Politique sur l'accès aux documents de la Société et sur la protection des renseignements personnels

DATE DE MISE À JOUR

2025-06-11

RÉSUMÉ

En tant qu'organisme public, la Société de l'assurance automobile du Québec (Société) doit appliquer la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (ci-après désignée « *Loi sur l'accès* »). La présente politique décrit les obligations et responsabilités découlant de la *Loi sur l'accès* et des règlements afférents de même que les différentes responsabilités administratives à l'intérieur de l'organisation.

BUT

Cette politique vise à assurer une application uniforme des obligations et responsabilités découlant de la *Loi sur l'accès* ainsi que le respect des cadres législatifs, réglementaires et administratifs applicables en matière d'accès et de protection des renseignements personnels. L'ensemble du personnel de la Société est concerné, de même que les ressources externes et les mandataires, puisque les obligations et responsabilités ne sont pas dévolues uniquement à la personne responsable de l'accès aux documents et de la protection des renseignements personnels. Cette politique vise ainsi à maintenir l'implication continue de tous et de toutes et décrit les obligations et responsabilités qui incombent à chaque personne.

CHAMP D'APPLICATION

Cette politique s'adresse à l'ensemble du personnel de la Société, de même qu'aux ressources externes et aux mandataires dans le cadre de leurs mandats respectifs.

Elle s'applique à l'information détenue et utilisée par la Société dans l'exercice de ses fonctions, que sa conservation soit assurée par la Société ou par un tiers, et ce, durant tout son cycle de vie. Elle s'applique aussi quelle que soit la nature de l'information ou la forme des documents : écrite, graphique, sonore, visuelle, informatisée, etc.

Cette politique vise tous les renseignements personnels détenus par la Société : ceux portant sur la clientèle, sur l'ensemble de son personnel, ainsi que sur de tierces personnes.

PRÉALABLES

- Répertoire des pouvoirs délégués (Réf. : 10.04.0)
- Politique sur la sécurité de l'information (Réf. : 37.01.0)
- Politique sur la gestion documentaire (Réf. : 53.01.0)

DÉFINITIONS

Consentement

Il doit être manifeste, libre et éclairé, puis être donné à des fins spécifiques. Il doit être manifesté de façon expresse dès qu'il s'agit d'un renseignement personnel sensible. Ce consentement ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé.

- Manifeste : évident, certain et qui démontre la volonté réelle de la personne concernée;

- Libre : exprimé sans conditions, contraintes, menaces ou promesses;
- Éclairé : formulé en ayant conscience de sa portée;
- Spécifique : autorisant la communication d'un renseignement personnel donné, à des personnes données, à des fins données et à un moment donné;
- Durée limitée : valide pour la durée requise à la réalisation des fins pour lesquelles il est demandé.

Décision fondée exclusivement sur un traitement automatisé

Signifie qu'aucune personne physique n'a exercé un contrôle important dans la décision, notamment, lorsque la décision est prise avec des paramètres logiques programmés dans le système par une personne physique.

Incident de confidentialité

Tout accès, utilisation ou communication non autorisés par une loi à un renseignement personnel, de même que sa perte ou toute autre forme d'atteinte à sa protection.

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.

Renseignement anonymisé

Un renseignement concernant une personne physique est 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 la personne concernée. Le terme « irréversible » implique qu'il ne doit pas être possible, au moment de l'anonymisation et en tout temps, et ce, en considérant un futur prévisible, d'identifier de nouveau la personne concernée directement ou indirectement.

Renseignement dépersonnalisé

Un renseignement personnel est dépersonnalisé lorsque ce renseignement ne permet plus d'identifier directement la personne concernée. La dépersonnalisation consiste à retirer tous les renseignements qui permettent l'identification directe de la personne concernée, notamment les renseignements identificatoires.

Les renseignements dépersonnalisés demeurent des renseignements personnels, car l'identification indirecte de la personne concernée est toujours possible. Cela peut se faire, par exemple, en combinant différents renseignements sur une personne, tels son sexe, son âge ou son code postal.

Renseignement personnel

Tout renseignement qui concerne une personne physique ou sa vie privée et qui permet de l'identifier directement ou indirectement, même ceux que la Société a créés. Par exemple : numéro d'assurance sociale, numéro d'assurance maladie, nom, date de naissance, numéro d'identification personnelle, numéro de réclamation, état civil, adresse personnelle, numéro de téléphone, adresse courriel personnelle ainsi que transactions effectuées au dossier d'une personne physique et confirmation de l'existence ou de l'exactitude d'un renseignement personnel.

Un renseignement personnel est considéré comme sensible lorsque, de par sa nature notamment médicale, biométrique ou autrement intime, ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de vie privée.

Renseignement personnel de nature biométrique

Il y a trois grandes catégories de renseignement personnel de nature biométrique : morphologique, comportementale et biologique. La biométrie morphologique regroupe notamment, mais pas exclusivement, la reconnaissance des empreintes digitales ainsi que la reconnaissance de la forme de la main, du visage, de la rétine et de l'iris de l'œil. La biométrie comportementale est basée sur l'analyse de certains comportements d'une personne, par exemple le tracé de sa signature, l'empreinte de sa voix, sa démarche ou sa façon de taper sur un clavier, tandis que la biométrie biologique est basée sur l'analyse des traces biologiques d'une personne, comme l'ADN, le sang ou la salive.

