Un programme de gestion de la protection de la vie privée : la clé de la responsabilité

Objectif

Le Commissariat à la protection de la vie privée (le Commissariat) et les Commissariats à l'information et à la protection de la vie privée (CIPVP) de l'Alberta et de la Colombie-Britannique ont travaillé en collaboration pour élaborer le présent document dans le but de fournir une ligne directrice cohérente sur la notion d'organisation responsable à l'intention des organisations visées par nos législations respectives en matière de protection des renseignements personnels dans le secteur privé. Dans le document, nous définissons ce à quoi nous nous attendons d'un programme de gestion de la protection de la vie privée.

En quoi consiste la responsabilité?

La responsabilité dans le domaine de la protection de la vie privée est la reconnaissance du devoir de protéger les renseignements personnels. Une organisation responsable doit se doter de politiques et de procédures appropriées pour promouvoir l'application d'un ensemble de bonnes pratiques qui constitue un programme de gestion de la protection de la vie privée. Un tel programme permet aux organisations de respecter, au minimum, les lois applicables sur la protection des renseignements personnels. S'il est bien appliqué, il permet habituellement de renforcer le niveau de confiance des consommateurs, ce qui donne un avantage concurrentiel et rehausse la réputation des organisations.

Le concept de responsabilité semble explicite, mais la mise en place d'un programme de gestion de la protection de la vie privée au sein d'une organisation exige une bonne planification et la prise en compte de plusieurs disciplines et fonctions professionnelles. Les employés des organisations responsables doivent connaître et comprendre les éléments applicables du programme de l'organisation. Les clients, les partenaires et les fournisseurs de services doivent aussi connaître les aspects pertinents du programme et être rassurés à cet égard. Enfin, en cas d'enquête ou de vérification découlant du dépôt d'une plainte, les organisations responsables doivent être capables de prouver aux commissaires à la protection de la vie privée qu'ils ont mis en place un programme

de gestion de la protection de la vie privée efficace et à jour. Ils doivent s'assurer de bien cerner leurs obligations en matière de protection des renseignements personnels et les risques connexes et d'en tenir compte comme il se doit au moment d'élaborer leurs modèles opérationnels et leurs pratiques technologiques et opérationnelles connexes et avant d'offrir de nouveaux produits et services. Ils doivent réduire au minimum les risques pour leur organisation, leurs employés et leurs clients et atténuer les répercussions de toute atteinte à la vie privée.

Il y aura toujours des erreurs. Cependant, un bon programme de gestion de la protection de la vie privée permettra aux organisations de cerner leurs faiblesses, de renforcer leurs pratiques exemplaires, de faire preuve de diligence raisonnable et d'offrir une protection des renseignements personnels en leur possession supérieure au strict minimum prévu dans la législation.

Le présent document décrit ce que nous considérons comme les pratiques exemplaires en matière d'élaboration d'un bon programme de gestion de la protection de la vie privée pour les organisations de toutes tailles qui veulent respecter les obligations aux termes des législations applicables en matière de protection des renseignements personnels. Ce document n'est cependant pas une solution « universelle ». Chaque organisation doit déterminer, en tenant compte de sa taille, la meilleure façon d'appliquer les lignes directrices contenues dans le présent document au moment d'élaborer leur programme de gestion de la protection de la vie privée. Le présent document peut aussi servir aux organisations du secteur public et aux institutions de soins de santé qui élaborent un programme de gestion de la protection de la vie privée.

La **partie A** du présent document définit les « éléments constitutifs » ou éléments de base dont chaque organisation doit se doter. Des éléments comme l'engagement de l'organisation et les mesures de contrôle du programme sont essentiels.

La **partie B** décrit comment s'y prendre pour maintenir et améliorer continuellement le programme de gestion de la protection de la vie privée. Un tel programme ne doit jamais être considéré comme définitif : il faut continuellement l'évaluer et le réviser afin d'en assurer l'efficacité et la pertinence. Il faut contrôler et évaluer régulièrement les éléments constitutifs et les mettre à jour en conséquence.

Au bout du compte, cela signifie que les éléments constitutifs évoluent constamment en fonction des changements à l'intérieur et à l'extérieur de l'organisation (p. ex. des changements technologiques et des modifications des modèles opérationnels, de la législation ou des pratiques exemplaires).

L'**annexe A** contient une liste de documents que les commissariats ont élaborés au fil des ans sur différents aspects liés à la conformité en matière de protection de la vie privée.

Le contexte canadien

Il y a quatre régimes législatifs en matière de protection de la vie privée qui s'appliquent au secteur privé au Canada. La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) s'applique aux entreprises fédérales (et aux renseignements personnels de leurs employés) et aux entreprises de compétence provinciale dans les provinces qui n'ont pas de lois essentiellement similaires à la loi fédérale qui recueillent, utilisent ou communiquent des renseignements personnels dans le cadre de leurs activités commerciales[1]. Trois provinces ont promulgué des lois sur la protection des renseignements personnels dans le secteur privé que le gouvernement du Canada juge « essentiellement similaires » à la LPRPDE : la Colombie-Britannique, l'Alberta et le Québec[2]. La Colombie-Britannique et l'Alberta se sont chacune dotées de lois sur la protection des renseignements personnels, et le Québec a promulgué la *Loi sur la protection des renseignements personnels dans le secteur privé*[3].

Le principe de la responsabilité est le premier de 10 principes relatifs à l'équité dans le traitement des renseignements qui figurent à l'annexe 1 de la LPRPDE. Ce principe est sous-entendu dans les lois de l'Alberta, de la Colombie-Britannique et du Québec. Il s'agit du premier principe parce que c'est celui en vertu duquel les organisations doivent appliquer les autres principes relatifs à l'équité dans le traitement des renseignements dont l'objectif est d'assurer la gestion appropriée et la protection des renseignements personnels des particuliers. (Le principe de la responsabilité de l'annexe I de la LPRPDE figure en entier à l'**annexe B**.)

Contexte international

Il convient de signaler l'importance de la nature conjointe (fédérale et provinciale) du présent document d'orientation. En effet, les renseignements personnels sont devenus une marchandise universelle qui circule constamment dans le monde entier et qui est utilisée par des organisations qui œuvrent dans diverses administrations. Le besoin d'adopter des approches cohérentes en matière de protection des renseignements personnels n'a jamais été aussi marqué.

---

[1] LPRPDE, alinéa 26(2)*b*).
[2] *Décret d'exclusion visant des organisations de la province de la Colombie-Britannique* (DORS/2004-220); *Décret d'exclusion visant des organisations de la province de l'Alberta* (DORS/2004-219); et *Décret d'exclusion visant des organisations de la province du Québec* (DORS/2003-374).
[3] Trois lois provinciales (de l'Ontario, du Nouveau-Brunswick et de Terre-Neuve-et-Labrador) portent sur la gestion des renseignements personnels liés à la santé et ont un statut essentiellement similaire.

En effet, la nature universelle et la grande quantité de renseignements personnels qui circulent ont poussé de nombreux experts du domaine de la protection de la vie privée à examiner de plus près ce que signifie, pour une organisation, être « responsable » dans le domaine de la protection des renseignements personnels, et à réfléchir à la façon dont on peut tirer profit de la notion de responsabilité pour communiquer l'importance de la protection des renseignements personnels aux organisations dans les administrations qui n'ont pas de législation sur la protection des renseignements personnels.

