AIBQ

ASSOCIATION DES INSPECTEURS EN BÂTIMENTS DU QUÉBEC

Politique de confidentialité et protection des renseignements personnels

Dernière version approuvée par le conseil d'administration

le 23 août 2023.

Politique de confidentialité et protection des renseignements personnels

Historique des mises à jour du document

Politique approuvée par le CA le 23 août 2023 :

Table des matières

Association des inspecteurs en bâtiment du Québec - AIBQ
7811, boulevard Louis-H. Lafontaine, Bureau 204, Anjou, Québec H1K 4E4
www.aibq.qc.ca (514) 352-2427 info@aibq.qc.ca

Association des inspecteurs en bâtiment du Québec - AIBQ
7811, boulevard Louis-H. Lafontaine, Bureau 204, Anjou, Québec H1K 4E4
www.aibq.qc.ca (514) 352-2427 info@aibq.qc.ca

Politique de confidentialité[1]

1) Objectif

La présente politique traite de la gestion et de la protection des informations jugées confidentielles pour l'Association des inspecteurs en bâtiment du Québec (AIBQ). Elle traite notamment des renseignements concernant ses données, des informations liées aux activités de l'organisme et des informations concernant les membres, les membres du conseil d'administration et le personnel.

Elle poursuit les objectifs suivants :

- Assurer le respect de la vie privée des personnes et la sécurité des informations personnelles détenues par l'AIBQ;
- Se donner des balises concernant les échanges d'informations tant à l'intérieur qu'à l'extérieur des locaux de l'organisme.

2) Portée

La présente politique s'applique à l'ensemble du personnel de l'AIBQ, aux membres, aux administrateurs, aux vérificateurs et à tous les niveaux hiérarchiques, notamment dans les lieux et contextes suivants :

- Les lieux de travail, incluant les lieux de télétravail le cas échéant;
- Tout autre lieu où les personnes sont susceptibles de se trouver dans le cadre de leur emploi (ex. : aires communes dans les locaux de l'employeur, lors de réunions, assemblées, formations, déplacements, inspections ou vérifications sur le terrain ou virtuelles, ou activités sociales organisées par l'employeur);

La présente politique vise également les communications transmises ou reçues par tout moyen, technologique ou autre, dans un contexte de travail.

3) Définitions

Discrétion : L'aptitude à garder secrètes les confidences et les informations privées obtenues en dehors du cadre de travail afin de préserver le respect, l'amitié et la confiance.

Confidentialité : Le fait de limiter ou d'interdire à d'autres personnes l'accès à des informations privées obtenues dans l'exercice de ses fonctions.

[1] Dans le but d'alléger le texte, la forme masculine est utilisée et désigne aussi bien le féminin que le masculin.

4) Engagements de l'AIBQ :

L'AIBQ s'engage à :

- Assurer la sécurité et la confidentialité des renseignements obtenus;
- Mettre en place des mécanismes afin de protéger les informations confidentielles;
- Assurer le traitement confidentiel des plaintes;
- Recueillir seulement les données nécessaires ou utiles;
- Appliquer la politique de confidentialité dans le respect des valeurs de l'AIBQ;
- Agir avec respect et transparence lors de l'application de cette politique et dans le respect des lois en vigueur.

5) Normes de discrétion

Toute personne qui, au sein de l'AIBQ, a des échanges qui sont ou ne sont pas liés à l'exercice de ses fonctions doit agir avec discrétion. De ce fait, elle doit:

- Respecter la vie privée des personnes;
- Ne pas divulguer l'information confidentielle obtenue au sein de l'Association;
- Savoir garder les informations sensibles des personnes qui se confient;
- Agir selon les valeurs de l'Association.

6) Normes de confidentialité

- Toute personne à l'intérieur de l'AIBQ qui obtient des informations confidentielles dans l'exercice de ses fonctions est tenue de respecter la confidentialité de ces informations.
- Exception est faite dans certains cas où il est essentiel que les intervenants puissent échanger certaines informations pour une meilleure intervention. Dans ce cas, les personnes concernées doivent aussi garder la confidentialité des informations échangées.

7) Normes

7.1) Échange d'information, tenue de dossier et mesures de sécurité

7.1.1) Échanges d'informations à l'extérieur de l'AIBQ

- Le conseil d'administration, la direction et les employés ne doivent pas discuter de dossiers, de personnes ou de décisions propres à l'AIBQ, avec des personnes extérieures ou non concernées, sauf si cela est nécessaire pour réaliser une intervention. Dans une telle situation, ils doivent :
- S'assurer de l'identité de la personne qui demande l'information si celle-ci n'est pas connue;
- Limiter les échanges d'informations au strict minimum.