PRINCIPES GÉNÉRAUX

En tant qu'organisme assujetti à la *Loi sur l'accès*, la Société, ses ressources externes et ses mandataires doivent respecter les différentes obligations édictées notamment par cette loi, soit :

- adopter une attitude de transparence et d'uniformité en matière d'accès aux documents administratifs de la Société;
- protéger la confidentialité des renseignements personnels détenus par la Société, et ce, tout au long de leur cycle de vie;
- garantir de façon uniforme l'exercice des droits reconnus aux citoyens par la *Loi sur l'accès* en ce qui a trait aux renseignements personnels que la Société détient.

De plus, la Société souhaite encadrer davantage les projets technologiques impliquant des renseignements personnels de nature biométrique en raison de la sensibilité des renseignements personnels en cause; c'est pourquoi certaines précisions portant sur les renseignements de cette nature ont été apportées dans la présente politique.

PRINCIPES DIRECTEURS

Voici les obligations imposées notamment par la *Loi sur l'accès* ou les règlements afférents :

1. Application générale;
2. Accès aux documents administratifs de la Société;
3. Protection des renseignements personnels.

1. APPLICATION GÉNÉRALE

La Société doit publier la présente politique sur son site Internet et, puisqu'elle collecte certains renseignements personnels à l'aide d'un moyen technologique, elle publie également sur son site Internet une politique de confidentialité rédigée en termes simples et clairs et fait de même pour l'avis dont toute modification à cette politique doit faire l'objet.

Dans le cas où un client souhaite porter plainte ou formuler un commentaire relativement à la protection des renseignements personnels par la Société, il pourrait utiliser le processus intégré de gestion des plaintes décrit dans la Politique de gestion des plaintes et des commentaires.

Toute personne nouvellement employée par la Société reçoit une formation en éthique dans laquelle est intégré un volet sur la protection des renseignements personnels.

De plus, la personne ayant la plus haute autorité au sein d'un organisme public veille à :

- y assurer le respect et la mise en œuvre de la *Loi sur l'accès* et des règlements afférents;
- ce que la personne responsable de l'accès aux documents et de la protection des renseignements personnels exerce ses fonctions de manière autonome et à lui en faciliter l'exercice;

- la sensibilisation et à la formation des membres du personnel de la Société sur les obligations et les pratiques en matière d'accès à l'information et de protection des renseignements personnels;
- insérer dans le rapport annuel de gestion un bilan qui atteste la diffusion des documents visés par le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* et rend compte des demandes d'accès, de communication de renseignements aux personnes concernées par ceux-ci (droit d'accès, voir 3.6.1) et de rectifications, reçues et traitées. Les mesures spéciales pour faciliter l'accès lorsque la personne requérante est handicapée et les demandes ayant fait l'objet d'une demande de révision à la Commission d'accès à l'information (ci-après désignée « CAI ») doivent aussi en faire partie;
- insérer dans le rapport annuel de gestion un bilan des activités relatives à l'accès à l'information et à la protection des renseignements personnels réalisées au sein de la Société.

Par ailleurs, un comité sur l'accès à l'information et la protection des renseignements personnels, qui relève de la personne ayant la plus haute autorité, soit le président-directeur général, est chargé de soutenir la Société dans l'exercice de ses responsabilités et dans l'exécution de ses obligations en vertu de la *Loi sur l'accès* et des règlements afférents. Ce comité est aussi chargé de soutenir la Société, dans une certaine mesure, en matière de sécurité de l'information. Ce comité sur l'accès à l'information, la protection des renseignements personnels et la sécurité de l'information (ci-après désigné « CAPS ») se compose de la personne responsable de l'accès aux documents et de la protection des renseignements personnels et de toute autre personne dont l'expertise est requise, y compris la personne responsable de la sécurité de l'information et celle responsable de la gestion documentaire.

De plus, le CAPS :

- doit approuver les règles encadrant la gouvernance de la Société à l'égard des renseignements personnels, dont les mesures de protection à prendre à l'égard des renseignements personnels recueillis ou utilisés dans le cadre d'un sondage (Réf. : 04.02.7). Ces mesures comprennent une évaluation de :
  - la nécessité de recourir au sondage,
  - l'aspect éthique du sondage compte tenu, notamment, de la sensibilité des renseignements personnels collectés et de la finalité de leur utilisation;
- doit être consulté, dès le début d'un projet d'acquisition, de développement et de refonte de système d'information, de solution numérique ou de prestation électronique de services (ci-après désignée « projet technologique ») impliquant des renseignements personnels (Réf. : 04.02.8);
- peut, à toute étape d'un projet technologique, suggérer des mesures de protection des renseignements personnels applicables à ce dernier (Réf. : 04.02.8).

2. ACCÈS AUX DOCUMENTS ADMINISTRATIFS DE LA SOCIÉTÉ

2.1 Droit d'accès

Toute personne qui en fait la demande a droit d'accès aux documents administratifs d'un organisme public. Ce droit ne s'étend pas aux notes personnelles inscrites sur un document administratif ni aux esquisses, ébauches, brouillons, notes préparatoires ou autres documents de même nature.

La Société doit classer ses documents administratifs de manière à en permettre le repérage. Elle doit établir et tenir à jour une liste de classement indiquant l'ordre selon lequel les documents sont classés (plan de classification). Le plan de classification doit être suffisamment précis pour faciliter l'exercice du droit d'accès.

Il ne faut pas confondre le droit d'accès aux documents administratifs de la Société avec la communication de renseignements personnels à une personne concernée par ceux-ci (décrit au point 3.6.1).

