Commissariat à la protection de la vie privée du Canada

Office of the Privacy Commissioner of Canada

OUTIL D'AUTOÉVALUATION – LPRPDE

Loi sur la protection des renseignements personnels et les documents électroniques

TABLE DES MATIÈRES

PARTIE 1 : GUIDE D'ÉVALUATION DE LA CONFORMITÉ

PARTIE 2 : LISTES DE CONTRÔLE DIAGNOSTIQUES

UTILITÉ DE CET OUTIL

Dans un monde où l'informatique et le partage des renseignements sont omniprésents, il est de plus en plus difficile de s'assurer d'une utilisation et d'une protection appropriées des renseignements personnels. Une gouvernance et une gestion sérieuses de la protection de la vie privée dans les organisations constituent des moyens efficaces d'atténuer les risques d'entrave à la vie privée et de s'assurer que des principes relatifs à l'équité dans le traitement de l'information sont appliqués dans les décisions d'affaires et dans les activités quotidiennes.

Le **Commissariat à la protection de la vie privée du Canada** (CPVP) a créé cet outil d'autoévaluation pour aider les organisations de moyenne et de grande taille à élaborer et à mettre en œuvre de bonnes gouvernance et gestion de la protection de la vie privée. L'autoévaluation de la protection de la vie privée est un processus grâce auquel une organisation amorce une évaluation visant à tester et à améliorer graduellement ses systèmes et ses pratiques de protection de la vie privée. Il s'agit d'évaluer l'organisation en fonction d'un ensemble de critères pour savoir à quel degré elle y répond. La vérification de la conformité à ces critères peut mettre au jour des lacunes ou des risques dont la prise en compte permettra d'orienter les mesures correctives et d'en faire le suivi.

Le CPVP considère l'autoévaluation par des organisations comme un moyen efficace et efficient de promouvoir les principes de protection de la vie privée. Voir l'annexe B pour plus d'information.

Cet outil vous est offert pour vous guider dans l'évaluation et l'amélioration de vos systèmes et de vos pratiques de gestion des renseignements personnels. Il est conçu pour les organisations du secteur privé de moyenne et de grande taille qui sont visées par la *Loi sur la protection des renseignements personnels et les documents électroniques* (la LPRPDE), mais peut être adapté et utilisé par d'autres organisations souhaitant appliquer les principes de la LPRPDE.

Chacun est libre d'utiliser ou non cet outil. Les moyens pris pour se conformer aux obligations imposées en vertu de la LPRPDE sont de la responsabilité de chacun. Rien dans le présent document ne doit être perçu comme un obstacle ou une entrave à l'exercice du pouvoir discrétionnaire du Commissariat à la protection de la vie privée du Canada dans le cadre de ses responsabilités, particulièrement en ce qui concerne les plaintes déposées par des personnes au titre de la LPRPDE ou de la *Loi sur la protection des renseignements personnels* ou la réalisation de vérifications par le CPVP au titre de l'une ou l'autre de ces lois.

En quoi consiste cet outil

- Un ensemble de normes grâce auxquelles les moyennes et grandes entreprises peuvent examiner leur conformité avec les dix principes relatifs à l'équité dans le traitement de l'information définis à l'annexe 1 de la LPRPDE[1] ;
- Un cadre de principes et de critères servant à évaluer le degré de conformité de votre entreprise à vos obligations;
- Un moyen d'interpréter les résultats et d'élaborer un plan d'action pour améliorer vos pratiques de gestion des renseignements personnels ou pour vérifier l'adéquation des pratiques en place.

Ce que cet outil n'est pas

- Une application globale et uniforme;
- Un outil de remplacement des méthodes d'évaluation éprouvées que vous avez peut-être déjà élaborées et mises en œuvre;
- Une solution définitive et complète pour toutes les organisations;
- Un outil de remplacement ou de substitution à la LPRPDE;
- Un outil approprié à toute autre loi que la LPRPDE.