7.1.2) Échanges d'informations au sein de l'AIBQ;

- Limiter les échanges d'informations entre intervenants lors de réunion d'équipe ou dans un endroit sécurisé (ex. : bureau à porte fermée);
- Éviter de discuter des dossiers, des personnes ou des décisions en dehors de ces moments. Si cela est impossible, s'assurer de ne pas identifier la personne concernée et échanger dans un lieu propice à la confidentialité;
- S'assurer que les conversations téléphoniques traitant d'informations confidentielles ne sont pas entendues par d'autres personnes.

7.1.3) Règles à respecter concernant la tenue de dossier

- N'inscrire au dossier que des informations vraies, pertinentes et nécessaires;
- Éviter de noter des commentaires personnels, des réflexions ou perceptions et s'en tenir aux faits rapportés par la personne concernée ou observés par l'intervenant lui-même.

7.2) Mesures de sécurité pour limiter l'accès à l'information

Bureaux

- Puisque les employés de l'AIBQ travaillent principalement dans un environnement décloisonné et principalement à distance, les mêmes règles de sécurité s'appliquent que si les activités avaient lieu dans les locaux de l'AIBQ, soient :
    - Ranger les espaces de bureau afin de ne jamais laisser d'informations confidentielles visibles;
    - Limiter l'accès à l'espace de travail aux personnes autorisées seulement;

Classeurs

- Fermer les classeurs contenant les dossiers des membres, des clients et des employés ainsi que ceux contenant des renseignements nominatifs, en dehors des heures de bureau ou en l'absence de leurs responsables;
- Dans la mesure du possible, limiter physiquement l'accès aux classeurs en tenant les locaux fermés en l'absence de leurs responsables.

Ordinateurs et autres

- Verrouiller les écrans d'ordinateur à l'aide d'un mot de passe confidentiel à l'heure du dîner ou en cas d'absence;
- Activer un mot de passe ou un code secret de façon à verrouiller l'accès au contenu de tout appareil mobile;
- Changer le mot de passe (serveur, ordinateur, téléphone cellulaire, boîte vocale ou autre) chaque mois;

- Consigner dans un registre le nom des personnes détenant une clé et un accès au système d'alarme donnant accès aux bureaux de l'AIBQ;
- En cas de départ d'une personne détenant les accès aux bureaux de l'AIBQ, procéder à la modification des codes d'accès du système d'alarme.

7.3) Procédures de conservation et de destruction des dossiers confidentiels

- Conserver les dossiers fermés en un lieu sûr dans le respect des normes de l'AIBQ;
- S'assurer que les dossiers fermés sont déchiquetés par un membre du conseil d'administration assisté par les autres membres dudit conseil ou par quelqu'un d'autre désigné par le conseil, à la fin de la période de conservation;
- Détruire tous autres documents confidentiels de la même manière.
- L'obligation pour les organisations de détruire les renseignements personnels une fois que l'objectif pour lequel ils ont été recueillis est atteint.

7.4) Pour les membres du conseil d'administration

7.4.1) Échanges d'informations à l'extérieur de l'AIBQ

- Les membres du conseil d'administration ne doivent pas discuter de dossiers, de personnes ou de décisions propres à l'AIBQ avec des personnes extérieures à l'organisation ou non concernées, sauf si cela est nécessaire pour réaliser une intervention. Dans une telle situation, ils doivent :
- S'assurer de l'identité de la personne qui demande l'information si celle-ci n'est pas connue;
- Limiter les échanges d'informations au strict minimum.

7.4.2) Échanges d'informations au sein de l'AIBQ

- Limiter les échanges d'informations sur les dossiers, les personnes ou les décisions lors des réunions du conseil d'administration, du comité exécutif ou encore dans les bureaux de la direction à porte fermée;
- Éviter de discuter de personnes, de dossiers ou de décisions en dehors de ces moments. Si cela est impossible, s'assurer de ne pas identifier la personne concernée et d'échanger dans un lieu propice à la confidentialité;
- S'assurer que les conversations téléphoniques traitant d'informations confidentielles ne sont pas entendues par d'autres personnes.

7.4.3) Réunions et procès-verbaux (conseil d'administration, comité exécutif, assemblée générale annuelle)

- Les résolutions adoptées en réunion doivent rester confidentielles à l'AIBQ lorsqu'une telle mention se retrouve sur le document;

- Les enregistrements des séances du conseil doivent être détruits après l'adoption des procès-verbaux de ces séances;
- Les procès-verbaux des séances du conseil doivent rester confidentiels en tout temps et n'être accessibles que par les membres actuels du conseil.