2.2 Restrictions au droit d'accès

La règle étant l'accessibilité, si elle doit retenir un document ou des renseignements, la Société doit pouvoir le justifier en vertu d'une disposition législative prévue à la *Loi sur l'accès*.

2.3 Procédure d'accès (Réf. : 04.02.1)

3. PROTECTION DES RENSEIGNEMENTS PERSONNELS

La Société est responsable de la protection des renseignements personnels qu'elle détient. Les renseignements personnels sont, par définition, confidentiels.

Afin de limiter les incursions et les indiscrétions de l'État dans la vie privée des citoyens et de veiller à ce que les décisions qui les affectent ne soient pas motivées par des considérations étrangères aux attributions de l'organisme public qui les prend, la loi n'autorise que la collecte des renseignements personnels nécessaires à l'exercice des attributions d'un organisme ou à la mise en œuvre d'un programme dont il a la gestion. Ainsi, la Société collecte les renseignements personnels qui sont nécessaires à l'exercice de ses attributions ou à la mise en œuvre des programmes dont elle a la gestion.

Plus précisément, la Société doit être capable de démontrer que chaque renseignement personnel collecté est nécessaire pour atteindre l'objectif poursuivi (toujours dans les attributions de la Société ou pour la mise en œuvre d'un programme dont elle a la gestion). Par exemple, les renseignements personnels collectés pour délivrer un permis de conduire ne seront pas nécessairement les mêmes renseignements personnels collectés que ceux pour verser une indemnité à une personne accidentée.

La Société doit prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support. Notamment, elle doit s'assurer que les accès à ces renseignements sont limités aux seules personnes employées qui ont qualité pour prendre connaissance d'un type de renseignement précis et que celles-ci n'y accèdent que dans le cadre de leurs fonctions respectives.

Voici une description des différentes obligations :

3.1 Collecte

Quiconque, au nom de la Société, collecte un renseignement personnel auprès de la personne concernée, verbalement ou par écrit, doit l'informer :

- du nom de l'organisme public au nom de qui la collecte est faite;
- des fins pour lesquelles ce renseignement est collecté;
- du caractère obligatoire ou facultatif de la demande;
- des conséquences pour la personne concernée d'un refus de répondre à la demande;
- des droits d'accès et de rectification prévus par la loi;

Sur demande, la personne concernée est également informée :

- de la liste de l'ensemble des renseignements collectés auprès d'elle;
- des catégories de personnes qui ont accès à ces renseignements au sein de la Société;
- de la durée de conservation de ces renseignements;
- des coordonnées de la personne responsable de l'accès aux documents et de la protection des renseignements personnels.

De plus, quiconque, au nom de la Société, collecte un renseignement personnel, verbalement ou par écrit, auprès d'un tiers doit informer ce dernier :

- que la collecte est faite au nom de la Société;
- des conséquences pour la personne concernée d'un refus de répondre à la demande;
- des droits d'accès et de rectification prévus par la loi.

Un organisme public ne peut obliger une personne à établir son identité au moyen d'un procédé biométrique; pour que l'organisme puisse avoir recours à ce procédé, le consentement exprès de la personne doit être obtenu (art. 44 de la *Loi concernant le cadre juridique des technologies de l'information*).

3.2 Utilisation

Un renseignement personnel ne peut être utilisé par la Société, ou ses mandataires, qu'aux fins pour lesquelles il a été collecté, à moins d'avoir le consentement de la personne concernée. En l'absence de consentement, la Société peut toutefois utiliser un tel renseignement à d'autres fins, soit lorsque son utilisation est :

1. compatible avec celles pour lesquelles il a été collecté (ce lien doit être pertinent et direct);
2. manifestement au bénéfice de la personne concernée;
3. nécessaire à l'application d'une loi au Québec;
4. nécessaire à des fins d'étude, de recherche ou de production de statistiques et qu'il est dépersonnalisé.

La personne responsable de l'accès au document et de la protection des renseignements personnels doit inscrire les trois premières utilisations du renseignement personnel, ci-dessus, dans le registre des communications.

Par ailleurs, si la Société souhaite utiliser des renseignements personnels de nature biométrique à d'autres fins que celles pour lesquelles ils ont été collectés, cette nouvelle utilisation devra être autorisée de façon expresse par le CAPS, et ce, même s'il y a mise en place d'un consentement auprès de la personne concernée.

Advenant le cas où la Société utilisait des renseignements personnels afin que soit rendue une décision fondée exclusivement sur un traitement automatisé de ceux-ci, elle devrait en informer la personne concernée au plus tard au moment où elle l'informe de cette décision. La Société devra permettre, aux personnes qui le demandent, de comprendre la logique derrière cette décision.

3.3 Communication

La Société, ou l'un de ses mandataires, ne peut communiquer un renseignement personnel sans le consentement de la personne concernée. Le consentement d'une personne mineure de moins de 14 ans est donné par la ou le titulaire de l'autorité parentale ou par la tutrice ou le tuteur. Quant au consentement de la personne mineure de 14 ans ou plus, il est donné par cette dernière, par la ou le titulaire de l'autorité parentale ou par la tutrice ou le tuteur. Lorsqu'un consentement est obtenu, il est limité aux fins spécifiques pour lesquelles il a été demandé et pour la durée nécessaire à leur réalisation. Les renseignements personnels demeurent donc confidentiels pour tout ce qui n'est pas prévu par le consentement.

