Politique de confidentialité

Résolution 2023-09-253

Ville d'Amqui

Table des matières

CONSIDÉRANT que la Ville d'Amqui s'engage à protéger la confidentialité et la sécurité des renseignements personnels de ses citoyens et autres partenaires;

CONSIDÉRANT que cette politique s'adresse directement aux citoyens et autres partenaires de la Ville d'Amqui;

EN CONSÉQUENCE, il est proposé par Mme Sarah-Josée Fournier, appuyé par Mme Elaine A. Guilbault, et résolu unanimement que la Ville d'Amqui adopte la présente procédure :

1. Préambule

La Ville d'Amqui 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.

2. Modalités

2.1. Foires aux questions

COMMENT : Lorsque vous naviguez sur notre site Web, 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 :

- Vous inscrivez à un cours ou un événement via notre plate-forme de réservation;
- Déposez une demande de permis et certificat;
- Procédez à un paiement en ligne.

Quels renseignements recueillons-nous et pourquoi?

Nous ne recueillons que les renseignements personnels dont nous avons besoin pour offrir nos services municipaux (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).

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 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.

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.

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.

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.

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? »

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.

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.

Pour exercer vos droits, écrivez-nous à l'adresse greffe@amqui.ca. Nous pourrions vous demander une pièce d'identité pour nous assurer qu'il s'agit bien de vous.

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 : greffe@amqui.ca

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 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.

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 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. Un consentement qui n'est pas donné conformément à la Loi sur l'accès est sans effet. Afin de s'assurer de la mise en œuvre 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. Ainsi, sauf dans les cas où la Loi sur l'accès autorise l'utilisation (et la communication) sans consentement, 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);
- 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.

Un renseignement personnel est « dépersonnalisé » lorsqu'il ne permet plus d'identifier directement la personne concernée. 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. 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.

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. 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. 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.

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. 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.

À la demande de la personne visée par une décision automatisée, la Ville d'Amqui 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 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.

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 utilisé4, 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.

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 fournis 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.

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 à ce qu'ils soient à jour, exacts et complets pour servir aux fins pour lesquelles ils sont recueillis ou utilisés.

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.
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.

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'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 loi61.

L'article 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. Lorsqu'il refuse l'accès, elle doit en expliquer les raisons à la personne concernée et indiquer la disposition de la Loi sur laquelle ce refus s'appuie.

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. 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.

L'article 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. »

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. Cette motivation doit permettre au requérant de comprendre le refus pour chacun des renseignements ou des documents visés.

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 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. 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 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.

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 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 qu'il ne soulève pas des difficultés pratiques sérieuses (voir la section 3.1.1).

5. Entrée en vigueur

La présente politique entre en vigueur dès son adoption et remplace toute autre politique ou pratique.