8) Modalités d'application

- La direction de l'AIBQ est responsable de la mise en œuvre et de l'application de la politique de confidentialité;
- Les administrateurs, la direction et les employés doivent remplir, dès l'entrée en vigueur de cette politique, un formulaire d'engagement à respecter celle-ci;
- Le conseil d'administration doit intervenir en cas de non-respect de la politique de confidentialité par la direction;
- L'autorité compétente est responsable d'imposer une sanction pour non-respect de la présente politique par un administrateur ou un employé. La sanction doit être conforme aux politiques et règlements en vigueur à l'AIBQ et peut aller de la simple réprimande au congédiement ou à l'expulsion.

9) transmission des informations personnelles à des tiers

Lorsque l'AIBQ transfère des données à des tiers, elle doit conclure un accord écrit avec ces derniers. L'autre partie doit fournir une description des mesures prises pour préserver la confidentialité des données.

Association des inspecteurs en bâtiment du Québec - AIBQ
7811, boulevard Louis-H. Lafontaine, Bureau 204, Anjou, Québec H1K 4E4
www.aibq.qc.ca (514) 352-2427 info@aibq.qc.ca

Protection des renseignements personnels

Source : https://www.cai.gouv.qc.ca/entreprises/

10) Objet

Depuis le 22 septembre 2022, la Loi sur le privé prévoit de nouvelles obligations pour les entreprises. En effet, elle a été modernisée notamment afin d'être mieux adaptée à la réalité technologique d'aujourd'hui.

Cette loi s'applique à l'égard des renseignements personnels qu'une entreprise recueille, détient, utilise ou communique à des tiers, et ce, quelle que soit la nature du support et la forme sous laquelle les renseignements personnels sont détenus, à savoir écrite, graphique, sonore, visuelle, informatisée ou autre.

Cette loi a pour objectif d'offrir un cadre de protection des renseignements personnels détenus par les entreprises.

11) Un renseignement personnel, c'est quoi ?

Les renseignements personnels sont ceux qui portent sur une personne physique et permettent de l'identifier. Ils sont confidentiels. Sauf exception, ils ne peuvent être communiqués sans le consentement de la personne concernée.

12) Collecte

Première étape du cycle de vie du renseignement personnel, la collecte est le moment où le renseignement personnel est :

- Recueilli (ex. : formulaire d'abonnement, sondage);
- Créé (ex. : no de membre);

La collecte est réalisée par l'AIBQ ou un tiers, comme un mandataire ou un prestataire de services (Didacte, Quickbooks, etc.)

À cette étape, les obligations suivantes doivent être respectées afin de protéger les renseignements personnels :

- Déterminer les fins de la collecte : un intérêt sérieux et légitime doit motiver la constitution d'un dossier sur une personne;
    - Informations sur le membre qui paye une cotisation annuelle afin de lui permettre de profiter des outils mis à sa disposition et de fournir l'information sur son profil d'inspecteur qui doit respecter la norme de pratique de l'Association

- Limiter la collecte de renseignements personnels : la collecte doit se limiter aux renseignements nécessaires aux fins déterminées. En cas de doute, un renseignement personnel est réputé non nécessaire;
    - Nom, prénom, date de naissance
    - Adresse postale et courriel
    - Nom, adresse et site internet de l'entreprise d'inspecteur
    - Langue(s) parlée(s) et écrite(s)
    - Profession autre que celle d'inspecteur
- Recueillir les renseignements personnels par des moyens légaux et légitimes : sauf exception, la collecte doit se faire auprès de la personne concernée;
- Informer la personne concernée via l'affichage et la signature d'un consentement, avant de constituer un dossier :
    - De l'objet du dossier – Dossier de membre
    - De l'utilisation qui sera faite des renseignements personnels – Permettre accès aux avantages de l'Association (formation, utilisation de documents, normes de pratique, conventions de service);
    - Des catégories de personnes qui y auront accès au sein de l'AIBQ – Employées et direction
    - De l'endroit où ils seront détenus – Serveurs sécurisés de l'Association
- De ses droits d'accès et de rectification.
- Obtenir le consentement des personnes concernées avant de collecter leurs renseignements personnels auprès d'un tiers, à moins d'une exception prévue par la loi.

L'AIBQ ne peut refuser d'offrir un bien, un service ou un emploi à une personne qui refuse de fournir un renseignement personnel, sauf exception prévue par la loi.

13) Utilisation

L'utilisation est la période où le renseignement personnel est utilisé par les personnes autorisées au sein de l'AIBQ.