L'Organisation de coopération et de développement économiques (OCDE) a exprimé pour la première fois le principe de la responsabilité en 1980 dans ses *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*. Ce document contient le premier ensemble de principes internationaux en matière de protection des renseignements personnels. L'annexe I de la LPRPDE reprend le code modèle de l'Association canadienne de normalisation (CSA), qui s'appuie fortement sur les *Lignes directrices* de l'OCDE. Depuis, le principe de la responsabilité a été intégré dans le cadre de protection de la vie privée de la Coopération économique Asie-Pacifique (APEC). On élabore dans cette région des règles transfrontalières en matière de protection de la vie privée afin d'appliquer le cadre de l'APEC. Ces règles étofferont le principe de la responsabilité.

Le concept de responsabilité suscite aussi de l'intérêt au sein de l'Union européenne. L'Avis sur le principe de la responsabilité du Groupe de travail « Article 29 » contient la même analyse minutieuse du principe de la responsabilité en matière de protection de la vie privée et décrit ce que les organisations devront faire à l'avenir pour prouver qu'elles s'y conforment. Le Groupe de travail formule une proposition qui, selon lui, « contribuerait à faire de la protection des données une réalité et aiderait les autorités compétentes en la matière dans leurs missions de supervision et de mise en application ». La Commission européenne a proposé un nouveau cadre juridique au sein de l'Union européenne en matière de protection de la vie privée qui contient une disposition sur la responsabilité. Cette disposition exigerait des organisations qu'elles adoptent des politiques et mettent en place des procédures appropriées pour prouver que leur traitement des données personnelles respecte la réglementation proposée.

En plus des accords internationaux et des lois nationales en matière de protection des renseignements personnels, Safe Harbor, les programmes d'auto-certification et les règles professionnelles contraignantes sont tous des exemples d'utilisation du concept de responsabilité pour promouvoir la protection de la vie privée tout en favorisant la communication des données transfrontalières. Dans le cadre du Accountability Project, le Centre for Policy and Information Leadership des États-Unis en collaboration avec des représentants d'organismes de protection de données, d'entreprises et d'universités, examine ce que signifie, pour une organisation, d'être « responsable » sur

le plan des pratiques liées à la protection de la vie privée. Le Commissariat et le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique ont participé à cette initiative internationale.

Avantages liés à l'adoption d'un programme de gestion de la protection de la vie privée

Toutes les organisations visées par les lois canadiennes sur la protection des renseignements personnels dans le secteur privé sont tenues de s'y conformer. L'adoption d'un programme de gestion de la protection de la vie privée complet est une bonne façon de satisfaire aux exigences des organismes de réglementation et d'assurer sa conformité. Mais ce n'est pas tout.

Un tel programme favorise la création d'une culture axée sur la protection de la vie privée à l'échelle de l'organisation. Le soutien de la haute direction est crucial pour réaliser cet objectif. Quand la haute direction fournit les ressources nécessaires pour assurer la formation et la sensibilisation appropriées, l'évaluation et le contrôle des risques et les activités de vérification qui s'imposent, elle envoie un message clair selon lequel la protection de la vie privée est essentielle à l'organisation. Une telle culture pousse les employés à appuyer et à renforcer les mesures de protection mises en place par l'organisation. Quand une organisation affirme que la protection de la vie privée lui est essentielle et qu'elle « prêche par l'exemple » en mettant en place un solide programme de gestion de la protection de la vie privée, le niveau de confiance des consommateurs et des clients augmente, ce qui est essentiel pour faire de bonnes affaires. Une organisation qui s'est dotée d'un solide programme de gestion de la protection de la vie privée peut bénéficier d'une meilleure réputation, ce qui lui donne un avantage concurrentiel. À long terme, un programme de gestion de la protection de la vie privée adapté aux besoins de l'organisation permettra d'économiser de l'argent, ce qui est profitable sur le plan des affaires.

À l'inverse, l'absence de bonnes mesures de protection des renseignements personnels mine la confiance des intervenants, ce qui nuit à l'organisation. Par exemple, les atteintes à la vie privée coûtent cher – tant sur le plan du « nettoyage » que sur le plan de la réputation qu'il faut alors rebâtir. Elles peuvent aussi se révéler très onéreuses pour les personnes touchées. La mise en place d'un bon programme de gestion de la protection de la vie privée peut permettre de réduire au minimum les risques, de maximiser la capacité de l'organisation de cerner les problèmes et d'y réagir et de réduire au minimum les préjudices.

Vu l'importante quantité de renseignements personnels conservés par les organisations et les institutions, la valeur économique croissante de ces renseignements et l'attention

et les préoccupations de plus en plus marquées concernant les atteintes à la vie privée, les organisations doivent absolument mettre en place des mesures pour élaborer et renforcer leurs programmes de gestion de la vie privée afin de réduire au minimum les risques et d'augmenter leur niveau de conformité.

Les Canadiens s'y attendent et le méritent.

Partie A Éléments constitutifs

Éléments de base de la responsabilité : Élaboration d'un programme de gestion de la protection de la vie privée complet

Que devrait faire une organisation pour s'assurer qu'elle gère bien les renseignements personnels en sa possession? Comment peut-elle savoir qu'elle le fait bien? De quelle façon peut-elle confirmer qu'elle est en mesure de se conformer aux exigences et de respecter ses obligations juridiques et le prouver à ses clients et aux commissaires à la protection de la vie privée?

Il y a un certain nombre d'exigences importantes liées à la responsabilité. Les organisations doivent nommer une personne responsable de surveiller l'élaboration, la mise en œuvre et le maintien du programme de gestion de la protection de la vie privée. Des politiques et des processus sont nécessaires, et la formation des employés est requise. Il faut conclure des contrats (ou utiliser d'autres moyens) relatifs au transfert de renseignements personnels à des tierces parties aux fins de traitement pour s'assurer que les renseignements communiqués sont protégés comme ils le seraient par l'organisation. On s'attend des organisations qu'elles mettent en place des systèmes pour répondre aux demandes des particuliers qui veulent avoir accès à leurs renseignements personnels ou les corriger. En outre, les organisations doivent pouvoir réagir aux plaintes de particuliers sur la protection des renseignements personnels.

Le Commissariat a élaboré un certain nombre d'outils que les organisations peuvent utiliser pour acquérir les connaissances de base sur la protection de la vie privée et la législation connexe. Parmi ces outils, mentionnons les suivants : *Guide à l'intention des entreprises et des organisations – Protection des renseignements personnels : vos responsabilités*, *Questionnaire sur la protection des renseignements personnels* et une vidéo pour les petites et moyennes entreprises intitulée *Protéger la vie privée de vos clients : LPRPDE pour les entreprises*.

L'Alberta a produit les documents suivants qui peuvent être utiles : *Guide for Businesses and Organizations on the Personal Information Protection Act*; *Information Privacy Rights* et *10 Steps to Implement PIPA*.

La Colombie-Britannique a aussi élaboré des outils semblables liés à la législation touchant le secteur privé, notamment : *What are My Organization's Responsibilities Under PIPA?* et *A Guide for Business and Organizations to BC's Personal Information Protection Act*.

Dans la partie A, on décrira les éléments constitutifs qui sont des composantes essentielles d'un programme de gestion de la protection de la vie privée en tous points conforme à la législation applicable au Canada en matière de protection des renseignements personnels dans le secteur privé.

1. Engagement de l'organisation

Le premier élément constitutif est l'élaboration d'une structure de gouvernance interne qui favorise une culture respectueuse de la vie privée.

On s'attend des organisations qu'elles élaborent et mettent en place des mesures de contrôle du programme qui permettent d'appliquer les principes de la protection des renseignements personnels des lois du gouvernement fédéral, de l'Alberta et de la Colombie-Britannique en matière de protection des renseignements personnels dans le secteur privé. Cependant, pour y arriver, les organisations doivent se doter d'une structure de gouvernance, de processus à respecter et de moyens pour confirmer leur application. À la base, pour être conforme et efficace, il faut adopter une culture respectueuse de la vie privée.

a) Participation de la haute direction

L'appui de la haute direction est essentiel à la réussite du programme de gestion de la protection de la vie privée et à l'adoption d'une culture respectueuse de la vie privée.

