

## MISE EN GARDE

Ce document, mis à jour en date du **22 février 2024**, se veut un outil de travail destiné aux membres de l'ACQ et est fourni uniquement à titre informatif. Il devra être adapté pour refléter les besoins et la réalité de votre entreprise. Les renseignements qu'il contient ne constituent PAS des avis juridiques et ne remplacent pas le texte de la *Loi sur la protection des renseignements personnels dans le secteur privé* (ci-après «*Loi secteur privé*») ou les autres lois et règlements applicables, qui ont valeur officielle. En cas de besoin, consultez un avocat pour vous assurer de la conformité de votre politique.

### A. OBJECTIFS

*Nom de l'entreprise* peut être appelée à recueillir, à détenir, à utiliser ou à communiquer à des tiers des renseignements personnels obtenus dans le cadre de l'exécution de ses travaux et activités. Dans ce contexte, la présente politique de confidentialité et de protection des renseignements personnels vise à établir les principes régissant la collecte, l'utilisation, la communication, la conservation et la destruction des renseignements personnels par *Nom de l'entreprise* afin d'assurer la protection de ceux-ci («*Politique*»).

À cette fin, la *Politique* a notamment pour but de:

- (i) Désigner et prévoir le rôle et les responsabilités du *Responsable à la protection des renseignements personnels* («*RPRP*») et de l'ensemble des employés de *Nom de l'entreprise* («*membre du Personnel*»);
- (ii) Établir des règles particulières en matière de collecte, d'utilisation, de communication, de conservation, de destruction, de droit d'accès et de rectification des renseignements personnels.

### B. DÉFINITIONS

Un **renseignement personnel** est tout renseignement qui concerne une personne physique et qui permet directement ou indirectement de l'identifier.

Il peut être notamment de nature:

- **Identitaire** – à titre d'exemple: nom, adresse, numéro de téléphone, date de naissance, etc.
- **Financière** – à titre d'exemple: salaire, carte de crédit, compte de banque, etc.
- **Fiscale** – à titre d'exemple: numéro d'assurance sociale, etc.

#### Exception:

Les renseignements personnels qui concernent une personne physique **exerçant une fonction au sein d'une entreprise**, tels que son nom, son titre et sa fonction, de même que l'adresse, l'adresse de courrier électronique et le numéro de téléphone de son lieu de travail ne sont pas visés par la présente *Politique*.

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

L'article 3.2 de la *Loi secteur privé* prévoit que toute personne qui exploite une entreprise doit établir et mettre en œuvre des politiques et des pratiques proportionnées à la nature et à l'importance des activités de l'entreprise qui encadrent sa gouvernance à l'égard des renseignements personnels et qui assure la protection de ces renseignements.

Celles-ci doivent notamment prévoir :

- l'encadrement applicable à la conservation et à la destruction des renseignements;
- les rôles et les responsabilités des membres du personnel tout au long du cycle de vie de ces renseignements et;
- un processus de traitement des plaintes relatives à la protection de ceux-ci.

Les politiques et pratiques mises en place au sein de votre entreprise doivent être approuvées par le responsable de la protection des renseignements personnels.

De plus, des informations détaillées au sujet de ces politiques et ces pratiques doivent être, en termes simples et clairs, publiées sur le site Internet de l'entreprise ou, si elle n'a pas de site, rendues accessibles par tout autre moyen approprié. Vous pouvez aussi simplement choisir de publier l'intégralité de vos politiques et pratiques concernant la protection des renseignements personnels, mais il ne s'agit pas d'une exigence prévue par la *Loi secteur privé*.

L'article 8.2 de la *Loi secteur privé* prévoit que la personne qui recueille par un moyen technologique des renseignements personnels doit publier une **politique de confidentialité** rédigée en termes simples et clairs sur le site Internet de l'entreprise, le cas échéant, et la diffuser par tout moyen propre à atteindre les personnes concernées. Elle doit également publier un avis de modification à cette politique, le cas échéant. La Commission d'accès à l'information a publié un guide concernant la rédaction d'une politique de confidentialité que nous vous invitons à consulter sur son site. Celui-ci explique également la différence entre une politique de confidentialité (article 8.2 *Loi secteur privé*) et une politique de protection des renseignements personnels (article 3.2 *Loi secteur privé*).