L'AIBQ doit respecter les obligations suivantes :

- Limiter l'accès aux renseignements personnels aux seules personnes ayant la qualité pour les recevoir au sein de l'AIBQ lorsque ces renseignements sont nécessaires à l'exercice de leurs fonctions;
- Limiter l'utilisation des renseignements personnels : à moins d'une exception prévue par la loi, l'AIBQ doit obtenir le consentement de la personne concernée pour utiliser ses renseignements une fois l'objet du dossier accompli.

14) Communication

La communication est la période où le renseignement personnel est communiqué, par exemple par courriel, au service à la clientèle, par le biais de sites Web ou à un tiers.

À cette étape, l'AIBQ doit respecter les obligations suivantes :

- Obtenir le consentement des personnes concernées pour communiquer leurs renseignements à un tiers (ex. : assureur ou prestataire de services), à moins d'une exception prévue par la loi;
- Respecter les obligations prévues par la loi lorsqu'elle communique des renseignements personnels sans le consentement de la personne concernée.

15) Conservation

La conservation est la période durant laquelle l'AIBQ garde des renseignements personnels, sous quelque forme que ce soit, et ce, peu importe que les renseignements soient activement utilisés ou non.

À cette étape, l'AIBQ doit respecter les obligations suivantes :

- Assurer la qualité des renseignements personnels en veillant à ce que les renseignements personnels qu'elle détient soient à jour et exacts au moment où elle les utilise pour prendre une décision relative à la personne concernée;
- Prendre des mesures de sécurité propres à assurer la sécurité des renseignements personnels.

16) Destruction

Le cycle de vie du renseignement personnel se termine lors de sa destruction.

À cette étape, l'AIBQ doit :

- Détruire les renseignements personnels de manière sécuritaire dès que la finalité pour laquelle ils ont été collectés est accomplie.

17) Autres obligations : sécurité, accès et rectification

- Mettre en place des mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits.
- Ces mesures sont raisonnables compte tenu, notamment, de la sensibilité, de la finalité, de la quantité, de la répartition et du support des renseignements personnels.

17.1) Mesures de sécurité

Action	Méthodes utilisées	Mesures de sécurité
Collecte	Téléphone, courriel et demande en ligne (site web)	Site web sécurisé
Utilisation	Excel, Didacte, Cyberimpact, Quickbooks, Stripe, Go Rendezvous, Moneris, RIM, Maximo, SharePoint	Espace nuagique (SharePoint) sécurisé par accès autorisés, accès restreints par mot de passe pour toutes les applications utilisées
Communication	Courriel, téléphone	
Conservation	Espace nuagique (SharePoint)	Sécurisé par accès autorisés
Destruction données physiques	Firme spécialisée en destruction de documents	Certificat d'attestation de destruction
Destruction données virtuelles	Détruites à partir de l'espace nuagique SharePoint	Registre des dates de destruction

19) Accéder aux renseignements personnels

Toute personne a le droit d'être informée que l'AIBQ détient des renseignements personnels la concernant.

Pour accéder à ses renseignements personnels, le membre doit justifier de son identité à titre de personne concernée.
Il est à noter qu'une demande sera également considérée si elle est faite par une personne agissant à titre de représentant, d'héritier ou de successible de la personne concernée, de liquidateur de la succession, de bénéficiaire d'une assurance-vie ou d'indemnité de décès, de titulaire de l'autorité parentale. Dans tous les cas, cette personne devra établir sa qualité et son identité.

19.1) Comment accéder aux renseignements personnels ?

Pour accéder à vos renseignements personnels, une demande doit être adressée par écrit à la personne qui détient le dossier au sein de l'AIBQ :

- Dossier d'assurances – Danny McNicoll
- Dossier de membre – Marie Côté
- Dossier d'employée - Denis St-Aubin ou Danny McNicoll

19.2) Quels sont les coûts reliés à une demande d'accès ?

En principe, l'accès à vos renseignements personnels est gratuit. Cependant, des frais n'excédant pas le coût de la transcription, de la reproduction ou de la transmission peuvent être exigés par l'AIBQ qui doit alors vous en indiquer préalablement le montant approximatif.

19.3) Quels sont les délais pour répondre à une demande d'accès

La personne détenant votre dossier donnera suite à votre demande dans les 30 jours de la date de sa réception.

19.4) Existe-t-il des restrictions au droit d'accès ?

Oui. Le droit d'accès aux renseignements personnels n'est pas absolu, il comporte certaines restrictions. Par exemple, l'AIBQ peut refuser de donner accès aux renseignements personnels s'il en résultait vraisemblablement un préjudice grave pour la personne concernée.