Quand la haute direction est déterminée à s'assurer que l'organisation respecte la législation sur la protection des renseignements personnels, le programme mis en place est plus susceptible d'être efficace, et il est plus probable que l'on puisse créer une culture respectueuse de la vie privée.

La haute direction doit promouvoir activement le programme de protection de la vie privée en faisant ce qui suit :

- nommer le ou les responsables en matière de protection de la vie privée (agent responsable de la protection de la vie privée);
- approuver les mesures de contrôle du programme;
- contrôler le programme et présenter des rapports au conseil, le cas échéant.

La haute direction doit aussi fournir les ressources nécessaires pour assurer la réussite du programme.

b) Agent responsable de la protection de la vie privée

Les organisations doivent nommer un responsable du programme de gestion de la protection de la vie privée.

Que ce soit un cadre de direction de niveau C d'une importante société ou le propriétaire/l'exploitant d'une très petite organisation, quelqu'un doit surveiller la conformité de l'organisation avec la législation applicable en matière de protection des renseignements personnels. D'autres personnes peuvent participer à la gestion des renseignements personnels, mais l'agent responsable de la protection de la vie privée est chargé de structurer, de concevoir et de gérer le programme, y compris toutes les procédures, la formation, le contrôle/la vérification, la documentation, l'évaluation et le suivi. Les organisations doivent affecter des ressources à la formation de l'agent. Celui-ci doit créer un programme qui garantira la conformité de l'organisation en le reliant à la législation applicable. Il est très important de montrer de quelle façon le programme sera géré à l'échelle de l'organisation.

Parmi les nombreux rôles de l'agent responsable de la protection de la vie privée, mentionnons les suivants :

- établir et appliquer les mesures de contrôle du programme;
- assurer la coordination avec les autres personnes responsables appropriées touchant les disciplines et les fonctions connexes au sein de l'organisation;
- être responsable de l'évaluation et de la révision continues des mesures de contrôle du programme;
- représenter l'organisation en cas d'enquête liée à une plainte réalisée par un commissariat à la protection de la vie privée;
- promouvoir le respect de la vie privée au sein de l'organisation elle-même.

Le dernier rôle mentionné est aussi important que les autres. Les organisations font souvent face à des intérêts contradictoires. La conformité en matière de protection de la vie privée n'est qu'un des programmes en place. Cependant, la protection des renseignements personnels ne se limite pas à trouver le juste équilibre entre les différents intérêts. Il faut l'envisager sur le plan de l'amélioration des processus, de la gestion des relations avec les clients et de la réputation. Par conséquent, il faut reconnaître à tous les niveaux l'importance du programme de gestion de la protection de la vie privée.

Il convient de signaler qu'une organisation reste responsable de la conformité avec la législation applicable en matière de protection des renseignements personnels, même si elle nomme une personne responsable du programme[4].

c) Bureau de la protection de la vie privée

Dans les grandes organisations, il faudra affecter du personnel à la gestion des enjeux liés à la protection de la vie privée.

Dans les grandes organisations, l'agent responsable de la protection de la vie privée aura besoin du soutien d'employés désignés. Il faut définir le rôle du bureau de la protection de la vie privée et cerner les ressources nécessaires. Le personnel du bureau doit avoir des responsabilités déléguées liées au contrôle de la conformité de l'organisation et à la promotion d'une culture respectueuse de la vie privée au sein de l'organisation. Il doit aussi s'assurer que la protection de la vie privée est intégrée dans toutes les fonctions principales qui utilisent des renseignements personnels, y compris l'élaboration de produits, les services à la clientèle ou les initiatives de commercialisation.

d) Préparation de rapports

L'organisation doit établir des mécanismes redditionnels et en tenir compte dans les mesures de contrôle de son programme.

L'organisation doit établir des mécanismes redditionnels internes pour s'assurer que les bonnes personnes connaissent la structure du programme de gestion de la protection de la vie privée et savent que tout fonctionne comme prévu. Dans les organisations relativement grandes, ce sont probablement les membres de la haute direction, qui relèvent du conseil d'administration, qui auront besoin de ces renseignements. Les mesures de contrôle du programme de l'organisation doivent refléter tous les mécanismes redditionnels.

Les organisations doivent créer des programmes de vérification interne/d'assurance pour contrôler la conformité avec leurs politiques en matière de protection des renseignements personnels. Cela peut inclure la rétroaction des clients et des employés dans les petites organisations ou, dans les grandes organisations, des vérifications effectuées par une tierce partie. Ces rapports serviront aussi si l'organisation fait l'objet d'une enquête ou d'une vérification aux termes d'une législation applicable en matière de protection des renseignements personnels parce qu'ils sont susceptibles de prouver que l'organisation a fait preuve de diligence raisonnable.

[4] http://www.priv.gc.ca/cf-dc/2001/cf-dc_011204_f.asp

Cependant, cela ne s'arrête pas là. Il arrive parfois que des enjeux liés à la protection de la vie privée soient transférés à l'échelon supérieur (p. ex. lorsqu'il y a une atteinte à la sécurité ou des plaintes de clients). Un tel processus exige la participation de personnes compétentes et l'assurance que tous les représentants nécessaires de l'organisation participent à la résolution. Dans de grandes organisations, cela peut inclure, par exemple, des représentants des domaines technique et juridique et des responsables des communications organisationnelles. Il faut définir et expliquer clairement à tous les employés quand et comment enclencher un tel processus. Pour s'assurer du respect des processus connexes, les organisations doivent confirmer que les mesures nécessaires sont prises au moment de l'activation (p. ex. certaines organisations ont trouvé utile de mettre à l'essai leurs protocoles de détermination, d'escalade et de confinement des atteintes à la vie privée).

Un programme redditionnel efficace :

- définit clairement la structure redditionnelle (en fait de rapport sur ses activités générales de conformité) et les structures redditionnelles des employés en cas de plainte ou d'une atteinte potentielle;
- est mis à l'essai, et on prépare des rapports sur les résultats de ses structures redditionnelles internes;
- documente toutes ses structures redditionnelles.

2. Mesures de contrôle du programme

Les mesures de contrôle du programme sont le deuxième élément constitutif. Elles permettent de garantir l'application au sein de l'organisation des éléments de la structure de gouvernance. La présente section définit les mesures de contrôle à appliquer dans le cadre d'un programme de gestion de la protection de la vie privée. L'élaboration de ces mesures de contrôle permettra à l'agent responsable de la protection de la vie privée de bien structurer son programme de gestion de la protection de la vie privée au sein de l'organisation et de bien définir les mesures de contrôle qui seront utilisées pour établir la conformité du programme avec la législation sur la protection des renseignements personnels.

a) Inventaire des renseignements personnels

Qu'elles comptent déjà sur un programme de gestion de la protection de la vie privée en place ou qu'elles en établissent un nouveau, les organisations bénéficieront toutes d'un examen minutieux des renseignements personnels qu'elles détiennent et de la façon dont elles les gèrent.

Une organisation doit connaître les renseignements personnels en sa possession, savoir comment elle les utilise et déterminer si elle en a réellement besoin. Il est extrêmement important de comprendre et de documenter les types de renseignements personnels recueillis et leurs conditions de conservation. Cela a un impact sur le type de consentement que l'organisation doit obtenir des personnes et sur la façon dont les renseignements sont protégés. En outre, il sera ainsi plus facile d'aider les personnes qui exercent leur droit d'accès et de correction. La création des composantes d'un programme de gestion de la protection de la vie privée conforme et responsable commence par une telle évaluation.