Par ailleurs, en vertu de certaines dispositions législatives prévues à la *Loi sur l'accès*, la Société, ou l'un de ses mandataires, peut communiquer un renseignement personnel sans consentement. Alors, la Société :

- effectue une évaluation des facteurs relatifs à la vie privée (ci-après désignée « EFVP »), préalablement à toute communication à une personne ou à un

organisme qui souhaite utiliser ces renseignements à des fins d'étude, de recherche ou de production de statistiques;

- effectue une EFVP et encadre certaines de ses communications de renseignements personnels par des ententes lorsque la loi l'exige ou lorsque les circonstances le justifient;
- détermine la nécessité d'obtenir un engagement de confidentialité rempli par toute personne à qui le renseignement personnel peut être communiqué en vertu d'un mandat ou d'un contrat pour la Société, et est avisée sans délai de toute violation ou tentative de violation de ces obligations.

Avant de communiquer à l'extérieur du Québec un renseignement personnel, la Société doit procéder à une EFVP. La communication peut s'effectuer si l'EFVP démontre que le renseignement bénéficierait d'une protection adéquate, notamment au regard des principes de protection des renseignements personnels généralement reconnus.

Pour toute communication de renseignements personnels de nature biométrique, une autorisation expresse du CAPS est requise.

Lorsqu'un renseignement est ainsi communiqué sans consentement, la personne responsable de l'accès aux documents et de la protection des renseignements personnels doit inscrire la communication dans un registre qu'elle tient à cette fin (registre des communications).

3.4 Incident de confidentialité

Lorsqu'une personne membre du personnel de la Société, une ressource externe ou un mandataire a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel détenu par la Société ou en son nom, cette personne ou ressource ou ce mandataire doit prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent (Procédure pour encadrer les incidents de confidentialité [Réf. : 37.01.7]). La Société doit tenir un registre des incidents de confidentialité. Si l'incident présente un risque qu'un préjudice sérieux soit causé, la Société :

- doit aviser avec diligence la CAI;
- doit aviser toute personne dont un renseignement personnel est concerné par l'incident, à moins que cela soit susceptible d'entraver une enquête faite par une personne ou un organisme qui est chargé de prévenir, de détecter ou de réprimer le crime ou les infractions aux lois;
- peut aviser toute personne ou tout organisme susceptible de diminuer ce risque, en ne lui communiquant que les renseignements personnels nécessaires à cette fin. Lorsqu'un renseignement est ainsi communiqué sans consentement, la personne responsable de l'accès aux documents et de la protection des renseignements personnels doit inscrire la communication dans un registre qu'elle tient à cette fin (registre des communications).

Lorsque la Société évalue le risque qu'un préjudice soit causé à une personne dont un renseignement personnel est concerné par un incident de confidentialité, la Société doit considérer, notamment, la sensibilité du renseignement concerné, les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables. La Société doit également consulter la personne responsable de l'accès aux documents et de la protection des renseignements personnels.

3.5 Établissement et gestion des fichiers

La Société doit établir et maintenir à jour un inventaire de ses fichiers de renseignements personnels.

La Société et ses mandataires doivent veiller à ce que les renseignements personnels qu'ils conservent soient à jour, exacts et complets pour servir aux fins pour lesquelles ils sont collectés ou utilisés.

Lorsque les fins pour lesquelles un renseignement personnel a été collecté ou utilisé sont accomplies, la Société et ses mandataires doivent :

- le détruire, sous réserve de la *Loi sur les archives* ou du *Code des professions* (pour davantage de précision sur la destruction des documents, consulter la Politique de gestion documentaire [Réf. : 53.01.0]).

  ou

- l'anonymiser, pour que le renseignement réponde à la définition de renseignement anonymisé et l'utiliser à des fins d'intérêt public. Si la Société ne perçoit pas d'avantages ou de plus-value pour l'intérêt public à conserver des renseignements personnels anonymisés, elle doit tout simplement détruire ceux-ci.

3.6 Droits de la personne concernée par un renseignement personnel

3.6.1 Droit d'accès et restrictions

Toute personne a le droit d'être informée de l'existence, dans un fichier de renseignements personnels, d'un renseignement personnel la concernant. Elle a le droit d'en prendre connaissance sur place ou à distance et d'en obtenir copie, sous réserve des restrictions prévues par la *Loi sur l'accès*. À sa demande, ce renseignement personnel lui est communiqué dans un format technologique structuré et couramment utilisé, à moins que cela ne soulève des difficultés pratiques sérieuses.

3.6.2 Droit de rectification

Toute personne qui reçoit confirmation de l'existence dans un fichier d'un renseignement personnel la concernant peut, s'il est inexact, incomplet ou équivoque, ou si sa collecte, sa communication ou sa conservation ne sont pas autorisées par la loi, exiger que le fichier soit rectifié.

3.6.3 Procédure d'accès ou de rectification (Réf. : 04.02.1)

3.7 Technologie et droit à la protection de la vie privée

La Société doit procéder à une EFVP de tout projet technologique impliquant des renseignements personnels (Réf. : 04.02.8).

Lorsque la Société offre un produit ou un service technologique impliquant des renseignements personnels, elle doit s'assurer que le plus haut niveau de confidentialité soit paramétré par défaut, sans intervention de la personne concernée. Le respect de la vie privée doit être intégré dans chaque norme, protocole et processus dès leur conception.

De plus, lorsque la Société collecte des renseignements personnels en ayant recours à une technologie comprenant des fonctions permettant de l'identifier, de la localiser ou d'effectuer un profilage de celle-ci, elle doit, au préalable, l'informer :

- lors de la collecte, des éléments inscrits à la section 3.1;
- du recours à une telle technologie;
- des moyens offerts pour activer les fonctions permettant d'identifier, de localiser ou d'effectuer un profilage.