20) Rectifier les renseignements personnels

Lorsqu'une personne est informée de l'existence dans un fichier ou un dossier d'un renseignement inexact, incomplet ou équivoque qui la concerne, ou si sa collecte, sa communication ou sa conservation ne sont pas autorisées par la loi, il est possible de faire une demande de rectification.

L'identité de la personne concernée doit être justifiée. Il est à noter qu'une demande sera également considérée si elle est faite par une personne agissant à titre de représentant, d'héritier ou de successible de la personne concernée, de liquidateur de la succession, de bénéficiaire d'une assurance-vie ou d'indemnité de décès, de titulaire de l'autorité parentale. Dans tous les cas, cette personne devra établir sa qualité et son identité.

20.1) Comment rectifier les renseignements personnels ?

Pour faire rectifier les renseignements personnels, la personne concernée doit adresser une demande écrite à la personne qui détient son dossier au sein de l'AIBQ selon les accès indiqués en **19.1)**.

20.2) Quels sont les délais pour répondre à une demande de rectification?

- La personne détenant le dossier donnera suite à la demande dans les 30 jours de la date de sa réception.

21) Responsable de la protection des renseignements personnels

L'AIBQ est responsable de la protection des renseignements personnels qu'elle détient. Le président du conseil d'administration veille à assurer le respect et la mise en œuvre de la *Loi sur la protection des renseignements personnels dans le secteur privé* (Loi sur le privé).

Cette personne exerce la fonction de responsable de la protection des renseignements personnels; elle peut déléguer cette fonction par écrit, en tout ou en partie, à toute personne. Dans ce cas, il est recommandé de désigner une personne pouvant assumer efficacement ce rôle. Par exemple, celle-ci devrait avoir les compétences requises et un pouvoir décisionnel important. Il est également important d'appuyer la personne responsable de la protection des renseignements personnels avec les ressources humaines, techniques et financières nécessaires pour assurer la conformité à la Loi sur le privé.

La loi confie des rôles spécifiques à ce responsable. En cas d'incident de confidentialité impliquant un renseignement personnel, notamment, il doit :

- Enregistrer les communications effectuées à toute personne ou tout organisme susceptible de diminuer le risque pour la personne concernée suivant l'incident;
- Prendre part à l'évaluation du préjudice causé par l'incident.

22) Communiquer des renseignements personnels sans le consentement de la personne concernée

Selon la *Loi sur la protection des renseignements personnels dans le secteur privé* (Loi sur le privé), un renseignement personnel est confidentiel et l'AIBQ ne peut, à moins d'exceptions prévues par la loi, communiquer ce renseignement sans le consentement de la personne concernée.

Cette page présente les différentes exceptions.

22.1) Tiers autorisés

À certaines conditions, la Loi sur le privé autorise l'AIBQ à communiquer un renseignement personnel, sans le consentement de la personne concernée, aux tiers ci-dessous (liste non exhaustive) :

- À son procureur;
- Au directeur des poursuites criminelles et pénales si le renseignement est requis aux fins d'une poursuite pour infraction à une loi applicable au Québec;
- À un organisme chargé, en vertu de la loi, de prévenir, détecter ou réprimer le crime ou les infractions aux lois, qui le requiert dans l'exercice de ses fonctions, si le renseignement est nécessaire pour la poursuite d'une infraction à une loi applicable au Québec;
- À une personne à qui il est nécessaire de communiquer le renseignement dans le cadre d'une loi applicable au Québec ou pour l'application d'une convention collective;
- À un organisme public au sens de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements publics et sur la protection des renseignements personnels* qui, par l'entremise d'un représentant, le recueille dans

l'exercice de ses attributions ou la mise en œuvre d'un programme dont il a la gestion;
- À une personne ou à un organisme ayant pouvoir de contraindre à leur communication et qui les requiert dans l'exercice de ses fonctions;
- À une personne à qui cette communication doit être faite en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de la personne concernée ou à des tiers en vue de prévenir un acte de violence, dont un suicide et lorsqu'il existe un motif raisonnable de croire qu'un risque sérieux de mort ou de blessures graves menace une personne ou un groupe de personnes identifiable et que la nature de la menace inspire un sentiment d'urgence;

22.2) Communication de renseignements personnels en cas d'urgence ou en vue de prévenir un acte de violence

Dans certaines circonstances exceptionnelles, *la Loi sur la protection des renseignements personnels dans le secteur privé* (Loi sur le privé), permet à l'AIBQ de communiquer des renseignements personnels sans le consentement de la personne concernée.

La Commission rappelle néanmoins qu'avant de le faire, l'AIBQ doit s'assurer de l'existence de toutes les conditions préalables.