[1] Ces dix principes sont : responsabilité, détermination des fins de la collecte des renseignements, consentement, limitation de la collecte, limitation de l'utilisation, de la communication et de la conservation, exactitude, mesures de sécurité, transparence, accès aux renseignements personnels, et possibilité de porter plainte à l'égard du non-respect des principes.

UTILISATION DE CET OUTIL

Cet outil est subdivisé en deux parties décrites plus en détail dans les sections suivantes :

Partie 1 : *Un guide de conformité* qui vous informe de vos obligations au titre de la LPRPDE;
Partie 2 : *Un outil diagnostique* constitué d'une série de listes de contrôle que vous pouvez utiliser pour évaluer le degré de conformité de votre entreprise (dans son ensemble ou pour certaines de ses divisions) avec les dix principes relatifs à l'équité dans le traitement de l'information de la LPRPDE.

Il convient d'envoyer les observations faites à l'égard de cette publication à l'attention du Directeur général, Vérification et revue, Commissariat à la protection de la vie privée du Canada, 112, rue Kent, Ottawa (Ontario) K1A 1H3.

Utilisez les deux outils de façon simultanée pour vous assurer de savoir si vous atteignez vos objectifs en matière de protection de la vie privée, à quel degré pour chacun, et d'être capable de faire la preuve de cette conformité.

Cet outil peut vous aider à diverses étapes de la définition des besoins de votre organisation en matière de développement. Il est possible de l'adapter à votre organisation dans son ensemble ou à des divisions de votre choix. Si vous ne disposez pas d'un programme de protection de la vie privée, vous pouvez utiliser cet outil pour déterminer les diverses mesures de protection de la vie privée (politiques, systèmes, procédures, contrôles d'accès, etc.) à élaborer et à mettre en œuvre dans votre organisation. Une fois que ces mesures ont été mises en œuvre et qu'elles ont été utilisées pendant un certain temps, utilisez les listes de contrôle pour procéder à une autoévaluation approfondie afin de déceler les lacunes et les points à améliorer en matière de pratiques de gestion des renseignements personnels.

Étapes suivantes :

Si votre organisation :

- a une taille allant de moyenne à grande et **est dotée d'un cadre de protection de la vie privée** permettant d'assurer la conformité avec les dix principes relatifs à l'équité dans le traitement de l'information de la LPRPDE, nous vous suggérons de passer directement aux listes de contrôle de la Partie 2 pour évaluer votre degré de conformité.
- a une taille allant de moyenne à grande et **n'est pas dotée d'un cadre de protection de la vie privée** permettant d'assurer la conformité avec les principes de la LPRPDE, nous vous suggérons de passer au guide de conformité de la Partie 1 pour prendre connaissance de vos obligations en vertu de la *Loi*.
- a une taille allant de moyenne à grande et **est dotée d'un cadre de protection de la vie privée et de certaines politiques, mais que vous n'êtes pas sûr qu'ils permettent d'assurer la conformité avec les exigences de la LPRPDE**, nous vous suggérons de passer aux listes de contrôle de la Partie 2 pour évaluer votre degré de conformité. Remplir ces listes de contrôle vous permettra de déceler les lacunes dans votre cadre de protection de la vie privée.

Pour de plus amples renseignements

L'annexe A présente un aperçu de la LPRPDE. Cet outil d'autoévaluation doit être utilisé conjointement avec la *Loi*. Il ne la remplace, ne s'y substitue ou ne l'annule en aucune manière.

L'annexe B présente le concept d'autoévaluation ainsi que ses avantages et décrit la façon dont une organisation peut s'y prendre pour procéder à une autoévaluation.

L'annexe C présente d'autres conseils donnés par le CPVP. Nous vous suggérons de consulter le site Web du CPVP à l'adresse **http://www.privcom.gc.ca/** où vous trouverez des conseils supplémentaires sur une variété de sujets liés à la conformité. Nous encourageons également les organisations à consulter les résumés des conclusions d'enquête publiés par le CPVP pour savoir comment le CPVP peut interpréter la LPRPDE, et pour avoir un aperçu des raisons systémiques expliquant les problèmes de conformité aux mesures de protection de la vie privée.