Veillez consulter le modèle d'une politique de confidentialité que vous pouvez adapter à vos besoins et à la réalité de votre entreprise afin de la publier sur votre site Internet comme l'exige la *Loi secteur privé*.

Nous avons conçu, à titre informatif, un modèle d'une politique de protection des renseignements personnels. Ce modèle doit être adapté aux besoins et à la réalité de votre entreprise. La politique que vous adoptez devrait prévoir des mesures de sécurité que vous allez appliquer au sein de votre entreprise pour assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits, lesquelles doivent être raisonnables, compte tenu, notamment, de la sensibilité des renseignements, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support. Nous vous recommandons de consulter des experts en matière de technologie pour compléter votre politique à cet égard. En cas de besoin, consultez également un avocat pour vous assurer de la conformité de votre politique.

**Nous vous invitons à prendre connaissance de la MISE EN GARDE au début de ce document.**

**Par exemple :**

- Renseignements concernant le groupe ethnique;
- Renseignements concernant les croyances philosophiques ou religieuses;
- Renseignements concernant la santé ou l'orientation sexuelle;
- Renseignements financiers;
- Renseignements biométriques: empreintes digitales, forme du visage, empreinte de l'iris, etc.;
- Identifiants uniques: permettent de distinguer un individu dans un ensemble (ex.: un numéro de client ou d'employé).

Pour les fins de la présente *Politique*, la référence au terme «renseignement personnel» inclut également un renseignement personnel sensible.

**C. CADRE RÉGLEMENTAIRE**

Cette *Politique* est établie conformément aux obligations qui incombent à Nom de l'entreprise en vertu de la *Loi secteur privé* et tout règlement qui s'y rattache.

**D. PORTÉE**

Cette *Politique* vise tous les renseignements personnels, tels que définis à la section B, quelle que soit la nature de leur support et la forme sous laquelle ils sont accessibles: écrite, graphique, sonore, visuelle, informatisée ou autre.

**E. PERSONNES VISÉES ET RESPONSABILITÉS**

Le *Personnel* est tenu de respecter la présente *Politique* pendant la durée de son emploi.

Chaque membre du *Personnel* est également tenu à une obligation de confidentialité et de loyauté relativement notamment aux renseignements, aux informations ou aux documents auxquels il a accès dans le cadre de son emploi, incluant les renseignements personnels, et ce, quelle que soit la nature de leur support et la forme sous laquelle ceux-ci sont accessibles (écrite, graphique, sonore, visuelle, informatisée ou autre). Cette obligation de confidentialité inclut une obligation de ne pas les utiliser (pour son propre bénéfice ou le bénéfice d'une tierce personne), les divulguer, les reproduire ou les transmettre à quiconque, sauf exception prévue à la loi.

**F. OBLIGATIONS**

La protection des renseignements personnels doit être assurée durant tout le cycle de vie de ces derniers, c'est-à-dire lors de la collecte, l'utilisation, la communication, la conservation et la destruction.

**1. COLLECTE ET CONSENTEMENT****Collecte**

*Avant la collecte*

Chaque membre du *Personnel*, avant de recueillir pour Nom de l'entreprise, dans le cadre de ses fonctions, un renseignement personnel concernant une personne physique, doit préalablement:

- Déterminer les fins pour lesquelles il veut collecter les renseignements personnels et s'assurer d'avoir un **intérêt sérieux et légitime** avant de recueillir des renseignements personnels sur autrui;
- limiter la collecte aux renseignements personnels **nécessaires** aux fins déterminées avant la collecte;
- recueillir les renseignements personnels par des **moyens licites** (c'est-à-dire légaux et légitimes);
- Prendre les **mesures de sécurité** pour assurer la protection des renseignements personnels qui seront collectés;
- Recueillir les renseignements personnels **auprès de la personne concernée**, à moins que celle-ci ne **consente** à la cueillette auprès de tiers ou que la **loi l'autorise**.

La **loi autorise** la collecte **auprès d'un tiers**, notamment dans les cas suivants:

a. Si la personne qui exploite une entreprise a un **intérêt sérieux et légitime** et si l'une ou l'autre des conditions suivantes se réalise:

1° *les renseignements sont recueillis dans l'intérêt de la personne concernée et ils ne peuvent être recueillis auprès de celle-ci en temps opportun;*

2° *la cueillette auprès d'un tiers est nécessaire pour s'assurer de l'exactitude des renseignements.*

b. Si la collecte se fait auprès d'un tiers dans le cadre de l'exercice d'un mandat ou l'exécution d'un contrat de service ou d'entreprise.