L'AIBQ peut communiquer un renseignement personnel, sans le consentement de la personne concernée, à une personne à qui cette communication doit être faite en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de la personne concernée.

L'AIBQ peut également communiquer un renseignement personnel, sans le consentement des personnes concernées, en vue de prévenir un acte de violence, dont un suicide, lorsqu'il existe un motif raisonnable de croire qu'un risque sérieux de mort ou de blessures graves menace une personne ou un groupe de personnes et que la nature de la menace inspire un sentiment d'urgence. On entend par « blessures graves » toute blessure physique ou psychologique qui nuit d'une manière importante à l'intégrité physique, à la santé ou au bien-être d'une personne ou d'un groupe de personnes identifiable. Les renseignements peuvent alors être communiqués à la ou aux personnes exposées à ce danger, à leur représentant ou à toute personne susceptible de leur porter secours.

L'AIBQ ne peut communiquer que les renseignements nécessaires aux fins poursuivies par la communication. Elle doit inscrire la communication afin que celle-ci fasse partie du dossier.
- À un service d'archives dans certaines conditions et/ou après un certain délai;
- À une personne qui peut utiliser ce renseignement à des fins d'étude, de recherche ou de statistique conformément à l'article 21 ou à une personne qui est autorisée conformément à l'article 21.1

- À une personne qui, en vertu de la loi, peut recouvrer des créances pour autrui et qui le requiert à cette fin dans l'exercice de ses fonctions;
- À une personne si le renseignement est nécessaire aux fins de recouvrer une créance de l'l'AIBQ;
- À toute personne ou tout organisme susceptible de diminuer un risque suivant un incident de confidentialité impliquant un renseignement personnel, en ne lui communiquant que les renseignements personnels nécessaires à cette fin.

22.3) Transaction commerciale

Lorsque la communication d'un renseignement personnel est nécessaire aux fins de la conclusion d'une transaction commerciale à laquelle elle entend être partie, l'AIBQ peut communiquer un tel renseignement, sans le consentement de la personne concernée, à l'autre partie à la transaction. Une entente doit préalablement être conclue avec l'autre partie, stipulant notamment que cette dernière partie s'engage:

- À n'utiliser le renseignement qu'aux seules fins de la conclusion de la transaction commerciale;
- À ne pas communiquer le renseignement sans le consentement de la personne concernée, à moins d'y être autorisée par la Loi sur le privé;
- À prendre les mesures nécessaires pour assurer la protection du caractère confidentiel du renseignement;
- À détruire le renseignement si la transaction commerciale n'est pas conclue ou si l'utilisation de celui-ci n'est plus nécessaire aux fins de la conclusion de la transaction commerciale.

22.3.1) Qu'est-ce qu'une transaction commerciale?

La Loi sur le privé prévoit qu'une transaction commerciale s'entend de l'aliénation ou de la location de tout ou partie de l'AIBQ ou des actifs dont elle dispose, d'une modification de sa structure juridique par fusion ou autrement, de l'obtention d'un prêt ou de toute autre forme de financement par celle-ci ou d'une sûreté prise pour garantir une de ses obligations.

22.4) Liste nominative

L'AIBQ peut, sans le consentement des personnes concernées, communiquer à un tiers une liste nominative ou un renseignement servant à la constitution d'une telle liste si les conditions suivantes sont réunies:

- Cette communication est prévue dans un contrat comportant une stipulation qui oblige le tiers à n'utiliser ou ne communiquer la liste ou le renseignement qu'à des fins de prospection commerciale ou philanthropique;
- Avant cette communication, lorsqu'il s'agit d'une liste nominative de ses membres ou de ses employés, elle a accordé aux personnes concernées l'occasion valable de refuser que ces renseignements soient utilisés par un tiers à des fins de prospection commerciale ou philanthropique;

- Cette communication ne porte pas atteinte à la vie privée des personnes concernées.

22.4.1) Qu'est-ce qu'une liste nominative

Une liste nominative est une liste de noms, de numéros de téléphone, d'adresses géographiques de personnes physiques ou d'adresses technologiques où une personne physique peut recevoir communication d'un document ou d'un renseignement technologique.

23) Incident de confidentialité impliquant des renseignements personnels

23.1) Quelles sont les lois visées?

Le terme « lois » vise autant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (Loi sur l'accès) que la Loi sur la protection des renseignements personnels dans le secteur privé (Loi sur le privé).

23.2) Qu'est-ce qu'un incident de confidentialité?

Pour l'application des lois, un incident de confidentialité correspond à tout accès, utilisation ou communication non autorisés par la loi d'un renseignement personnel, de même qu'à la perte d'un renseignement personnel ou à toute autre atteinte à sa protection.