PARTIE 1 : GUIDE D'ÉVALUATION DE LA CONFORMITÉ

INTRODUCTION

Chaque section de ce guide décrit un des dix principes relatifs à l'équité dans le traitement de l'information, qui constituent la base d'une norme de protection de la vie privée servant à évaluer la conformité avec la LPRPDE. Pour vous assurer de la conformité de vos politiques et de vos pratiques de gestion des renseignements personnels, vous devez respecter les critères associés à chaque principe. Pour chacun des dix principes, le guide comprend deux types d'information :

- La description de vos responsabilités précises de gestion des renseignements personnels en vertu du principe traité et en fonction de la LPRPDE;
- Les activités et les meilleures pratiques qui vous permettent d'honorer chaque obligation en matière de conformité. Puisqu'il ne s'agit que d'exemples, vous pourriez devoir les adapter ou décider de vos propres façons de mettre en œuvre les mesures visant la conformité.

Le Guide de conformité vous aidera à concevoir les divers éléments de votre cadre de protection de la vie privée. Une fois qu'il aura été mis à l'essai durant une certaine période, remplissez les listes de contrôle d'autoévaluation de la Partie 2 pour vous assurer de son efficacité.

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.

Responsabilités de votre organisation en matière de protection de la vie privée

En vertu du principe de responsabilité, votre organisation doit :

- accepter la responsabilité des renseignements personnels dont elle a la gestion;
- désigner au moins un représentant qui sera responsable de la conformité de l'organisation avec les dix principes définis à l'annexe 1 de la LPRPDE;
- communiquer l'identité de la personne désignée, sur demande;
- protéger tous les renseignements personnels en la possession de l'organisation ou sous sa garde, y compris les renseignements confiés à une tierce partie aux fins de traitement;
- par voie contractuelle ou autre, fournir un degré comparable de protection aux renseignements personnels qui sont en cours de traitement par une tierce partie;
- élaborer et mettre en œuvre des politiques et des pratiques pour appuyer les dix principes définis à l'annexe 1 de la LPRPDE, notamment :
  - la mise en œuvre de procédures pour protéger les renseignements personnels;
  - la mise en place de procédures pour recevoir les plaintes et les demandes de renseignements et y donner suite;
  - la formation du personnel et la transmission au personnel de l'information relative aux politiques et aux pratiques de l'organisation;
  - la rédaction des documents explicatifs concernant les politiques et procédures.

En vertu du principe de responsabilité, votre organisation peut :

- déléguer d'autres personnes dans l'organisation pour agir au nom du représentant désigné pour la protection de la vie privée.

Comment atteindre ces objectifs

Désigner un représentant de la protection de la vie privée

- Nommez au moins une personne dans l'organisation qui sera responsable des politiques et des pratiques de gestion des renseignements personnels de votre organisation. Si cette personne n'est pas un responsable de la protection de la vie privée désigné, assurez-vous que sa description d'emploi comprend la responsabilité de gérer les renseignements personnels, comme l'exige la *Loi*. Cette personne doit :
  - être un décisionnaire principal qui reçoit un appui clair de la direction dans son rôle de promoteur de la protection de la vie privée comme valeur d'entreprise;
  - être capable, au besoin, d'intervenir sur les enjeux en matière de protection de la vie privée dans l'organisation;
  - s'assurer d'une allocation de ressources suffisantes et appropriées pour mettre en œuvre les politiques de protection de la vie privée, pour gérer les risques liés à la protection de la vie privée et pour veiller à ce que des évaluations périodiques soient effectuées afin de vérifier si les politiques de protection de la vie privée sont respectées et si l'organisation se conforme à la LPRPDE.

- Le cas échéant, publiez, à l'interne comme à l'externe, le nom ou le titre et l'adresse professionnelle du responsable de la protection de la vie privée (par exemple, sur des sites Web et dans la documentation de l'entreprise). Soyez prêt à donner les coordonnées de votre responsable de la protection de la vie privée lorsqu'on vous le demandera;
- Élaborez des conseils qui aideront le personnel à répondre aux questions des clients sur votre programme de protection de la vie privée, y compris des renseignements sur les façons de communiquer avec le responsable de la protection de la vie privée s'ils le demandent.