*Dans ce cas, assurez-vous que le mandat ou le contrat est confié à votre entreprise par écrit.*

*De plus, à moins que les renseignements personnels ne soient communiqués à un membre d'un ordre professionnel ou à un organisme public, il faut que le mandat ou le contrat prévoie les mesures de protection qui s'imposent au mandataire ou à l'exécutant du contrat afin d'assurer le caractère confidentiel des renseignements personnels obtenus, pour que ceux-ci ne soient utilisés que dans l'exercice du mandat ou l'exécution du contrat de service et pour qu'ils ne soient pas conservés après leur expiration.*

c. Si la collecte se fait auprès d'une personne qui exploite une entreprise dans le cadre d'une transaction commerciale<sup>2</sup>.

*Dans ce cas, une entente doit préalablement être conclue stipulant notamment que la partie recevant le renseignement personnel s'engage:*

(i) *À n'utiliser le renseignement qu'aux seules fins de la conclusion de la transaction commerciale;*

(ii) *À ne pas communiquer le renseignement sans le consentement de la personne concernée, à moins d'y être autorisée par la présente loi;*

(iii) *À prendre les mesures nécessaires pour assurer la protection du caractère confidentiel du renseignement;*

(vi) *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<sup>3</sup>.*

*Lorsque la transaction commerciale est conclue et que la partie ayant reçu le renseignement personnel souhaite continuer d'utiliser celui-ci ou le communiquer, elle doit utiliser ou communiquer ce renseignement conformément à la Loi secteur privé. De plus, la partie ayant reçu le renseignement personnel doit aviser la personne concernée qu'elle détient maintenant un renseignement personnel la concernant en raison de la transaction.*

\* Les exceptions sont discrétionnaires et vous pourrez plutôt décider d'obtenir le consentement de la personne concernée, notamment lorsque son obtention ne pose aucune difficulté.

\*\* Si vous n'êtes pas certain(e) qu'une exception s'applique, vous devez obtenir le consentement valide de la personne concernée.

#### *Obligation d'information/de transparence lors de la collecte*

Lors de la collecte, et par la suite sur demande, chaque membre du *Personnel* qui recueille des renseignements personnels pour Nom de l'entreprise **auprès de la personne concernée** doit informer celle-ci, en **termes simples et clairs**, des éléments suivants:

(i) Des **fins** auxquelles ces renseignements personnels sont recueillis;

<sup>2</sup> Une transaction commerciale s'entend de l'aliénation ou de la location de tout ou partie d'une entreprise 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.

<sup>3</sup> Loi secteur privé, RLRQ, c. P-39.1, article 18.4.

Il existe d'autres exceptions qui permettent la cueillette de renseignements personnels auprès d'un tiers. Veuillez vous référer à la *Loi secteur privé* afin de connaître toutes ces exceptions.

#### Par exemple :

- a. Traiter une demande d'emploi et un curriculum vitæ;
- b. Pour offrir les services demandés;
- c. Veiller à la bonne conduite de nos affaires, incluant la facturation et la gestion de nos dossiers;
- d. Prévenir la fraude et/ou effectuer toute vérification d'antécédents requise par la loi ou la réglementation applicables;
- e. Toute autre utilisation permise ou requise par les lois applicables;
- f. Toute autre fin à laquelle vous avez consenti.

- (ii) Des **moyens** par lesquels les renseignements sont recueillis;
- (iii) De ses **droits d'accès et de rectification** de ses renseignements personnels prévus par la loi;
- (iv) De son **droit de retirer son consentement** à la communication ou à l'utilisation des renseignements recueillis;
- (v) Le cas échéant, du nom des tiers pour qui la collecte est faite, des catégories de personnes à qui il est nécessaire de communiquer les renseignements personnels aux fins pour lesquelles ils sont recueillis et de la possibilité que les renseignements soient communiqués à l'extérieur du Québec.