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

- Un membre du personnel consulte un renseignement personnel sans autorisation;
- Un membre du personnel communique des renseignements personnels au mauvais destinataire;
- L'organisation est victime d'une cyberattaque : hameçonnage, rançongiciel, etc.

24) Les obligations en cas d'incident de confidentialité

24.1) Prendre des mesures pour diminuer les risques et éviter de nouveaux incidents

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

24.1.1) Les questions suivantes sont utiles afin d'évaluer rapidement la situation :

- **Qui :** quelles sont les personnes concernées par l'incident? S'agit-il d'employés, de clients ou de partenaires d'affaires? Qui peut avoir eu accès aux renseignements personnels?
- **Combien :** combien de personnes sont touchées par l'incident?
- **Quoi :** quelle est la nature des renseignements personnels visés par l'incident? Sont-ils des renseignements sensibles? Quels sont les risques pour les personnes concernées?
- **Quand :** quand l'incident a-t-il eu lieu? Quand a-t-il été découvert?
- **Où :** où l'incident a-t-il eu lieu? Au sein de l'organisation? Si oui, dans quel secteur? L'incident a-t-il eu lieu chez un tiers détenant des renseignements personnels pour le compte de l'organisation (ex. : un mandataire, un fournisseur)?
- **Pourquoi:** quelles sont les causes? Quelles mesures de sécurité étaient en place au moment de l'incident? Pourquoi n'ont-elles pas été efficaces?

Les mesures raisonnables à mettre en place dépendent de cet état de la situation. Toutes les situations sont différentes. Même si l'ensemble des informations pertinentes ne sont pas connues dès le départ, il est important de réagir rapidement. Au besoin, l'organisation continue d'**adapter ses mesures ou à d'en adopter de nouvelles** au fur et à mesure que les circonstances et les impacts de l'incident se précisent par la suite.

25) Évaluer les risques

Pour tout incident de confidentialité, l'organisation doit évaluer la gravité du risque de préjudice pour les personnes concernées. Pour ce faire, elle doit considérer, notamment :

- La sensibilité des renseignements concernés;
- Les conséquences appréhendées de leur utilisation;
- La probabilité qu'ils soient utilisés à des fins préjudiciables.

L'organisation doit consulter son responsable de la protection des renseignements personnels. Elle peut également impliquer d'autres acteurs, comme le responsable de la sécurité de l'information ou des experts externes.

Si l'analyse fait ressortir un risque de préjudice sérieux, l'organisation doit aviser la Commission et les personnes concernées de l'incident.

Dans le cas contraire, elle doit tout de même poursuivre ses travaux pour réduire les risques et éviter qu'un incident de même nature se produise à nouveau dans le futur.

26) Aviser la Commission et les personnes dont les renseignements sont concernés

Quand l'incident présente le risque qu'un préjudice sérieux soit causé aux personnes dont les renseignements sont concernés, l'organisation doit s'empresser d'aviser la

Commission. Toutes les personnes dont les renseignements personnels sont concernés par l'incident doivent également être informées par l'organisation. Si cette dernière n'informe pas les personnes concernées, la Commission peut lui ordonner de le faire.

Toutefois, l'organisation n'a pas à aviser les personnes dont les renseignements personnels sont concernés, si cet avis est susceptible d'entraver une enquête menée en vertu de la loi pour prévenir, détecter, réprimer le crime ou les infractions aux lois.

Le Règlement sur les incidents de confidentialité détermine le contenu et les modalités des avis qui doivent être transmis à la Commission et aux personnes concernées.

26.1) Avis à la Commission d'accès à l'information

Quand un incident de confidentialité présente le risque d'un préjudice sérieux, l'organisation doit aviser par écrit la Commission. Le **formulaire d'avis** précise toutes les informations à fournir.

Suivant l'envoi de son formulaire d'avis, l'organisation qui prend connaissance de nouvelles informations doit s'empresser de les communiquer à la Commission.

26.2) Avis aux personnes concernées

L'avis à la personne concernée doit l'informer de la portée et des conséquences de l'incident présentant le risque de préjudice sérieux.

Cet avis doit contenir :

- Une description des renseignements personnels visés par l'incident. Si cette information n'est pas connue, l'organisation doit communiquer la raison justifiant l'impossibilité de fournir cette description.
- Une brève description des circonstances de l'incident;
- La date ou la période où l'incident a eu lieu, ou une approximation de cette période si elle n'est pas connue;
- Une brève description des mesures prises ou envisagées pour diminuer les risques qu'un préjudice soit causé à la suite de l'incident;
- Les mesures proposées à la personne concernée afin de diminuer le risque qu'un préjudice lui soit causé ou d'atténuer celui-ci;
- Les coordonnées d'une personne ou d'un service avec qui la personne concernée peut communiquer pour obtenir davantage d'informations au sujet de l'incident.