Élaborer des politiques et des procédures de protection de la vie privée[2]

- Élaborez et mettez en œuvre des politiques et des procédures de gestion des renseignements personnels correspondant aux principes énoncés à l'annexe 1 de la LPRPDE. Si votre organisation est une « entreprise fédérale », telle qu'elle est définie au paragraphe 2(1) de la LPRPDE, ces politiques et ces procédures s'appliquent aux renseignements personnels de vos employés et de vos clients;
- Élaborez une politique de protection de la vie privée qui s'applique à l'organisation dans son ensemble, ainsi que des sous-politiques qui s'appliquent à des secteurs d'activités précis, le cas échéant;
- Mettez au point des procédures pour :
  - informer les personnes des fins de la collecte *(Deuxième principe – Détermination des fins de la collecte des renseignements)*;
  - obtenir le consentement approprié *(Troisième principe – Consentement)*;
  - permettre aux personnes de retirer leur consentement *(Troisième principe – Consentement)*;
  - limiter la collecte de renseignements personnels (sur le plan de la quantité et de la nature des renseignements et sans induire en erreur ou tromper les clients) à ce qui est nécessaire pour les fins déterminées et s'assurer qu'ils sont recueillis de façon honnête et licite *(Quatrième principe – Limitation de la collecte)*.
  - conserver et détruire les renseignements personnels *(Cinquième principe – Limitation de l'utilisation, de la communication et de la conservation)*;
  - s'assurer que les renseignements personnels sont exacts, complets et à jour *(Sixième principe – Exactitude)*;
  - s'assurer que des mesures de sécurité adéquates sont adoptées *(Septième principe – Mesures de sécurité)*;
  - rendre accessible au public l'information sur les politiques et les pratiques *(Huitième principe – Transparence)*;
  - recevoir les demandes d'accès et y donner suite *(Neuvième principe – Accès aux renseignements personnels)*;
  - recevoir les demandes de renseignements et les plaintes, et y donner suite *(Dixième principe – Possibilité de porter plainte à l'égard du non-respect des principes)*.

- Élaborez des politiques administratives en matière de protection et de gestion de la vie privée en définissant des critères portant sur :
  - les structures organisationnelles, les rôles et les responsabilités nécessaires au respect des exigences en matière de protection de la vie privée;
  - la production de rapports pour la haute direction sur les procédures de gestion des politiques de protection de la vie privée et du risque;
  - l'allocation de ressources suffisantes et appropriées pour mettre en œuvre et soutenir les politiques de protection de la vie privée;

[2] Votre cadre de protection de la vie privée peut être constitué d'une seule politique déterminante ou d'un ensemble de politiques de moindre importance, toutes à l'appui des dix principes.

- les exigences en matière d'évaluation des facteurs relatifs à la vie privée avant que de nouveaux produits, services ou systèmes d'information ne soient lancés ou que des produits, services ou systèmes d'information existants ne fassent l'objet de modifications importantes;
- les normes de sécurité et de gestion des renseignements, pour s'assurer que les renseignements sont protégés contre toute communication, toute modification, toute interruption, toute élimination ou toute destruction non autorisée;
- les exigences relatives à l'examen périodique de la conception, de l'acquisition, du développement, de la mise en œuvre, de la configuration et de la gestion de l'infrastructure, des systèmes, des applications et des sites Web pour s'assurer de l'adéquation avec les politiques et les procédures de protection de la vie privée;
- les exigences relatives à la détermination et à l'évaluation des conséquences des atteintes à la vie privée, incluant la perte de renseignements ou l'utilisation inappropriée des renseignements personnels, ainsi que la production de rapports connexes, et les exigences relatives à l'élimination du problème à la source;
- les procédures à suivre pour donner suite aux plaintes concernant la protection de la vie privée et pour adopter les mesures correctives qui s'imposent;
- la formation continue des employés sur la protection de la vie privée;
- la vérification de la conformité avec les bonnes pratiques de gestion de la protection de la vie privée.