Sur demande, la personne concernée doit également être informée:

- (i) Des renseignements personnels recueillis auprès d'elle;
- (ii) Des catégories de personnes qui ont accès à ces renseignements au sein de l'entreprise;
- (iii) De la durée de conservation de ces renseignements;
- (iv) Des coordonnées du responsable de la protection des renseignements personnels.

Nous vous recommandons d'informer la personne concernée des éléments ci-haut par écrit ou bien de documenter que ceux-ci lui ont été relatés et d'en conserver une copie dans vos dossiers.

#### Consentement

Si *Nom de l'entreprise* respecte son obligation d'information/de transparence lors de la collecte **auprès de la personne concernée**, elle peut considérer que cette personne a consenti à l'utilisation et à la communication de ses renseignements personnels qui sont nécessaires aux fins pour lesquelles ils ont été recueillis.

Chaque membre du *Personnel* doit toutefois obtenir le consentement de la personne concernée pour recueillir ses renseignements personnels auprès d'un tiers, s'il utilise ceux-ci à des fins autres que celles pour lesquelles ils ont été recueillis ou s'il les communique à un tiers, et ce, sauf **certaines exceptions**.

Lorsque le consentement de la personne concernée est nécessaire, nous vous recommandons d'utiliser le formulaire de consentement des renseignements personnels disponible sur le centre de documentation de l'ACQ.

#### Pour être valide, le consentement de la personne concernée doit être :

- (i) **Manifeste**: certain et sans ambiguïté.
- (ii) **Libre**: exprimé sans condition, contrainte ou menace.
- (iii) **Éclairé**: formulé en connaissance de sa portée. Le membre du *Personnel* requérant le consentement doit lui prêter assistance afin de l'aider à comprendre la portée du consentement donné.
- (iv) Donné à des **fins spécifiques**.
- (v) Demandé en termes **simples et clairs**.
- (vi) Demandé pour **chacune des fins spécifiques**.
- (vi) Présenté **distinctement** de toute autre information communiquée à la personne concernée lorsque demandé par écrit.

Rappelons que la *Loi secteur privé* prévoit certaines exceptions permettant la collecte auprès d'un tiers sans le consentement de la personne concernée. Voir la sous-section **Collecte**, la section **Communication** et les autres exceptions prévues par la *Loi secteur privé*.

#### Certaines exceptions

Veillez noter que ce ne sont pas toutes les exceptions ne nécessitant pas le consentement de la personne concernée qui sont abordées dans la *Politique*. Ainsi, nous vous invitons à consulter la *Loi secteur privé*, afin de connaître toutes les exceptions prévues à celle-ci à cet égard.

Le consentement **ne vaut que pour la durée nécessaire** à la réalisation des fins pour lesquelles il est demandé.

Notez qu'un consentement qui ne respecte pas ces critères de validité est considéré comme étant sans effet.

En cas de refus de la personne concernée d'octroyer son consentement, le membre du Personnel qui a fait la demande doit informer immédiatement **par écrit** le RPRP.

Le RPRP procédera à l'analyse de la situation et déterminera si l'absence de consentement permet à Nom de l'entreprise de refuser d'acquiescer à une demande en raison du refus de la personne visée par la demande selon les cas permis par la *Loi secteur privé*.

## 2. UTILISATION

Tout membre du *Personnel* qui doit utiliser des renseignements personnels dans le cadre de ses fonctions ne peut les utiliser qu'aux fins pour lesquelles ils ont été recueillis, sauf si la personne concernée consent à l'utilisation de ses renseignements personnels à d'autres fins.

Cependant, un renseignement personnel peut être utilisé à une autre fin sans le consentement de la personne concernée dans les seuls cas suivants:

- (i) lorsque son utilisation est à des fins **compatibles** avec celles pour lesquelles il a été recueilli;
- (ii) lorsque son utilisation est **manifestement au bénéfice** de la personne concernée;
- (iii) lorsque son utilisation est **nécessaire** à des fins de prévention et de détection de la fraude ou d'évaluation et d'amélioration des mesures de protection et de sécurité;
- (iv) lorsque son utilisation est **nécessaire** à des fins de fourniture ou de livraison d'un produit ou de prestation d'un service demandé par la personne concernée;
- (v) lorsque son utilisation est **nécessaire** à des fins d'étude, de recherche ou de production de statistiques et qu'il est dépersonnalisé.