De plus, une organisation peut donner un avis public afin d'agir rapidement pour diminuer le risque qu'un préjudice sérieux soit causé ou pour l'atténuer. L'organisation demeure toutefois tenue de transmettre un avis à la personne concernée dans les plus brefs délais.

Seulement trois situations permettent de faire un avis public sans transmettre un avis à la personne concernée :

- La transmission de l'avis peut causer un plus grand préjudice à la personne concernée;

- La transmission de l'avis représente une difficulté excessive pour l'organisation;
- L'organisation n'a pas les coordonnées de la personne concernée.

Cet avis peut être fait par tout moyen raisonnable permettant de joindre la personne concernée.

26.3) Aviser les personnes susceptibles de prévenir ou de diminuer le risque de préjudice sérieux

L'organisation peut aviser toute personne ou organisme susceptible de diminuer le risque de préjudice sérieux. Seuls les renseignements personnels nécessaires peuvent alors être communiqués, sans le consentement de la personne concernée. Le responsable de la protection des renseignements personnels de l'organisation doit enregistrer cette communication.

27) Tenir un registre des incidents de confidentialité

Toute organisation doit tenir un registre dans lequel elle collige tous les incidents de confidentialité impliquant des renseignements personnels. Elle doit y inscrire même les incidents qui ne présentent pas de risque de préjudice sérieux. À la demande de la Commission, l'organisation doit transmettre une copie de son registre.

Le registre des incidents de confidentialité doit contenir les éléments suivants :

- Une description des renseignements personnels visés par l'incident. Si cette information n'est pas connue, l'organisation doit inscrire la raison justifiant l'impossibilité de fournir cette description.
- Une brève description des circonstances de l'incident;
- La date ou la période où l'incident a eu lieu, ou une approximation de cette période si elle n'est pas connue;
- La date ou la période au cours de laquelle l'organisation a pris connaissance de l'incident;
- Le nombre de personnes concernées par l'incident ou, s'il n'est pas connu, une approximation de ce nombre;
- Une description des éléments qui amènent l'organisation à conclure qu'il y a, ou non, risque qu'un préjudice sérieux soit causé aux personnes concernées, comme :
    - La sensibilité des renseignements personnels concernés;
    - Les utilisations malveillantes possibles des renseignements;
    - Les conséquences appréhendées de l'utilisation des renseignements et la probabilité qu'ils soient utilisés à des fins préjudiciables;
- Les dates de transmission des avis à la Commission et aux personnes concernées, quand l'incident présente le risque de préjudice sérieux. L'organisation doit aussi préciser si elle a donné des avis publics et la raison de ceux-ci;

- Une brève description des mesures prises par l'organisation à la suite de l'incident, pour diminuer les risques qu'un préjudice soit causé.

Les renseignements du registre doivent être mis à jour et conservés pour une période minimale de cinq ans, après la date ou période de prise de connaissance de l'incident par l'organisation.

28) Pouvoirs d'ordonnance de la Commission

La Commission peut ordonner à toute personne, après lui avoir fourni l'occasion de présenter ses observations, l'application de toute mesure visant à protéger les droits des personnes concernées. Elle peut, notamment, ordonner la remise des renseignements personnels impliqués à l'organisation ou leur destruction. Une personne visée par une ordonnance sans qu'elle en ait été informée au préalable parce que, de l'avis de la Commission, il y a urgence ou danger de causer un préjudice irréparable, peut, dans le délai indiqué dans l'ordonnance, présenter ses observations pour en permettre le réexamen par la Commission.

Si l'incident présente un risque de préjudice sérieux, la Commission peut également ordonner à l'organisation d'aviser les personnes concernées si celle-ci ne l'a pas fait alors qu'elle était tenue de le faire.

29) Responsabilité des renseignements personnels conservés par un tiers

Dans divers contextes, les organisations confient des renseignements personnels à des tiers qui en assurent la conservation. Les organisations demeurent malgré tout responsables de l'ensemble des leurs obligations en cas d'incident de confidentialité : mesures à prendre, registre à tenir et à mettre à jour, avis à donner, etc.

30) Entrée en vigueur

La présente politique entre en vigueur à la suite de son adoption par le conseil d'administration de l'AIBQ. Elle pourra être modifiée au moment opportun après analyse. Les modifications doivent respecter les valeurs et les règlements de l'AIBQ.