Cependant, il n'est pas toujours facile de déterminer ce qui est considéré comme des renseignements personnels et ce qui ne l'est pas. Le Commissariat a produit une interprétation utile sur la définition de renseignements personnels. Il résume les diverses décisions rendues par les tribunaux et les constatations du Commissariat liées à la définition. Qu'ils soient de nature délicate (comme des renseignements financiers ou liés à la santé) ou non, tous les renseignements personnels doivent être protégés adéquatement et utilisés uniquement aux fins pour lesquelles ils ont été recueillis. Il se peut qu'il faille accorder un traitement spécial aux renseignements de nature délicate[5].

Chaque organisation doit déterminer ce qui suit :

- les renseignements qu'elle détient et où elle les conserve (au sein de l'organisation ou auprès d'une tierce partie, par exemple); il faut aussi documenter cette évaluation;
- pourquoi elle recueille, utilise ou communique des renseignements personnels; il faut aussi documenter ces raisons;
- la nature délicate des renseignements personnels conservés.

Un document intitulé *Protégez les renseignements personnels : Un outil d'auto-évaluation à l'intention des organisations*, produit par les commissariats, porte aussi sur les enjeux touchant la détermination des renseignements personnels conservés.

b) Politiques

Les organisations doivent élaborer et documenter des politiques internes relatives aux obligations législatives. Ces politiques doivent être accessibles aux employés, et les employés doivent les signer de temps en temps.

[5]Certains renseignements personnels sont presque toujours considérés comme de nature délicate, comme les renseignements financiers et sur la santé. D'autres renseignements personnels peuvent être considérés comme étant de nature délicate, selon le contexte. Les renseignements personnels de nature délicate peuvent exiger des mesures de protection plus poussées et l'obtention du consentement éclairé.

Les organisations doivent élaborer des politiques internes pour appliquer les principes contenus dans la législation canadienne sur la protection des renseignements personnels dans le secteur privé. Il faut documenter ces politiques et préciser en quoi elles sont liées à la législation applicable sur la protection des renseignements personnels.

Les organisations doivent élaborer des politiques internes pour appliquer les principes contenus dans la législation canadienne sur la protection des renseignements personnels dans le secteur privé.

Les principales politiques dont les organisations doivent se munir sont les suivantes :

(i) collecte, utilisation et communication des renseignements personnels, y compris les exigences en matière de consentement et d'avis;
(ii) accès aux renseignements personnels et leur correction;
(iii) conservation et élimination des renseignements personnels;
(iv) utilisation responsable des renseignements et des technologies de l'information, y compris les mesures de contrôle de sécurité administratives, physiques et technologiques et le contrôle approprié de l'accès;
(v) possibilité de porter plainte à l'égard du non-respect des principes.

Les organisations doivent aussi intégrer des exigences liées à la conformité en matière de protection de la vie privée dans certaines autres de leurs politiques, le cas échéant (p. ex. dans les politiques sur la gestion des contrats, d'approvisionnement et liées aux ressources humaines et des politiques liées à la communication des renseignements personnels aux organismes de réglementation, aux organismes d'application de la loi et aux ministères responsables de la sécurité nationale).

Nous avons analysé chacune des politiques clés ci-dessous.

(i) Collecte, utilisation et communication des renseignements personnels, y compris les exigences en matière de consentement et d'avis

Il faut que les employés comprennent leur obligation d'informer les personnes de la raison pour laquelle ils recueillent, utilisent et communiquent des renseignements personnels et d'obtenir leur consentement. La législation sur la protection des renseignements personnels exige que l'on recueille, utilise et communique uniquement des renseignements personnels à des fins appropriées.

(ii) Accès aux renseignements personnels et leur correction

Les employés doivent savoir que les personnes ont le droit d'avoir accès à leurs renseignements personnels et de les corriger et comment aider les consommateurs et

les employés à exercer ce droit en sachant quels sont les processus à suivre, y compris les délais que l'organisation doit respecter.

(iii) *Conservation et élimination des renseignements personnels*

Afin de réduire au minimum la collecte, l'utilisation et la communication interdites de renseignements, les organisations ne doivent pas conserver les renseignements personnels dont ils n'ont plus besoin dans le cadre de la prestation de leurs services. Elles doivent aussi avoir une politique sur l'élimination ou la destruction des dossiers. Les clients s'attendent à ce qu'une organisation détruise leurs renseignements personnels qui ne sont plus nécessaires. Par conséquent, conformément à cette politique, il faut s'assurer d'éliminer de façon sécuritaire les dossiers des clients.

(iv) Utilisation responsable des renseignements et des technologies de l'information, y compris les mesures de contrôle de sécurité administratives, physiques et technologiques et le contrôle approprié de l'accès

Les organisations doivent protéger les renseignements personnels qu'elles détiennent en mettant en place des mesures de sécurité raisonnables. Ce qui est considéré comme raisonnable varie en fonction de la nature délicate des renseignements. Des mesures de sécurité pourraient inclure, par exemple, des classeurs verrouillés, des mesures de contrôle de l'accès et le chiffrement pour protéger les bases de données électroniques. Il s'agit d'une responsabilité très importante, et, dans la plupart des cas, il faut une expertise technique spécialisée pour concevoir un système approprié.

Le contrôle de l'accès en fonction des rôles est l'une des meilleures méthodes que peuvent utiliser les organisations pour limiter l'accès aux renseignements. Conformément au principe du « besoin de savoir », les employés doivent uniquement avoir accès aux renseignements personnels dont ils ont besoin pour s'acquitter de leurs tâches au sein de l'organisation. Il faut bien documenter les rôles, tenir à jour le registre et accorder l'accès de façon uniforme, préférablement par une instance centralisée au sein de l'organisation.

Les trois lois exigent la mise en place de mesures de protection des renseignements personnels.

Le Commissariat, et les CIPVP de l'Alberta et de la Colombie-Britannique ont produit un document sur la protection des renseignements personnels dont l'objectif est d'aider les organisations, particulièrement les petites et moyennes entreprises à réfléchir aux divers aspects de leurs activités qui peuvent avoir un impact sur la sécurité et les renseignements personnels. Nous recommandons aux organisations d'utiliser cet outil.

(v) Possibilité de porter plainte à l'égard du non-respect des principes

Les personnes ont le droit de remettre en question la conformité des organisations avec la législation applicable en matière de protection des renseignements personnels. Par conséquent, les organisations doivent se doter de politiques internes à l'intention de leurs employés qui s'appliquent si une personne veut déposer une plainte au sujet des pratiques de gestion des renseignements personnels de l'organisation.

c) Outil d'évaluation du risque

Les risques liés à la vie privée évoluent au fil du temps. Le fait de réaliser, au minimum, des évaluations du risque chaque année est une partie importante de tout programme de gestion de la protection de la vie privée pour s'assurer que l'organisation respecte la législation applicable.

Nous avons constaté que, parfois des organisations offrent de nouveaux services dans le cadre desquels ils recueillent, utilisent et communiquent des renseignements personnels sans avoir procédé à des examens minutieux au chapitre de la protection de la vie privée. L'utilisation appropriée d'outils d'évaluation du risque peut éliminer de tels problèmes. Régler un problème lié à la protection de la vie privée après coup peut être très coûteux. Par conséquent, il est essentiel de bien évaluer les objectifs d'une initiative, d'un produit ou d'un service de façon à réduire d'emblée au minimum les répercussions sur la protection de la vie privée.