S'assurer de la responsabilité de l'organisation et du personnel

Accordez à votre responsable de la protection de la vie privée l'appui de la direction, ainsi que le pouvoir d'intervenir sur les enjeux en matière de protection de la vie privée relatifs à toute activité de votre organisation, et concrétisez l'ajout de responsabilités en matière de protection de la vie privée en mettant à jour la description d'emploi officielle;

Assurez-vous que le responsable de la protection de la vie privée de votre organisation peut :

- démontrer sa connaissance des politiques et des procédures de gestion des renseignements personnels de l'organisation;
- démontrer sa connaissance des responsabilités de l'organisation en vertu de la LPRPDE;
- expliquer les procédures de demande de renseignements personnels et de dépôt de plaintes;
- procéder à l'examen des plaintes ou le superviser.

Formez vos employés de première ligne et vos cadres et tenez-les au courant, de sorte qu'ils :

- puissent répondre eux-mêmes aux demandes de renseignements sur les politiques et les pratiques de protection de la vie privée de votre organisation ou aiguiller les demandeurs vers le responsable de la protection de la vie privée ou tout autre représentant autorisé;
- puissent expliquer les fins de la collecte des renseignements personnels de l'organisation;
- comprennent les politiques et les procédures de votre organisation relatives au consentement, et puissent obtenir le consentement au besoin;
- expliquent aux clients quand et comment ils pourront retirer leur consentement et quelles seront, le cas échéant, les conséquences d'un tel retrait;
- puissent reconnaître les demandes d'accès aux renseignements personnels et y donner suite;
- puissent transmettre les plaintes concernant des questions liées à la protection des renseignements personnels au responsable de la protection de la vie privée de l'organisation;
- soient au courant des activités en cours dans votre organisation et des nouvelles initiatives sur la protection des renseignements personnels.

Assurez-vous de :

- quotidiennement tenir vos employés au courant des nouveaux enjeux relatifs à la protection de la vie privée que soulèvent les changements technologiques, les examens internes, les plaintes des citoyens et les décisions des tribunaux;
- développer et mettre en œuvre un système pour surveiller la conformité de votre organisation à la LPRPDE de manière continue.

Communiquer des renseignements au public

Les clients sont de plus en plus conscients des enjeux en matière de protection de la vie privée et de protection des renseignements personnels. Vous devriez leur communiquer vos politiques et vos pratiques en matière de collecte et d'utilisation des renseignements personnels, ainsi que les mesures que vous prenez pour protéger leurs renseignements personnels. À cette fin :

- Concevez et diffusez auprès des clients et du public des documents d'information (c. à-d. des dépliants, des brochures, des sites Web, ou toute forme écrite) pour leur expliquer, en des termes clairs, les politiques, les pratiques et les procédures de votre organisation en matière de protection de la vie privée;
- Assurez-vous que ces documents indiquent clairement aux personnes comment :
  - accéder à leurs renseignements personnels;
  - faire corriger leurs renseignements personnels;
  - faire des demandes de renseignements sur les politiques ou les pratiques de l'organisation en matière de protection de la vie privée;
  - porter plainte contre les politiques ou les pratiques de l'organisation en matière de protection de la vie privée.
- Pour les clients en particulier, expliquez-leur clairement avec qui communiquer au sein de votre organisation pour qu'ils puissent :
  - faire des demandes de renseignements généraux sur leurs renseignements personnels;
  - demander l'accès à leurs renseignements personnels;
  - corriger leurs renseignements personnels.