3.7.1 Projet technologique impliquant des renseignements personnels de nature biométrique

La vice-présidence responsable du projet doit :

- justifier dès l'initiative du projet, plutôt qu'au moment de l'EFVP comme c'est le cas dans tous les autres types de projet technologique, le fait que le recours aux données biométriques est proportionnel, c'est-à-dire que :
  - le projet vise à résoudre une situation problématique, il vise donc à poursuivre un objectif important et légitime (c'est le critère de nécessité déjà décrit dans la section 3);
  - la collecte des renseignements personnels de nature biométrique permet d'atteindre cet objectif;
  - d'autres moyens portant moins atteinte à la vie privée ont été explorés et documentés, mais ont révélé l'impossibilité d'atteindre cet objectif, le cas échéant;
  - l'atteinte à la vie privée des personnes concernées et les conséquences susceptibles de résulter de la mise en place du système sont moins importantes que les avantages de l'utilisation de renseignements personnels de natures biométriques;
- faire approuver le projet par le président-directeur général dès sa création;
- présenter au CAPS, avant la phase de réalisation, toutes les mesures de protection des renseignements personnels suggérées dans l'EFVP et la façon dont elles seront mises en place;
- divulguer la création d'une banque de caractéristiques ou de mesures biométriques à la CAI au plus tard 60 jours avant sa mise en service (art. 45 de la *Loi concernant le cadre juridique des technologies de l'information*).

DIRECTIVES

RÔLES ET RESPONSABILITÉS

1. Le **président-directeur général** est le premier responsable de la protection des renseignements personnels ainsi que de sa gouvernance. Dans le cadre de la politique, il doit, par ailleurs :

- assurer le respect et la mise en œuvre de la *Loi sur l'accès* et des règlements afférents;
- s'assurer du bon fonctionnement du CAPS;
- approuver tout projet technologique impliquant des renseignements personnels de nature biométrique dès la création du projet en question;
- veiller à ce que la personne responsable de l'accès aux documents et de la protection des renseignements personnels exerce ses fonctions de façon autonome et à lui en faciliter l'exercice;
- veiller à la sensibilisation et à la formation des membres du personnel de la Société sur les obligations et les pratiques en matière d'accès à l'information et de protection de renseignements personnels;
- insérer dans le rapport annuel de gestion la reddition de comptes requise.

2. Le **CAPS** est composé du président-directeur général, de l'entièreté des membres du comité de direction, du directeur du Bureau de l'accès à l'information et de la protection des renseignements personnels (ci-après désignée « BAIPRP ») à titre de responsable de l'accès

aux documents et de la protection des renseignements personnels et de toute autre personne dont l'expertise est requise pour exercer sa fonction, notamment le vice-président à l'expérience numérique à titre de chef de la sécurité de l'information organisationnelle et de responsable de la gestion documentaire. Ce comité doit :

- approuver la présente politique de même que la politique de confidentialité;
- soutenir la Société dans l'exercice de ses responsabilités et obligations en vertu de la *Loi sur l'accès*;
- prendre connaissance du plan intégré de sensibilisation et de formation des membres du personnel de la Société portant sur les obligations et les pratiques en matière d'accès à l'information, de protection de renseignements personnels et de sécurité de l'information;
- autoriser de façon expresse toute utilisation de renseignements personnels de nature biométrique à d'autres fins que celles pour lesquelles ils ont été collectés, et ce, même s'il y a mise en place d'un consentement auprès de la personne concernée;
- autoriser de façon expresse toute communication de renseignements personnels de nature biométrique à l'extérieur de la Société;
- être consulté dès le début d'un projet technologique et déléguer cette tâche au sous-comité sur la protection des renseignements personnels lorsqu'il s'agit de projets technologiques autres que ceux impliquant des renseignements personnels de nature biométrique;
- prendre connaissance, avant la phase de réalisation d'un projet technologique impliquant des renseignements personnels de nature biométrique : de l'EFVP du projet en question et de toutes les mesures de protection des renseignements personnels qui y sont suggérées ainsi que de la documentation venant du projet et traitant de la façon dont les mesures de protection des renseignements personnels seront mises en place;
- être consulté lorsqu'un projet technologique entraîne des risques disproportionnés pour la vie privée des personnes concernées par rapport aux avantages du projet;
- prendre connaissance de la reddition de comptes reçue du sous-comité sur la protection des renseignements personnels, du responsable de l'accès aux documents et de la protection des renseignements personnels et du chef de la sécurité de l'information organisationnelle, selon la fréquence déterminée;
- suggérer au projet technologique des mesures de protection des renseignements personnels, le cas échéant.

3. Le **sous-comité sur la protection des renseignements personnels** est composé du directeur du Bureau de l'accès à l'information et de la protection des renseignements personnels à titre de responsable de l'accès aux documents et de la protection des renseignements personnels et de toute autre personne dont l'expertise est requise pour exercer sa fonction, soit : le directeur du chapitre Gouvernance, Architecture et Conception à titre de responsable de la gouvernance en sécurité de l'information, le directeur du chapitre Gouvernance et Gestion des données et de l'information à titre de responsable de la gestion documentaire et leur équipe respective.

Ce sous-comité doit soutenir le CAPS dans les projets technologiques. Ainsi le sous-comité doit :

- être consulté, dès le début d'un projet technologique impliquant des renseignements personnels;
- suggérer aux personnes responsables du projet technologique des mesures de protection des renseignements personnels, le cas échéant;
- rendre des comptes au CAPS, par l'entremise du responsable de l'accès aux documents et de la protection des renseignements personnels, selon la fréquence déterminée par le CAPS.