C'est pourquoi il faut réaliser de telles évaluations à l'échelle de l'organisation dans le cadre de tous les nouveaux[6] projets liés aux renseignements personnels ou à la collecte, à l'utilisation et à la communication de nouveaux renseignements personnels. Les organisations doivent élaborer un processus pour cerner les risques liés à la protection de la vie privée et à la sécurité et les atténuer, y compris en utilisant des évaluations de l'impact sur la protection de la vie privée et des évaluations du risque de menace pour la sécurité.

Lorsqu'elles conçoivent de nouvelles initiatives, de nouveaux services ou de nouveaux programmes, les organisations devraient élaborer des procédures pour réaliser de telles évaluations et définir un processus d'examen et d'approbation qui fait intervenir l'agent responsable de la protection de la vie privée ou le bureau de protection de la vie privée. Dans les grandes organisations, l'agent responsable de la protection de la vie privée doit connaître le processus d'examen. En outre, le bureau de la protection de la vie privée devrait participer directement lorsqu'il est question d'initiatives, de services ou de programmes à risque élevé.

[6]Le nouveau projet peut porter sur la modification de systèmes, de composantes et de processus.

d) Exigences en matière de formation et de sensibilisation

Un bon programme de gestion de la protection de la vie privée exige que tous les membres de l'organisation soient au courant des obligations en matière de protection de la vie privée et soient prêts à les respecter. Des exigences en matière de formation et de sensibilisation à jour et adaptées aux besoins pour tous les employés sont essentielles à la conformité.

Pour qu'un programme de gestion de la protection de la vie privée soit efficace, les employés doivent participer activement à la protection de la vie privée. Ils doivent être sensibilisés à la protection de la vie privée en général. En outre, ceux qui manipulent directement des renseignements personnels doivent suivre des cours de formation supplémentaires adaptés à leur rôle. La formation et la sensibilisation doivent être récurrentes, et il faut revoir de temps en temps le contenu du programme pour le mettre à jour en fonction des changements survenus.

La formation et la sensibilisation générale sur la protection de la vie privée sont très importantes. Nous avons vu des situations dans le cadre desquelles des organisations ne reconnaissaient pas que des enjeux étaient liés à la protection de la vie privée. Par conséquent, elles n'ont pas pris de mesures appropriées pour prévenir ou régler les atteintes à la vie privée[7]. Dans d'autres cas, nous avons vu des employés qui ne comprenaient pas suffisamment les risques ou n'y étaient pas suffisamment sensibles, ce qui a fait en sorte qu'ils ont élaboré des produits ou des services qui ne respectaient pas les lois applicables en matière de protection des renseignements personnels[8]. En Alberta, l'erreur humaine est la cause la plus courante des atteintes déclarées qui entraînent un risque réel et un préjudice important à des particuliers. Mentionnons, par exemple, des documents envoyés par télécopieur au mauvais numéro et des courriels envoyés à la mauvaise adresse, des adresses de courriel visibles dans un envoi massif, l'élimination inappropriée de documents et la communication de mots de passe.

Les employés seront en meilleure position pour protéger la vie privée lorsqu'ils pourront reconnaître les situations liées à la protection des renseignements personnels. Les organisations peuvent se doter de très bonnes politiques et de très bonnes mesures de contrôle; cependant, si les employés ne les respectent pas, le programme de gestion de la protection de la vie privée reste lettre morte. Il faut que les employés signent un accord selon lequel ils respecteront les politiques et les mesures de contrôle du programme de l'organisation.

[7]Par exemple, http://www.priv.gc.ca/cf-dc/incidents/2005/050418_01_f.asp.
[8]Par exemple, http://www.priv.gc.ca/cf-dc/2011/2011_001_0520_f.asp, lié à la collecte par Google de renseignements personnels à partir de réseaux wifi non chiffrés.

Il y a de nombreuses méthodes que peuvent utiliser les organisations pour offrir des cours de formation ou de sensibilisation générale sur la protection de la vie privée. Elles peuvent, par exemple, fournir des modules de formation obligatoires sur l'intranet de l'entreprise, organiser des séances en petits groupes, tenir des séances de formation en tête-à-tête, produire des communiqués électroniques mensuels ou insérer des modules dans la formation sur les politiques de l'organisation. L'organisation doit documenter ses processus de formation et mesurer les taux de participation et de réussite connexes.

Pour que les cours de formation et de sensibilisation sur la protection de la vie privée soient efficaces, il faut :

- qu'ils soient obligatoires pour tous les nouveaux employés avant qu'ils puissent avoir accès à des renseignements personnels et périodiquement par la suite;
- qu'ils portent sur les politiques et les procédures établies par l'organisation;
- qu'ils soient offerts de la façon la plus appropriée et efficace en fonction des besoins de l'organisation;
- qu'ils permettent de communiquer des renseignements essentiels aux employés pertinents dès que possible et en cas d'urgence.

e) Protocoles d'intervention/de gestion en cas d'atteinte ou d'incident

Les évaluations des risques internes et externes peuvent aider à réduire le nombre d'atteintes à la vie privée qui, malheureusement, font de plus en plus la une. Comme nous l'avons déjà dit, de telles situations sont onéreuses à de nombreux égards et minent la confiance des consommateurs.

En Alberta, une organisation qui détient des renseignements personnels doit, sans retard déraisonnable, fournir un avis au commissaire en cas d'incidents liés à la perte ou la communication d'un renseignement personnel ou à l'accès sans autorisation à de tels renseignements, quand on peut raisonnablement s'attendre à ce qu'il y ait un risque réel de préjudice important pour une personne découlant de la perte, de l'accès non autorisé ou de la communication.

Par conséquent, les organisations doivent mettre en place une procédure et nommer une personne responsable de la gestion des atteintes à la vie privée. Dans les grandes organisations, une approche axée sur la collaboration qui fait intervenir les employés de différentes parties de l'organisation peut être requise. Il faut définir clairement les responsabilités en matière de déclarations internes et externes des violations.

Il se peut aussi qu'il faille aviser les commissaires à la protection de la vie

privée et les personnes touchées. Les organisations exploitées en Alberta ou qui recueillent les renseignements personnels des Albertains doivent, aux termes de la loi, déclarer certaines violations au commissaire à l'information et à la protection de la vie privée de l'Alberta. Que la déclaration soit obligatoire ou non dans une administration précise, on encourage les organisations à déclarer les violations aux intervenants appropriés.

Pour plus de directives sur les attentes concernant les atteintes, veuillez consulter les documents *Privacy Breach Checklist*, *Breach Notification Assessment Tool*, *Key Steps in Responding to Privacy Breaches*, de la Colombie-Britannique, les documents *Reporting a Breach to the Commissioner*, *Breach Report Form* et *Notifying Affected Individuals*, de l'Alberta, et le document *Guide en matière d'atteinte à la vie privée*, du Commissariat.

f) Gestion des fournisseurs de services

La manipulation des renseignements personnels par des tierces parties est un autre élément dont il faut tenir compte. Y a-t-il des contrats ou d'autres dispositifs mis en place pour protéger les renseignements personnels? Des renseignements quittent-ils le pays? Dans l'affirmative, est-ce que l'organisation a tenu compte de la nature délicate des renseignements et des exigences du régime à l'étranger? Les *Lignes directrices sur le traitement transfrontalier des données personnelles* du Commissariat fournissent des renseignements supplémentaires sur la responsabilité et l'utilisation des organisations de traitement et de communication de données transfrontalières.