## 3. COMMUNICATION

### Accès interne aux renseignements personnels

L'accès aux renseignements personnels doit être limité aux seules personnes ayant la qualité pour les recevoir au sein de Nom de l'entreprise lorsque ces renseignements sont nécessaires à l'accomplissement de leurs fonctions.

### Communication aux personnes autorisées par la personne concernée

Les renseignements personnels d'une personne concernée ne peuvent être communiqués à des tiers (personne morale ou physique), sous réserve d'avoir obtenu préalablement son consentement à une telle communication ou d'une exception prévue par la *Loi secteur privé*.

### Communication à des tiers autorisée par la *Loi secteur privé* sans le consentement de la personne concernée

En vertu de la *Loi secteur privé*, il est possible pour Nom de l'entreprise de devoir communiquer, à des fins légitimes, des renseignements personnels à des tiers sans le consentement de la personne concernée, dont notamment dans les cas suivants:

- (i) Lorsque permis par la *Loi secteur privé* **notamment**:
  - Lorsque cette communication est nécessaire à **l'exercice d'un mandat ou l'exécution d'un contrat** de service ou d'entreprise;

Dans ce cas, Nom de l'entreprise doit confier le mandat ou le contrat par écrit à la personne ou à l'organisme.

De plus, à moins que les renseignements personnels ne soient communiqués à un membre d'un ordre professionnel ou à un organisme public, il faut que le mandat ou le contrat prévoie les mesures de protection qui s'imposent au mandataire ou à l'exécutant du contrat afin d'assurer le caractère confidentiel des renseignements personnels obtenus, pour que ceux-ci ne soient utilisés que dans l'exercice du mandat ou l'exécution du contrat de service et pour qu'ils ne soient pas conservés après leur expiration.

**Par écrit: Bonne pratique! Ce n'est cependant pas obligatoire.**

**Une bonne pratique serait d'inscrire notamment les informations suivantes dans l'avis écrit:**

- Le membre du *Personnel* de votre entreprise à l'origine de la demande;
- La nature des renseignements demandés;
- À quelles fins ces derniers étaient demandés;
- La nécessité de ces renseignements;
- Le motif du refus de la personne concernée.

Selon l'article 12 de la *Loi secteur privé*, pour qu'une fin soit compatible, «il doit y avoir un lien pertinent et direct avec les fins auxquelles le renseignement a été recueilli.» La prospection commerciale ou philanthropique n'est toutefois pas considérée comme une fin comptable selon l'article 12 de la *Loi secteur privé*.

La *Loi secteur privé* prévoit d'autres cas d'exception permettant la communication à des tiers sans le consentement de la personne concernée. Veuillez vous référer à la *Loi secteur privé* afin de connaître toutes ces exceptions.

- Lorsque la communication est faite à l'autre partie à une **transaction commerciale** telle que défini aux présentes;

*Dans ce cas, une entente doit préalablement être conclue avec l'autre partie à la transaction, stipulant notamment que cette dernière 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 présente loi;
  - 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<sup>4</sup>.
- Lorsque la communication est faite à **une personne ou à un organisme ayant pouvoir de contraindre** leur communication et qui les requiert dans l'exercice de ses fonctions;
  - Lorsque la communication est faite 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;
  - Lorsque la communication est faite 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;
  - Lorsque la communication est faite à une personne si le renseignement est nécessaire aux fins de **recouvrer une créance de l'entreprise**.

(ii) Lorsque requis par la loi ou qu'une autorité compétente l'exige.

#### Registre des communications à des tiers

*Nom de l'entreprise* \_\_\_\_\_ doit tenir un registre à jour des renseignements personnels communiqués **notamment dans le cadre des exceptions permises par la Loi secteur privé décrites à la sous-section précédente**. Ainsi, chaque membre du Personnel qui, dans l'exercice de ses fonctions, communique des renseignements personnels sur autrui à un tiers dans les cas d'exception susmentionnés doit inscrire cette communication dans un **registre** prévu à cet effet.

#### Niveau de protection

Tout membre du *Personnel* qui communique, à l'interne ou à une tierce partie, des renseignements personnels dans le cadre de ses fonctions, que ce soit dans le cadre d'une communication autorisée par la personne concernée ou une disposition de la *Loi secteur privé*, doit:

- Veiller à appliquer les **mesures de sécurité** énoncées à la présente *Politique* pour en préserver le caractère confidentiel;
- **Limiter** la communication qu'aux **renseignements nécessaires** aux fins poursuivies par la communication.