4. Le **vice-président aux affaires juridiques et corporatives** doit :

- faire partie du CAPS;
- approuver la section « L'accès à l'information et la protection des renseignements personnels » du rapport annuel de gestion.

5. Le **directeur du Bureau de l'accès à l'information et de la protection des renseignements personnels, à titre de responsable de l'accès aux documents et de la protection des renseignements personnels**, doit :

- exercer ses fonctions de façon autonome;
- faire partie du CAPS et faire une reddition de compte selon la fréquence déterminée par ce dernier;
- faire partie du sous-comité sur la protection des renseignements personnels;
- être le représentant de la Société auprès de la CAI et transmettre à celle-ci les documents exigés par elle-même ou la *Loi sur l'accès*;
- agir à titre de répondant dans le cadre d'une plainte adressée à la CAI contre la Société ou d'une enquête effectuée par la CAI, en collaboration avec le secteur visé;
- s'assurer que la Société publie sur son site Internet une politique de confidentialité rédigée en termes simples et clairs et fait de même pour l'avis dont toute modification à cette politique doit faire l'objet;
- offrir conseil à l'ensemble de la Société en ce qui a trait à la protection des renseignements personnels;
- contribuer au plan intégré de sensibilisation et de formation des membres du personnel de la Société sur les obligations et les pratiques en matière d'accès à l'information, de protection de renseignements personnels et de sécurité de l'information;
- être mis à contribution dans la réalisation de tout projet technologique impliquant des renseignements personnels et effectuer une EFVP;
- divulguer la création d'une banque de caractéristiques ou de mesures biométriques à la CAI au plus tard 60 jours avant sa mise en service (art. 45 de la *Loi concernant le cadre juridique des technologies de l'information*);
- effectuer, avec la collaboration du secteur concerné, une EFVP préalablement à toute communication de renseignements personnels à une personne ou à un organisme :
  - qui souhaite utiliser ces renseignements à des fins d'étude, de recherche ou de production de statistiques,
  - lorsque la loi l'exige ou lorsque les circonstances le justifient,
  - à l'extérieur du Québec. La communication peut s'effectuer si l'EFVP démontre que le renseignement bénéficierait d'une protection adéquate;
- conseiller le personnel de la Société dans le cadre de communications de renseignements personnels à des tiers, et à ce titre, valider le contenu des ententes contenant des échanges de renseignements personnels et s'assurer que les nouvelles ententes sont notées au registre des communications;
- valider les autres nouveaux éléments notés au registre des communications en l'absence de consentement et maintenir à jour le registre des communications;
- évaluer la non-nécessité d'obtenir un engagement de confidentialité rempli par toute personne à qui le renseignement personnel peut être communiqué en vertu d'un mandat ou d'un contrat pour la Société, et être avisé sans délai de toute violation ou tentative de violation de ces obligations;

- donner son avis lors de la réalisation d'un sondage qui implique la collecte, l'utilisation et/ou la communication de renseignements personnels. Cet avis doit conclure sur la nécessité de recourir au sondage;
- être avisé avec diligence lorsqu'il y a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel et, si l'incident présente un risque qu'un préjudice sérieux soit causé, aviser la CAI et s'assurer que le CAPS sera également avisé;
- conseiller la Vice-présidence à l'expérience numérique (VPEN) lors de l'évaluation du risque qu'un préjudice soit causé à une personne dont un renseignement personnel est concerné par un incident de confidentialité;
- coordonner la mise à jour de l'inventaire des fichiers de renseignements personnels;
- répondre aux demandes d'accès aux documents administratifs et offrir conseil à l'ensemble de la Société à ce sujet (Réf. : 04.02.1);
- répondre aux demandes de communication de renseignements personnels à une personne concernée par ceux-ci (droit d'accès) et aux demandes de rectification, puis offrir conseil à l'ensemble de la Société à ce sujet (Réf. : 04.02.1);
- préparer la section « L'accès à l'information et la protection des renseignements personnels » du rapport annuel de gestion.

6. La personne **responsable du Bureau-conseil en éthique** doit :

- intégrer un volet sur la protection des renseignements personnels dans la formation offerte à toute personne nouvellement employée par la Société;
- évaluer l'aspect éthique d'un sondage compte tenu, notamment, de la sensibilité des renseignements personnels collectés et de la finalité de leur utilisation.

7. Le **vice-président** dans sa gestion courante de la protection des renseignements personnels doit, selon ses attributions :

- faire partie du CAPS;
- solliciter le BAIPRP dans le cadre des projets technologiques qui impliquent des renseignements personnels, dont ceux impliquant des renseignements personnels de nature biométrique et prendre en considération les exigences spécifiques et les mesures de protection des renseignements personnels pour atténuer des risques repérés dans l'EFVP élaborée pour le projet en question;
- justifier, dès l'initiative du projet technologique impliquant des renseignements personnels de nature biométrique, plutôt qu'au moment de l'EFVP comme c'est le cas dans tous les autres types de projet technologique, le fait que le recours aux données biométriques est proportionnel, c'est-à-dire que :
    - le projet vise à résoudre une situation problématique, donc à poursuivre un objectif important et légitime;
    - la collecte des renseignements personnels de nature biométrique permet d'atteindre cet objectif;
    - d'autres moyens portant moins atteinte à la vie privée ont été explorés et documentés, mais ont révélé l'impossibilité d'atteindre cet objectif, le cas échéant;
    - l'atteinte à la vie privée des personnes concernées et les conséquences susceptibles de résulter de la mise en place du système sont moins importantes que les avantages de l'utilisation de renseignements personnels de natures biométriques;
    - consulter la personne responsable de l'accès aux documents et de la protection des renseignements personnels;

