 3.
[52] Id., art. 65.1 al. 1.
[53] Id.
[54] Id., art. 59 in fine.
[55] Id., art. 65.2.
[56] Loi sur l'accès, préc., note 2, art. 83.
[57] Id., art. 84 al. 3.
[58] Code civil du Québec, art. 37 ; Loi sur le privé, préc., note 3, art. 4-5 ; Loi sur l'accès, préc., note 2, art. 64.
[59] Loi sur l'accès, préc., note 2, art. 72.
[60] Id., art. 88.0.1 (non encore en vigueur).
[61] Id., art. 89.
[62] Id., art. 98, sous réserve des exceptions prévues à cet article.
[63] Id., art. 100.
[64] Id., art. 65.
[65] Id., art. 100.
[66] Id.
[67] Guide CAI ÉFVP.
[68] Loi sur l'accès, préc., note 2, art. 63.5.
[69] (quebec.ca).
[70] (quebec.ca).
[71] Loi sur l'accès, préc., note 2, art. 59 al. 2).
[72] Id., art. 68 al. 1 par. 1(1).
[73] Id., art. 70.1. al. 4 référant au chapitre III de la Loi sur le ministère des Relations internationales, RLRQ, c. M-25.1.1 ou à une communication prévue à l'article 133 de la Loi sur la santé publique, RLRQ, c. S-2.2.
[74] Id., art. 67.2.1. à 67.2.3.
[75] Id., art. 68 al. 1 par. 1.1 à 3 et al. 2.
[76] Id., art. 68 al. 2.
[77] Id., art. 68 al. 3.
[78] Id., art. 64 al. 2.
[79] Id., art. 64 al. 3.
[80] Id., art. 64 al. 4.
[81] Id., art. 67.2.
[82] Id., art. 63.5 al. 1.
[83] Ces obligations ne s'appliquent pas si le fournisseur ou le mandataire est un autre organisme public ou le membre d'un ordre professionnel, Id., art. 67.2 al. 3.
[84] Id., art. 67.2.
[85] Id., art. 63.7 ; quebec.ca.
[86] RGPD, art. 25.
[87] quebec.ca.
[88] Loi sur l'accès, préc., note 2, art. 63.7.
[89] Id.
[90] Id., art. 63.5.
[91] (art. 25 du RGPD).
[92] Loi sur l'accès, préc. note 2, art. 67.3
[93] Au sein de la municipalité à d'autres fins et sans le consentement de la Personne concernée lorsque cette utilisation est compatible avec les fins pour lesquelles ils ont été recueillis, qu'elle est clairement à l'avantage de la Personne concernée ou qu'elle est nécessaire à l'application d'une loi au Québec.
[94] Les municipalités sont soumises à la Loi sur les archives, RLRQ, c. A-21.1 ; art. 73 Loi sur l'accès.
[95] (art. 7 de la Loi sur les archives ; l'article 2 prévoit quant à lui les définitions de documents actifs, inactifs et semi-actifs.
[96] (art. 8 al. 3 de la Loi sur les archives).
[97] (art. 6 Loi sur les archives).
[98] (art. 14 Loi sur les archives).
[99] Loi sur l'accès, préc., note 2, art. 73.
[100] Id.
[101] (art. 13 Loi sur les archives).
[102] Mémoire, p. 12, reprenant elle-même un document de la Commission Nationale informatique et libertés (CNIL) en France.
[103] quebec.ca.
[104] Pour un exemple de preuve de l'existence de risques de réidentification dans le secteur public, voir Shiab c. Régie de l'assurance maladie du Québec (RAMQ), 2023 QCCAI 30.
[105] Loi sur l'accès, préc., note 2, art. 164.1.
[106] Id., art. 164.2.
[107] Id., art. 160.

UMQ

La voix des GOUVERNEMENTS de proximité