#### 4. CONSERVATION

Sous réserve d'un délai de conservation prévu par une loi, les renseignements personnels collectés ne doivent être conservés que pour la période nécessaire à l'accomplissement des fins pour lesquelles ils ont été recueillis.

Si vous souhaitez en apprendre davantage sur la durée de conservation des renseignements personnels, nous vous invitons à communiquer avec le *RPRP* dont les coordonnées figurent à la section G «Responsable de la protection des renseignements personnels et l'application».

<sup>4</sup> *Loi secteur privé*, RLRQ, c. P-39.1, article 18.4.

La *Loi secteur privé* prévoit d'autres communications à des tiers faites sans le consentement de la personne concernée qui doivent être inscrites.

Veillez vous référer à la *Loi secteur privé* afin de connaître les autres communications qui doivent être inscrites selon celle-ci.

#### Registre des communications à des tiers

La *Loi secteur privé* ne prescrit pas le contenu de l'information qui doit être inscrite en ce qui concerne les communications à des tiers sans le consentement de la personne concernée. Une bonne pratique serait d'inscrire notamment les informations suivantes au registre:

- Date de la communication;
- Identité de la personne et/ou l'entité et/ou l'autorité à qui les renseignements ont été communiqués;
- Nature ou type de renseignements personnels communiqués;
- Finalité/raison de la communication;
- Mode de transmission et les mesures de sécurité applicables à ce mode de transmission;
- Présence de renseignements personnels sensibles;
- Communication hors Québec
- Le cas échéant, date de réalisation de l'EFVP;
- Entente de confidentialité;
- Fondement juridique/raison justifiant la communication des RP;
- Commentaires.

## 5. DESTRUCTION

Lorsque les fins auxquelles les renseignements personnels ont été recueillis sont accomplies, ces derniers doivent être détruits, sous réserve d'un délai de conservation prévu par une loi.

**Pour déterminer s'il convient de détruire un dossier, il faut tenir compte notamment des éléments suivants :**

- La période pendant laquelle votre entreprise est tenue de conserver les documents en vertu de dispositions législatives ou réglementaires particulières;
- La probabilité que votre entreprise ait besoin des renseignements pour faire valoir un droit ou un recours à l'avenir;
- La période pendant laquelle votre entreprise peut être tenue responsable de réclamations et/ou faire l'objet d'un recours impliquant les renseignements personnels;
- Les mesures de sécurité en place pour assurer la confidentialité et la protection des renseignements personnels.

Toute destruction de renseignements personnels devra être documentée par écrit et inscrite dans un **registre** à cette fin, lequel registre devra être tenu à jour par le *RPRP*.

## 6. ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE (« EFVP »)

L'EFVP est une démarche préventive visant à mieux protéger les renseignements personnels et à mieux respecter la vie privée des personnes physiques. Elle consiste à considérer tous les facteurs qui auront un impact positif ou négatif pour le respect de la vie privée des personnes concernées.

Lorsqu'applicable, *Nom de l'entreprise* procédera à la réalisation d'une EFVP afin d'identifier les risques d'atteinte à la vie privée engendrés par la collecte, l'utilisation, la communication, la conservation ou la destruction des renseignements et l'évaluation de leurs impacts. *Nom de l'entreprise* verra également à mettre en place des stratégies pour éviter ces risques ou les réduire efficacement et prendre toutes les mesures afin de protéger efficacement ces renseignements personnels.

## 7. MESURES DE SÉCURITÉ

Afin de protéger les renseignements personnels que *Nom de l'entreprise* recueille, détient, utilise, communique, conserve et détruit, *Nom de l'entreprise* a adopté diverses mesures de sécurité. Ces mesures de sécurité sont adaptées au degré de sensibilité des renseignements personnels, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support. *Nom de l'entreprise* prend plus particulièrement les mesures de sécurité suivantes :

*Indiquer ici les mesures de sécurité qui vont être implantées au sein de votre entreprise*

Afin d'assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits, il est très important de prévoir des **mesures de sécurité raisonnables** compte tenu, notamment, de la sensibilité des renseignements, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support (article 10 de la *Loi secteur privé*). De plus, lorsqu'un document contient des renseignements que la loi déclare confidentiels, **leur confidentialité doit être protégée** lors de leur transmission (article 34 de la *Loi concernant le cadre juridique des technologies de l'information*, RLRQ, c. C-1.1). Ainsi, il est possible que l'envoi d'un document contenant des renseignements personnels par simple courriel ne permette pas de respecter ces exigences légales.