La loi précise que les organisations qui transmettent des renseignements personnels à une tierce partie aux fins de traitement sont responsables des renseignements personnels communiqués. Elles peuvent utiliser des contrats ou d'autres moyens en guise de protection. Il se peut qu'elles doivent inclure de l'information sur la destination des renseignements et les motifs de communication dans leurs politiques et leurs procédures.

Il faut tenir compte de cela dans le cadre de l'évaluation du risque. Au minimum, les exigences en matière de protection de la vie privée imposées aux fournisseurs de services devraient inclure les éléments suivants :

- dispositions relatives à la protection de la vie privée dans les contrats qui définissent les exigences en matière de conformité, y compris le respect par les fournisseurs de services des politiques et des protocoles de l'organisation et le fait que l'organisation doit être informée en cas d'atteinte;

- la formation et la sensibilisation de tous les employés du fournisseur de services qui ont accès à des renseignements personnels;
- de la sous-traitance;
- les vérifications et les ententes signées avec les employés du fournisseur de services indiquant qu'ils respecteront les politiques et les protocoles en matière de protection de la vie privée de l'organisation.

g) Communication externe

Les organisations doivent aussi se doter d'une procédure pour informer les personnes de leurs droits en matière de vie privée et des mesures de contrôle du programme de l'organisation. Ce type de communication externe devrait être clair et compréhensible et ne pas réitérer tout simplement la loi. Il doit faire ce qui suit :

- fournir suffisamment de renseignements pour que les membres du grand public comprennent le but de la collecte, de l'utilisation et de la communication des renseignements personnels ainsi que leur protection et durée de rétention;
- informer les personnes si leurs renseignements personnels sont communiqués à l'extérieur du Canada;
- inclure les coordonnées de la personne-ressource à qui faire part des questions ou des préoccupations;
- être facilement accessible aux personnes.

Il faut dire aux personnes qu'elles ont le droit d'avoir accès à leurs renseignements personnels conservés par l'organisation. Il faut leur décrire la procédure pour demander des corrections ou se plaindre au sujet de la conformité de l'organisation en matière de protection de la vie privée, y compris le droit de remettre en question les gestes de l'organisation en présentant une plainte à la commissaire à la protection de la vie privée.

Le Commissariat a élaboré un certain nombre de documents utiles que peuvent utiliser les organisations pour élaborer des politiques internes et des communications externes. Mentionnons les suivantes : *Concevez un plan de protection de la vie privée – En fonction des besoins de votre entreprise*, *Outil d'autoévaluation – LPRPDE*, *Guide pour la petite entreprise : Rudiments de la protection de la vie privée*, *Lignes directrices sur le traitement transfrontalier des données personnelles*, *La protection de la vie privée au sein de votre entreprise – Guide en matière d'atteinte à la vie privée* et *Guide à l'intention des entreprises et des organisations – Protection des renseignements personnels : vos responsabilités*.

L'Alberta a élaboré les documents suivants : *Key Steps in Responding to Privacy Breaches*, *PIPA Advisory 2: Access Requests: An Overview*, *PIPA Advisory 3: Access*

Requests: Responding to a Request et *PIPA Advisory 8: Access Requests: Reasonable Safeguards*.

La Colombie-Britannique a élaboré les documents suivants : *Privacy Breach Management Policy Template*, *Key Steps in Responding to Privacy Breaches*, *Breach Notification Assessment tool* et *PIPA and the Hiring Process*.

Partie B Évaluation continue et révision

Dans la partie A, nous avons décrit les éléments constitutifs d'un programme de gestion de la protection de la vie privée. Dans la partie B, nous allons décrire les tâches essentielles liées au maintien du programme de gestion de la protection de la vie privée pour nous assurer qu'il reste efficace, conforme et responsable. Afin de bien protéger la vie privée et de respecter les obligations législatives, les organisations doivent contrôler, évaluer et réviser leur cadre pour s'assurer qu'il reste pertinent et efficace. Afin d'y arriver, il faut affecter suffisamment de ressources à l'agent responsable de la protection de la vie privée et prévoir suffisamment de cours de formation.

1. Élaborer un plan de surveillance et de révision

Un plan de surveillance et de révision permettra à l'organisation de veiller à ce que son programme de gestion de la protection de la vie privée soit sur la bonne voie et à jour.

L'agent responsable de la protection de la vie privée doit élaborer un plan de surveillance et de révision annuel qui établit comment et quand il surveillera et évaluera l'efficacité du programme de gestion de la protection de la vie privée de l'organisation conformément aux engagements de l'organisation. Le plan doit définir les mesures de rendement et inclure un calendrier de révision de toutes les politiques et de toutes les autres mesures de contrôle du programme.

2. Évaluer et réviser les mesures de contrôle du programme

Il faut contrôler, vérifier de temps à autre et, au besoin, réviser l'efficacité des mesures de contrôle du programme.

Le contrôle est un processus continu qui devrait permettre de répondre, au minimum, aux questions suivantes :

- Quelles sont les dernières menaces et quels sont les derniers risques?

- Est-ce que les mesures de contrôle du programme permettent de gérer les nouvelles menaces et reflètent les dernières constatations liées aux plaintes ou découlant des vérifications ou encore l'orientation des commissaires à la protection de la vie privée?
- Offre-t-on de nouveaux services qui exigent une collecte, une utilisation ou une communication accrue de renseignements personnels?
- Offre-t-on de la formation? Est-elle efficace? Respecte-t-on les politiques et les procédures? Le programme est-il à jour?

Si on découvre des problèmes durant le processus de contrôle, il faut documenter les préoccupations et s'assurer que les intervenants appropriés y donnent suite.

En ce qui a trait aux processus critiques ou à risque élevé, les vérifications internes ou externes régulières sont une bonne façon d'évaluer l'efficacité du programme de protection de la vie privée de l'organisation. Cependant, l'agent responsable de la protection de la vie privée devrait, au minimum, réaliser des évaluations régulières pour veiller au respect des processus clés. Dans les petites organisations ou dans le cadre d'examens moins officiels, les organisations pourraient élaborer des listes de vérification révisées régulièrement. Quels que soient les moyens appropriés utilisés, les organisations doivent s'assurer que les employés et les entrepreneurs respectent les politiques et les mesures de contrôle du programme de l'organisation.

Comme nous l'avons déjà dit, le présent document n'est pas une solution « universelle ». Chaque organisation doit déterminer la structure appropriée de son programme de gestion de la protection de la vie privée en tenant compte d'un certain nombre de facteurs, y compris sa taille, la quantité de renseignements personnels manipulés et leur nature délicate.

Quand les organisations commencent à élaborer leur programme de gestion de la protection de la vie privée, il se peut qu'elles ne mettent pas immédiatement en place tous les éléments d'un programme conforme. Même les organisations qui n'en sont pas à leurs premières armes en la matière doivent s'assurer de prendre des mesures raisonnables pour maintenir le niveau de conformité. Il est important pour les organisations d'évaluer le progrès en utilisant des mesures, avec pour objectif le maintien de la conformité.

On s'attend à ce qu'une organisation réalise des évaluations de ses mesures de contrôle du programme (conformément à la Partie A) de façon ciblée, continue et minutieuse.

À la lumière des résultats du processus d'évaluation, l'agent responsable de la protection de la vie privée doit déterminer s'il y a des mesures à prendre pour mettre à

jour ou réviser les mesures de contrôle du programme. Il s'agit d'une responsabilité cruciale. Les changements doivent être communiqués aux employés au moment où ils sont apportés ou dans le cadre de modules de sensibilisation et de formation « d'appoint ».