- faire approuver le projet technologique impliquant des renseignements personnels de nature biométrique par le président-directeur général dès la création du projet en question;
- transmettre au CAPS, avant la phase de réalisation d'un projet technologique impliquant des renseignements personnels de nature biométrique : l'EFVP contenant toutes les mesures de protection des renseignements personnels suggérées ainsi que la documentation liée au projet portant sur la façon dont les mesures de protections des renseignements personnels seront mises en place;
- faire des suivis ponctuels au CAPS, le cas échéant;
- obtenir l'approbation du CAPS pour toute utilisation de renseignements personnels de nature biométrique à d'autres fins que celles pour lesquelles ils ont été collectés;
- obtenir l'approbation du CAPS pour toute communication de renseignements personnels de nature biométrique à l'extérieur de la Société;
- collaborer à la rédaction de la politique de confidentialité et à ses modifications subséquentes;
- mettre en place les mesures de protection des renseignements personnels suggérés par le CAPS;
- autoriser la réalisation d'un sondage qui implique la collecte, l'utilisation et/ou la communication de renseignements personnels.

8. Le **vice-président à l'expérience numérique** doit :

- faire partie du CAPS et faire une reddition de compte selon la fréquence déterminée par ce dernier;
- mettre en place des mesures de protection des renseignements personnels suggérés par le CAPS;
- mettre en place des mesures de sécurité pour protéger les renseignements personnels détenus par la Société sur support informatique, peu importe le lieu où ils sont hébergés;
- mettre en place un processus de gestion des accès informatiques octroyés à l'ensemble du personnel de la Société, de même qu'aux ressources externes et aux mandataires. Ce processus doit permettre de s'assurer que les accès aux renseignements personnels sont limités aux seules personnes qui ont qualité pour prendre connaissance d'un type de renseignement précis et qu'elles n'y accèdent que dans le cadre de leurs fonctions respectives;
- collaborer à la mise en place ou mettre en place, selon le cas, le plus haut niveau de confidentialité « par défaut » pour chaque produit ou service technologique impliquant des renseignements personnels offert par la Société;
- mettre en place des systèmes permettant aux personnes concernées par un renseignement personnel d'en obtenir communication dans un format technologique structuré et couramment utilisé;
- contribuer au plan de sensibilisation et de formation intégré des membres du personnel de la Société portant sur les obligations et les pratiques en matière d'accès à l'information, de protection de renseignements personnels et de sécurité de l'information;
- s'il y a des motifs de croire que s'est produit un incident de confidentialité impliquant un renseignement personnel que la Société détient :
    - conseiller la personne responsable de la gestion afin qu'elle puisse prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent;
    - évaluer le risque qu'un préjudice soit causé à une personne dont un renseignement personnel est concerné par un incident de confidentialité en considérant notamment

la sensibilité du renseignement, les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables;

- consulter la personne responsable de l'accès aux documents et de la protection des renseignements personnels;

- tenir un registre des incidents de confidentialité;
- si l'incident présente un risque qu'un préjudice sérieux soit causé :
  - aviser la personne responsable de l'accès aux documents et de la protection des renseignements personnels avec diligence afin que cette dernière puisse aviser la CAI;
  - informer et conseiller la personne responsable de la gestion afin qu'elle puisse aviser toute personne concernée par l'incident, sauf dans les cas prévus à la *Loi sur l'accès*;
  - aviser s'il y a lieu toute personne ou tout organisme susceptible de diminuer ce risque, en ne lui communiquant que les renseignements personnels nécessaires à cette fin sans le consentement de la personne concernée et aviser la personne responsable de l'accès aux documents et de la protection des renseignements personnels;
  - informer le CAPS par le biais de sa reddition de comptes;
- collaborer avec le BAIPRP et les secteurs concernés lors de la mise à jour de l'inventaire des fichiers de renseignements personnels;
- fournir un environnement informatique permettant à la Société de conserver des renseignements personnels à jour, exacts et complets pour servir aux fins pour lesquelles ils sont collectés ou utilisés;
- élaborer et tenir à jour le plan de classification de la Société pour permettre la classification des documents administratifs de manière à en faciliter le repérage;
- mettre en place des mesures d'anonymisation ou de destruction sécuritaire des documents contenant des renseignements personnels, peu importe leur support ou le lieu où ils sont hébergés.

9. Le **vice-président aux affaires publiques et aux stratégies de sécurité routière** doit solliciter la VPEN pour mettre en place le plus haut niveau de confidentialité « par défaut » pour chaque produit ou service technologique offert par la Société (notamment, le site Web de la Société et les médias sociaux) impliquant des renseignements personnels.