Les mesures de sécurité mises en place au sein de votre entreprise doivent être adaptées selon votre réalité. Nous vous recommandons de consulter des experts en matière de technologie à cet égard pour bien vous outiller.

## Registre des renseignements personnels détruits

C'est une **bonne pratique** de conserver un registre de destruction avec les éléments énoncés afin de conserver une trace des renseignements détruits pour vos dossiers. Toutefois, il ne s'agit pas d'une obligation.

Une bonne pratique serait d'inscrire notamment les informations suivantes au **registre de destruction** :

- Emplacement des renseignements personnels ou du dossier;
- Nom du ou des personnes concernées ou numéro du dossier;
- Délai de conservation du dossier;
- Date de la destruction;
- Personne ayant autorisé la destruction
- Personne ayant procédé à la destruction

Une EFVP est nécessaire dans les situations suivantes :

- Lors d'un projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services (articles 3.3 et 3.4 de la *Loi secteur privé*)
  - Aux fins de l'EFVP, il faut consulter, dès le début du projet, le *RPRP* et s'assurer que ce projet permet qu'un renseignement personnel informatisé recueilli auprès de la personne concernée soit communiqué à cette dernière dans un format technologique structuré et couramment utilisé.
  - La réalisation d'une EFVP en application de la *Loi sur le secteur privé* doit être proportionnée à la sensibilité des renseignements concernés, leur finalité, leur quantité, leur réparation et leur support.
  - Le *RPRP* peut à toute étape de l'EFVP, suggérer des mesures de protection des renseignements personnels applicables à un projet, telles que la nomination d'une personne chargée de la mise en œuvre des mesures de protection des renseignements personnels et une description des responsabilités des participants au projet en matière de protection des renseignements personnels.
  - Lors de la communication d'un renseignement personnel à l'extérieur du Québec ou lorsqu'une entreprise confie à une personne ou un organisme à l'extérieur du Québec la tâche de recueillir, d'utiliser, de communiquer ou de conserver pour son compte un tel renseignement (article 17 de la *Loi secteur privé*)
  - Aux fins de l'EFVP, l'entreprise doit notamment tenir compte de « 1° la sensibilité du renseignement; 2° la finalité de son utilisation; 3° les mesures de protection, y compris celles qui sont contractuelles, dont le renseignement bénéficierait; 4° le régime juridique applicable dans l'État où ce renseignement serait communiqué, notamment les principes de protection des renseignements personnels qui y sont applicables ».
  - La communication peut s'effectuer si l'EFVP démontre que le renseignement serait adéquatement protégé, notamment au regard des principes de protection des renseignements personnels généralement reconnus.
  - Lors de la communication sans consentement à un organisme qui souhaite utiliser ces renseignements à des fins d'étude, de recherche ou de production de statistiques (article 21).
- \*\* Veuillez consulter la *Loi secteur privé* pour davantage de détails à l'égard des situations susmentionnées nécessitant une EFVP.

## 8. INCIDENT DE CONFIDENTIALITÉ ET TENUE D'UN REGISTRE DES INCIDENTS DE CONFIDENTIALITÉ

On entend par «incident de confidentialité» l'accès, l'utilisation ou la communication non autorisés par la loi à un renseignement personnel, de même que la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

Tout membre du *Personnel* qui a des motifs de croire qu'un incident de confidentialité impliquant un renseignement personnel qu'il détient s'est produit doit prendre les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé, communiquer avec le *RPRP* afin de traiter de l'incident de confidentialité et éviter que de nouveaux incidents de même nature ne se produisent.

Veillez vous référer à l'aide-mémoire de l'ACQ: **AIDE-MÉMOIRE Incident de confidentialité impliquant un renseignement personnel.**

De plus, un **registre des incidents de confidentialité** doit être tenu par Nom de l'entreprise.