Bref, l'agent responsable de la protection de la vie privée doit prendre les mesures suivantes :

a) **contrôler et mettre à jour continuellement l'inventaire des renseignements personnels** pour en assurer l'actualité et cerner et évaluer les nouveaux cas de collecte, d'utilisation et de communication;

b) **examiner et réviser les politiques** au besoin, à la suite d'évaluations de vérification, en réponse à une atteinte ou une plainte, en fonction d'une nouvelle orientation ou de nouvelles pratiques exemplaires de l'industrie ou à la suite d'analyses environnementales. On ne peut pas surévaluer l'importance de ce travail. Rien ne sert d'avoir des politiques si elles ne sont ni efficaces ni pertinentes – ou si personne au sein d'une organisation ne les connaît;

c) **traiter les évaluations d'impact sur la vie privée et les évaluations des menaces et des risques à la sécurité comme des documents à caractère évolutif** de façon à ce que l'on cerne toujours les risques liés à la vie privée et à la sécurité, les modifications ou les nouvelles initiatives au sein de l'organisation et qu'on en tienne compte;

d) **examiner et modifier les cours de formation et de sensibilisation** régulièrement à la lumière d'évaluations continues et communiquer les changements apportés aux mesures de contrôle du programme;

e) **examiner et adapter les protocoles d'intervention/de gestion en cas d'atteinte et d'incident** pour mettre en œuvre les pratiques exemplaires ou les recommandations et les leçons apprises d'examens réalisés à la suite d'incidents;

f) **examiner et**, au besoin, **peaufiner** les exigences dans les contrats conclus avec les **fournisseurs de services**;

g) **mettre à jour et clarifier les communications externes** expliquant les politiques en matière de protection de la vie privée.

Conclusion

Prouver la conformité

Les organisations responsables peuvent prouver qu'elles ont mis en œuvre un programme de gestion de la protection de la vie privée complet.

Le présent document décrit les éléments et les stratégies d'un programme de gestion de la protection de la vie privée qui peuvent aider les organisations à se responsabiliser comme il se doit. Grâce à un tel programme, les organisations peuvent prouver à leurs clients, à leurs employés, à leurs partenaires, aux actionnaires et aux commissaires à la protection de la vie privée qu'ils ont mis en place un solide programme de conformité en matière de vie privée. Elles pourront décrire et documenter tous les éléments abordés dans le présent document d'orientation et prouver de quelle façon elles ont mis en œuvre leur programme.

Dans le cadre d'une enquête au sujet d'une plainte ou d'une possible violation de la loi ou dans le cadre d'une vérification des pratiques, un commissariat à la protection de la vie privée peut demander à une organisation d'expliquer de quelle façon elle s'y prend pour respecter les exigences législatives applicables. L'agent responsable de la protection de la vie privée doit bien documenter le programme au cas où cela se produit. Durant une enquête ou une vérification, nos commissariats s'attendront à ce que les organisations puissent prouver qu'elles ont mis en place un programme à jour et complet en matière de protection de la vie privée. Les éléments probants liés à la présence d'un programme efficace de gestion de la vie privée aideront les commissaires à déterminer si, oui ou non, une organisation a mis des mesures de protection raisonnables en place et si elle a respecté les exigences d'une loi applicable en matière de responsabilité.

Les organisations qui ne répondent pas aux attentes auront plus de travail à faire pour créer un tel programme ou le mettre à jour.

Au-delà de la loi – Pourquoi la vie privée est-elle importante aux affaires

Beaucoup de personnes tiennent à leur vie privée et considèrent que la protection de la vie privée est un droit fondamental de la personne. Au sein d'une organisation, la protection de la vie privée est essentielle pour favoriser et maintenir la confiance. Si les consommateurs, les clients ou les employés croient que leurs renseignements personnels seront manipulés de façon respectueuse, ouverte et transparente, qu'il y

aura de solides et raisonnables mesures de protection en place et qu'ils y auront accès sur demande, cela favorise la confiance et la poursuite d'une relation positive. Si les clients sont bel et bien l'atout le plus important d'une entreprise, alors il en va de même pour leurs renseignements personnels. Les organisations veulent renforcer et protéger leurs atouts, et les renseignements personnels, en tant que tels, n'échappent pas à la règle.

Une organisation responsable peut prouver à ses clients, ses employés, ses actionnaires, les organismes de réglementation et ses compétiteurs qu'elle tient à la protection de la vie privée, pas seulement à des fins de conformité, mais aussi parce que la protection de la vie privée favorise une saine gestion des affaires. Nous espérons que les directives contenues dans le présent document aideront toutes les organisations à réaliser cet objectif.

Aperçu d’un programme de gestion de la protection de la vie privée

A. Éléments constitutifs

Engagement organisationnel	**a) Participation de la haute direction**	L’appui de la haute direction est essentiel à la réussite du programme de gestion de la protection de la vie privée et à l’adoption d’une culture respectueuse de la vie privée.
	b) Agent responsable de la protection de la vie privée	• Le rôle existe et est essentiel au processus décisionnel opérationnel. • Les rôles et les responsabilités en matière de contrôle de la conformité sont définis et communiqués clairement à l’échelle de l’organisation. • Responsable de l’élaboration et de la mise en œuvre des mesures de contrôle du programme et de leur évaluation et révision continue.
	c) Bureau de la protection de la vie privée	• Le rôle est défini, et les ressources sont cernées et adéquates. • La structure organisationnelle renforce la capacité du personnel de contrôler la conformité et de créer une culture de respect de la vie privée au sein de l’organisation. • S’assure que la protection de la vie privée est intégrée à toutes les fonctions principales dans le cadre desquelles on utilise des renseignements personnels.
	d) Préparation de rapports	L’organisation doit établir des mécanismes redditionnels et en tenir compte dans les mesures de contrôle de son programme.

<table>
<tr><td rowspan="3">Mesures de contrôles du programme</td><td>a) Inventaire des renseignements personnels</td><td>L’organisation est en mesure de déterminer :
les renseignements personnels qu’elle possède ou contrôle;
son pouvoir de recueillir, d’utiliser et de communiquer des renseignements personnels;
la nature délicate des renseignements personnels.</td></tr>
<tr><td>b) Politiques</td><td>(i) collecte, utilisation et communication des renseignements personnels, y compris les exigences en matière de consentement et d’avis;
(ii) accès aux renseignements personnels et leur correction;
(iii) conservation et élimination des renseignements personnels;
(iv) utilisation responsable des renseignements et des technologies de l’information, y compris les mesures de contrôle de sécurité administratives, physiques et technologiques et le contrôle approprié de l’accès;
(v) possibilité de porter plainte à l’égard du non-respect des principes.</td></tr>
<tr><td colspan="2">c) Outil d’évaluation du risque
d) Exigences en matière de formation et de sensibilisation
e) Protocoles d’intervention/de gestion en cas d’atteinte ou d’incident
f) Gestion des fournisseurs de services
g) Communication externe</td></tr>
</table>

B. Évaluation et révision continues

Plan de surveillance et de révision	**a) Élaborer un plan de surveillance et de révision**	L'agent responsable de la protection de la vie privée doit élaborer un plan de surveillance et de révision annuel qui établit comment et quand il surveillera et évaluera l'efficacité des mesures de contrôle du programme de l'organisation.
Évaluer et réviser les mesures de contrôle du programme au besoin	**a) Mettre à jour l'inventaire des renseignements personnels** **b) Réviser les politiques** **c) Traiter les outils d'évaluation du risque comme des documents à caractère évolutif** **d) Modifier les cours de formation et de sensibilisation** **e) Adapter les protocoles d'intervention en cas d'atteinte et d'incident** **f) Peaufiner la structure de gestion des fournisseurs de services** **g) Améliorer les communications externes**	