10. Le **directeur général des ressources matérielles et immobilières** doit mettre en place des mesures de protection des locaux et des équipements pour protéger les renseignements personnels situés dans les locaux de la Société (peu importe leur support) et accompagner les gestionnaires qui souhaitent mettre en place des mesures de sécurité physiques supplémentaires limitant l'accès à des renseignements personnels aux seules personnes qui ont qualité pour en prendre connaissance et qu'elles n'y accèdent que dans le cadre de leurs fonctions;

11. Les **gestionnaires** doivent :

- s'assurer du respect de la protection des renseignements personnels conformément à la présente politique; protéger la confidentialité des renseignements personnels détenus par la Société, et ce, tout au long de leur cycle de vie, autant pour les renseignements personnels sous leur responsabilité que pour les renseignements personnels auxquels ils ont accès dans le cadre de leurs fonctions;
- faire partie du sous-comité sur la protection des renseignements personnels, selon leurs attributions;

- solliciter le BAIPRP pour tout besoin particulier de sensibilisation et de formation de son secteur en ce qui a trait à l'accès à l'information et à la protection des renseignements personnels;
- solliciter le BAIPRP dans le cadre des projets technologiques qui impliquent des renseignements personnels et prendre en considération les exigences spécifiques et les mesures de protection des renseignements personnels pour atténuer des risques repérés dans l'EFVP élaborée pour le projet en question;
- respecter les mesures de sécurité mise en place par la VPEN et prendre les mesures raisonnables, relevant de leurs attributions, propres à assurer la protection des renseignements personnels tout au long de leur cycle de vie, solliciter la Direction générale des ressources matérielles et immobilières si des mesures de sécurité nécessitant des ressources matérielles doivent être mises en place pour s'assurer que les accès aux renseignements personnels sont limités aux seules personnes qui ont qualité pour prendre connaissance d'un type de renseignement précis et qu'elles n'y accèdent que dans le cadre de leurs fonctions respectives;
- autoriser les accès propres aux fonctions de chaque membre du personnel sous leur responsabilité, les accès tant informatiques que physiques, et les mettre régulièrement à jour;
- veiller à aviser correctement, verbalement ou par écrit, les personnes auprès de qui l'on collecte des renseignements personnels. De plus, advenant le cas où la collecte était faite en ayant recours à une technologie comprenant des fonctions permettant d'identifier la personne concernée par le renseignement, de la localiser ou d'effectuer un profilage, de l'informer du recours à une telle technologie et des moyens offerts pour activer les fonctions;
- advenant le cas où des renseignements personnels seraient utilisés pour rendre une décision fondée exclusivement sur un traitement automatisé de ceux-ci, en informer la personne concernée et permettre aux personnes qui le demandent de comprendre la logique derrière cette décision;
- s'assurer que les renseignements personnels sont utilisés aux fins collectées et pour la durée requise, et qu'ils s'avèrent nécessaires à l'exercice des attributions de la Société ou à la mise en œuvre d'un programme dont elle a la gestion;
- obtenir le consentement exprès de la personne avant d'établir son identité au moyen d'un procédé biométrique;
- obtenir les consentements requis avant de divulguer des renseignements personnels ou de les utiliser à d'autres fins que celles pour lesquelles ils ont été collectés;
- solliciter le BAIPRP préalablement à toute communication à une personne ou à un organisme qui souhaite utiliser des renseignements à des fins d'étude, de recherche ou de production de statistiques et collaborer à l'EFVP, le cas échéant;
- aviser le BAIPRP lorsque des renseignements personnels sont détenus, utilisés et/ou communiqués à l'extérieur du Québec et de tout changement dans les modalités et collaborer à l'EFVP, le cas échéant;
- informer le BAIPRP de toute modification à apporter au registre des communications;
- informer la VPEN de tout incident de confidentialité impliquant un renseignement personnel détenu par la Société et suivre ses conseils pour prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé et éviter que de nouveaux incidents de même nature ne se produisent;
- être informés par la VPEN lorsque cette dernière évalue que l'incident de confidentialité présente un risque qu'un préjudice sérieux soit causé et, alors, collaborer, signer l'avis transmis à la CAI et aviser toute personne concernée par l'incident en prenant soin de se nommer, sauf dans les cas prévus à la *Loi sur l'accès*;

- alimenter le BAIPRP lors de la mise à jour de l'inventaire des fichiers de renseignements personnels sous sa responsabilité;
- veiller à ce que les renseignements personnels que la Société conserve et dont ils sont détenteurs soient à jour, exacts et complets pour servir aux fins pour lesquelles ils sont collectés ou utilisés;
- respecter les mesures de destruction sécuritaire des documents contenant des renseignements personnels mises en place;
- obtenir l'avis du BAIPRP et de la personne responsable du Bureau-conseil en éthique lors de l'élaboration de sondages collectant, utilisant et/ou communiquant des renseignements personnels;
- obtenir l'avis du BAIPRP pour tout autre questionnement concernant l'accès à l'information ou la protection de renseignements personnels;
- communiquer un renseignement personnel à la personne qui a le droit de le recevoir (répondre à une demande d'information);
- collaborer avec le BAIPRP lors des demandes d'accès aux documents administratifs, des demandes de communication de renseignements personnels (droit d'accès) et des demandes de rectification concernant son secteur;
- appliquer le plan de classification pour faciliter l'exercice du droit d'accès.

12. Le **personnel**, les **ressources externes** et les **mandataires** doivent :

- accéder uniquement aux renseignements personnels nécessaires en vertu de leurs fonctions respectives;
- aviser sans délai leur gestionnaire ou la Société, selon le cas, s'il y a des motifs de croire que s'est produit un incident de confidentialité;
- protéger les renseignements personnels auxquels ils ont accès.

RESPONSABILITÉS ADMINISTRATIVES

Le BAIPRP de la Vice-présidence aux affaires juridiques et corporatives est responsable de la conception, de la publication sur le site Internet et de la mise à jour de cette politique.