

# POLITIQUE DE CONFIDENTIALITE

Municipalité de St-Elphège

(la « Municipalité »)

## RÉSOLUTION DU CONSEIL MUNICIPAL

### ADOPTION DE LA POLITIQUE DE CONFIDENTIALITE

**CONSIDERANT** l'importance pour la Municipalité d'assurer la protection des renseignements personnels qu'elle détient en toute transparence :

**CONSIDERANT** 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 :

**CONSIDERANT** 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.

#### EN CONSÉQUENCE

#### RÉSOLUTION : 2023-102

Il est proposé par M. Stefano Gianoli, appuyé en cela par Mme Myriam Normandin et 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

**Adoptée à l'unanimité**

## 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<sup>42</sup> pour être valide :

<b>MANIFESTE</b>	Evident, certain et indiscutable et qu'il ne doit laisser aucun doute quant à la volonté qui y est exprimée.
<b>LIBRE</b>	Donne sans contrainte. Ce critère ne serait pas satisfait si, par exemple, le consentement résultait d'une pression exercée sur la personne concernée.
<b>ECLAIRE</b>	Qui permet à la personne concernée de donner son consentement en toute connaissance de cause.
<b>DONNE À DES FINS SPECIFIQUES</b>	Demande 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.
<b>D'UNE DURÉE NECESSAIRE À LA RÉALISATION DES FINS AUXQUELLES IL A ÉTÉ DEMANDÉ</b>	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<sup>43</sup>. Un consentement qui n'est pas donné conformément à la Loi sur l'accès est sans effet<sup>44</sup>.

## 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<sup>45</sup>. Ainsi, sauf dans les cas où la Loi sur l'accès autorise l'utilisation (et la communication) sans consentement<sup>46</sup>, 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

La 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<sup>47</sup>.**

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<sup>48</sup>.

**Un renseignement personnel est « dépersonnalisé » lorsqu'il ne permet plus d'identifier directement la personne concernée<sup>49</sup>. 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<sup>50</sup>.**

## 2) Le consentement des personnes concernées a été obtenu

Si la 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<sup>52</sup>. 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<sup>53</sup>. 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<sup>54</sup>.**

### 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<sup>55</sup>. 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, la municipalité devra 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 et réaliser une EFVP (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 :

Lorsqu'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 EFVP (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<sup>56</sup>.

#### 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 structure et couramment utilisé. 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<sup>57</sup>.

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 la 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<sup>58</sup>.

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<sup>59</sup>.

**Selon le SR/DAIL, « 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 structure 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.

<sup>4</sup> Selon le SR/DAIL, un format est dit « structure 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 • la municipalité peut 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<sup>60</sup>.

Lorsqu'elle souhaite mettre en œuvre 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'EFVP 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 structure 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<sup>61</sup>.

**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<sup>62</sup>. 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<sup>63</sup>.

### 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<sup>64</sup>. Il faudra attendre des lignes directrices de la CAI ou du SRIDAIL quant à la manière dont ce droit sera mis en œuvre, 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<sup>65</sup>. Cette motivation doit permettre au requérant de comprendre le refus pour chacun des renseignements ou des documents visés<sup>66</sup>.

**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. Evaluation des facteurs relatifs à la vie privée

Une EFVP 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<sup>67</sup>. 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'EFVP 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'EFVP 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 EFVP 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 EFVP, la municipalité doit sensibiliser leur personnel et peut 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.

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'acquies, 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, la municipalité devra procéder à une EFVP<sup>68</sup>.

En principe, l'obligation de faire une EFVP 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 vise, le Comité peut suggérer:

- de nommer une personne pour mettre en œuvre 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).