Annexe A

Documents préparés par le Commissariat à la protection de la vie privée du Canada et les commissaires à l'information et à la protection de la vie privée de l'Alberta et de la Colombie-Britannique cités dans le présent document d'orientation

Liste des documents préparés par le Commissariat à la protection de la vie privée du Canada

Renseignements généraux pour les entreprises sur la protection de la vie privée

Protection des renseignements personnels : vos responsabilités – Guide à l'intention des entreprises et des organisations
http://www.priv.gc.ca/information/guide_f.asp

Questionnaire sur la protection des renseignements personnels?
http://www.priv.gc.ca/resource/tool-outil/ekit/quest_01_f.asp

Protégez la vie privée de vos clients : la LPRPDE pour les entreprises (vidéo pour les petites et moyennes entreprises)
http://www.priv.gc.ca/resource/videos/2010/bus_2010_index_f.asp

Interprétations

La responsabilité
http://www.priv.gc.ca/leg_c/interpretations_02_acc_f.asp

Renseignements personnels
http://www.priv.gc.ca/leg_c/interpretations_02_f.asp

Atteintes à la vie privée

Guide en matière d'atteinte à la vie privée
http://www.priv.gc.ca/resource/pb-avp/pb_hb_f.asp

Communication transfrontalière de renseignements personnels/externalisation

Lignes directrices sur le traitement transfrontalier des données personnelles
http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_f.asp

Politiques internes et communications externes

Concevez un plan de protection de la vie privée
http://www.priv.gc.ca/resource/tool-outil/francais/index.asp?a=logout

Outil d'autoévaluation – LPRPDE
http://www.priv.gc.ca/information/pub/ar-vr/pipeda_sa_tool_200807_f.asp

Guide pour la petite entreprise : Rudiments de la protection de la vie privée
http://www.priv.gc.ca/information/pub/guide_sb_f.asp

Lignes directrices sur le traitement transfrontalier des données personnelles
http://www.priv.gc.ca/information/guide/2009/gl_dab_090127_f.asp

La protection de la vie privée au sein de votre entreprise – Guide en matière d'atteinte à la vie privée
http://www.priv.gc.ca/resource/pb-avp/pb_hb_f.asp

Protection des renseignements personnels : vos responsabilités – Guide à l'intention des entreprises et des organisations
http://www.priv.gc.ca/information/guide_f.asp

Liste des documents préparés par le Commissariat à l'information et à la protection de la vie privée de l'Alberta

Renseignements généraux pour les entreprises sur la protection de la vie privée

Guide for Businesses and Organizations on the Personal Information Protection Act
http://www.oipc.ab.ca/Content_Files/Files/Publications/PIPAguide_Nov2008_web.pdf

Information Privacy Rights
http://www.oipc.ab.ca/Content_Files/Files/Publications/Information_Privacy_Right_2007.pdf

10 Steps to Implement PIPA
http://servicealberta.ca/pipa/documents/ImplementPIPA.pdf

Atteintes à la vie privée

Reporting a Breach to the Commissioner
http://www.oipc.ab.ca/Content_Files/Files/Publications/Reporting_a_Breach_to_the_Commissioner.pdf

Breach Report Form
http://www.oipc.ab.ca/Content_Files/Files/Publications/Breach_Report_Form_2010.pdf

Notifying Affected Individuals
http://www.oipc.ab.ca/Content_Files/Files/Publications/Notifying_Affected_Individuals.pdf

Politiques internes et communications externes

Key Steps in Responding to Privacy Breaches
http://www.oipc.ab.ca/Content_Files/Files/Publications/Key_Steps_in_Responding_to_a_Privacy_Breach.pdf

PIPA Advisory 2: Access Requests: An Overview
http://www.oipc.ab.ca/Content_Files/Files/Publications/2JCRightofAccessRequestsAnOverviewApr2007.pdf

PIPA Advisory 3: Access Requests: Responding to a Request
http://www.oipc.ab.ca/Content_Files/Files/Publications/3_JC_Right_of_Access_Requests_Responding_to_a_Request_Apr2007.pdf

PIPA Advisory 8: Access Requests: Reasonable Safeguards
http://www.oipc.ab.ca/Content_Files/Files/Publications/PIPA_Advisory_8_Reasonable_Safeguards2007.pdf

Liste des documents préparés par le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique

Renseignements généraux pour les entreprises sur la protection de la vie privée

What are My Organization's Responsibilities Under PIPA?
http://www.oipc.bc.ca/index.php?option=com_content&view=article&catid=17%3Aprivate-sector-pages&id=73%3Aprivate-sector-g-what-are-my-organizations-responsibilities-under-pipa&Itemid=78

A Guide for Business and Organizations to BC's Personal Information Protection Act.
http://www.oipc.bc.ca/pdfs/private/a-_GUIDE_TO_PIPA%283rd_ed%29.pdf

Atteintes à la vie privée

Privacy Breach Checklist
http://www.oipc.bc.ca/pdfs/Policy/Privacy_Breach_Checklist%28June2008%29.pdf

Breach Notification Assessment Tool

http://www.oipc.bc.ca/pdfs/Policy/ipc_bc_ont_breach.pdf

Key Steps in Responding to Privacy Breaches
http://www.oipc.bc.ca/pdfs/Policy/Key_Steps_Privacy_Breaches%28June2008%29.pdf

Politiques internes et communications externes

Privacy Breach management Policy Template
http://www.oipc.bc.ca/pdfs/Policy/Privacy_Breach_Management_Policy_Template%28June2008%29.pdf

Key Steps in Responding to Privacy Breaches
http://www.oipc.bc.ca/pdfs/Policy/Key_Steps_Privacy_Breaches%28June2008%29.pdf

Breach Notification Assessment tool
http://www.oipc.bc.ca/pdfs/Policy/ipc_bc_ont_breach.pdf

PIPA and the Hiring Process
http://www.oipc.bc.ca/pdfs/private/PIPAHiringFAQ(10APR06).pdf

Document d'orientation conjoint

Protéger les renseignements personnels : Un outil d'auto-évaluation à l'intention des organisations
http://www.priv.gc.ca/resource/tool-outil/security-securite/francais/AssessRisks.asp?x=1

Annexe B

Le principe de la responsabilité de l'annexe 1 de la LPRPDE est ainsi libellé :

4.1 Premier principe — Responsabilité

Une organisation est responsable des renseignements personnels dont elle a la gestion et doit désigner une ou des personnes qui devront s'assurer du respect des principes énoncés ci-dessous.

4.1.1

Il incombe à la ou aux personnes désignées de s'assurer que l'organisation respecte les principes même si d'autres membres de l'organisation peuvent être chargés de la collecte et du traitement quotidiens des renseignements personnels. D'autres membres de l'organisation peuvent aussi être délégués pour agir au nom de la ou des personnes désignées.

4.1.2

Il doit être possible de connaître sur demande l'identité des personnes que l'organisation a désignées pour s'assurer que les principes sont respectés.

4.1.3

Une organisation est responsable des renseignements personnels qu'elle a en sa possession ou sous sa garde, y compris les renseignements confiés à une tierce partie aux fins de traitement. L'organisation doit, par voie contractuelle ou autre, fournir un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie.

4.1.4

Les organisations doivent assurer la mise en œuvre des politiques et des pratiques destinées à donner suite aux principes, y compris :

a) la mise en œuvre des procédures pour protéger les renseignements personnels;
b) la mise en place des procédures pour recevoir les plaintes et les demandes de renseignements et y donner suite;
c) la formation du personnel et la transmission au personnel de l'information relative aux politiques et pratiques de l'organisation; et
d) la rédaction des documents explicatifs concernant leurs politiques et procédures.