## G. RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET L'APPLICATION

La personne ayant la fonction de *RPRP* au sein de l'entreprise est:

Nom: \_\_\_\_\_

Titre du Responsable de la protection des renseignements personnels: \_\_\_\_\_

Adresse: \_\_\_\_\_

Téléphone: \_\_\_\_\_

Courriel: \_\_\_\_\_

Le *RPRP* veille à assurer le respect et la mise en œuvre de la *Loi secteur privé*. Le *RPRP* veille également au respect de la présente *Politique*.

## H. DEMANDE D'ACCÈS À L'INFORMATION ET DE RECTIFICATION

Sous réserve des limites prévues par la loi, une personne concernée a un droit d'accès et un droit de rectification en ce qui concerne ses renseignements personnels. Toute demande d'accès ou de rectification formulée par une personne concernant ses renseignements personnels doit être transmise au *RPRP* pour étude et réponse. Le *RPRP* répondra à la demande dans les 30 jours de sa réception.

## I. PLAINTÉ

Toute plainte concernant le traitement des renseignements personnels devra être acheminée au *RPRP* pour étude et réponse.

## J. ENTRÉE EN VIGUEUR ET MISE À JOUR

La *Politique* est en vigueur à compter du Date d'entrée en vigueur (année-mois-jour).

La présente *Politique* pourrait être mise à jour par Nom de l'entreprise en tout temps afin de l'adapter à la réalité organisationnelle de Nom de l'entreprise ou advenant toute modification au cadre législatif applicable en la matière.

Pour vous assurer d'avoir l'information la plus à jour, visitez régulièrement le site Web de Nom de l'entreprise ou veuillez communiquer avec le *RPRP*.

La date de dernière mise à jour de la *Politique* est le Date d'entrée en vigueur (année-mois-jour).

## Registre des incidents de confidentialité

L'article 7 du *Règlement sur les incidents de confidentialité* (chapitre A-2.1, r. 3.1) prévoit que le registre doit contenir les renseignements suivants:

- «1° une description des renseignements personnels visés par l'incident ou, si cette information n'est pas connue, la raison justifiant l'impossibilité de fournir une telle description;
- 2° une brève description des circonstances de l'incident;
- 3° la date ou la période où l'incident a eu lieu ou, si cette dernière n'est pas connue, une approximation de cette période;
- 4° la date ou la période au cours de laquelle l'organisation a pris connaissance de l'incident;
- 5° le nombre de personnes concernées par l'incident ou, s'il n'est pas connu, une approximation de ce nombre;
- 6° une description des éléments qui vous amène à conclure qu'il existe ou non un risque qu'un préjudice sérieux soit causé aux personnes concernées, telles que la sensibilité des renseignements personnels concernés, les utilisations malveillantes possibles de ces renseignements, les conséquences appréhendées de leur utilisation et la probabilité qu'ils soient utilisés à des fins préjudiciables;
- 7° si l'incident présente un risque qu'un préjudice sérieux soit causé, les dates de transmission des avis à la Commission d'accès à l'information et aux personnes concernées, en application de l'article 3.5 de la *Loi le privé*, de même qu'une mention indiquant si des avis publics ont été donnés par l'organisation et la raison pour laquelle ils l'ont été, le cas échéant;
- 8° une brève description des mesures prises par l'organisation, à la suite de la survenance de l'incident, afin de diminuer les risques qu'un préjudice soit causé.»

L'article 3.1 al. 2 de la *Loi secteur privé* prévoit que la personne ayant la plus haute autorité au sein de l'entreprise exerce la fonction de responsable de la protection des renseignements personnels. Toutefois, celle-ci peut déléguer cette fonction **par écrit**, en toute ou en partie, à toute personne.

Nous vous rappelons que la *Loi secteur privé* prévoit que des informations détaillées au sujet des politiques et des pratiques concernant la protection des renseignements personnels soient publiées en termes simples et clairs sur le site Internet de l'entreprise.

Ainsi, si vous décidez de publier des informations détaillées concernant votre politique de protection des renseignements personnels en termes simples et clairs sur votre site Web, il n'est pas nécessaire d'inclure cette phrase. Toutefois, si vous affichez la politique sur votre site Web dans son intégralité, vous pouvez l'inclure.