Responsabilité du transfert à des tierces parties

Plusieurs raisons poussent les organisations à confier les renseignements à des tierces parties à des fins de traitement. Il est important de mentionner que l'organisation émettrice qui transfère des renseignements personnels à une tierce partie aux fins de traitement en conserve le contrôle. Parmi les pratiques exemplaires figurent celles-ci :

- Utiliser des dispositions de protection de la vie privée dans les contrats pour s'assurer que les tierces parties à qui sont transférés les renseignements personnels aux fins de traitement offrent le même niveau de protection au titre de la LPRPDE que votre organisation, à moins que la tierce partie ne soit une filiale ou une société affiliée tenue par le même code type sur la protection des renseignements personnels;

- S'assurer que la tierce partie :
  - nomme une personne responsable de gérer toutes les questions de protection de la vie privée relatives aux renseignements transférés;
  - limite l'utilisation des renseignements aux fins autorisées par votre organisation;
  - limite la communication des renseignements à ce qui est autorisé par votre organisation ou exigé par la loi;
  - transfère à votre organisation toute demande d'accès ou toute plainte relative aux renseignements transférés;
  - adopte des mesures de sécurité appropriées pour protéger les renseignements personnels;
  - renvoie ou élimine en toute sécurité les renseignements transférés une fois le contrat terminé;
  - fait un rapport sur le caractère adéquat de ses mesures de sécurité et de gestion des renseignements personnels et permet à votre organisation, au besoin, de vérifier sa conformité.

DEUXIÈME PRINCIPE – DÉTERMINATION DES FINS DE LA COLLECTE DES RENSEIGNEMENTS

Les fins auxquelles des renseignements personnels sont recueillis doivent être déterminées par l'organisation avant la collecte ou au moment de celle-ci.

Responsabilités de votre organisation en matière de protection de la vie privée

En vertu du principe de détermination des fins de la collecte des renseignements, votre organisation doit :

- préciser les fins de la collecte des renseignements personnels avant celle-ci ou au moment de celle-ci;
- documenter les fins de la collecte des renseignements personnels;
- prévenir ses clients avant d'utiliser leurs renseignements personnels pour toute fin non précisée au moment de la collecte.

En vertu du principe de détermination des fins de la collecte des renseignements, votre organisation devrait :

- déterminer la quantité et la nature des renseignements nécessaires pour réaliser les fins auxquelles ils ont été recueillis, conformément au principe de la limitation de la collecte;
- s'assurer que quiconque recueille des renseignements personnels pour votre organisation peut en expliquer la raison à vos clients.

En vertu du principe de détermination des fins de la collecte des renseignements, votre organisation peut :

- choisir la meilleure façon d'expliquer à vos clients, verbalement ou par écrit, les raisons pour lesquelles leurs renseignements personnels sont recueillis.

Remarques

- Le principe de détermination des fins de la collecte des renseignements est étroitement associé à l'exigence en matière de connaissance définie dans le principe de consentement. Ainsi, selon le principe 4.3.2 de l'annexe 1 :

  > *Suivant ce principe, il faut informer la personne au sujet de laquelle on recueille des renseignements et obtenir son consentement. Les organisations doivent faire un effort raisonnable pour s'assurer que la personne est informée des fins auxquelles les renseignements seront utilisés. Pour que le consentement soit valable, les fins doivent être énoncées de façon que la personne puisse raisonnablement comprendre de quelle manière les renseignements seront utilisés ou communiqués.*

- Le paragraphe 5(3) de la LPRPDE est également approprié :

  > *5(3) L'organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.*

Comment atteindre ces objectifs

Déterminer les fins

- Examinez vos pratiques actuelles et déterminez les fins précises de la collecte de renseignements personnels;
- Le responsable de la protection de la vie privée devrait examiner les nouvelles fins pour déterminer si elles sont appropriées, et pour prendre en compte et atténuer les risques d'entrave à la vie privée découlant des nouvelles utilisations;
- Déterminez la quantité et la nature des renseignements que votre organisation doit absolument recueillir pour arriver à ses fins, en gardant en mémoire le principe de limitation de la collecte;
- Confirmez que les raisons pour lesquelles vous recueillez les renseignements personnels sont celles auxquelles une personne raisonnable (par exemple, un client typique) s'attendrait ou qu'elle jugerait appropriées dans des circonstances d'affaires normales, conformément au paragraphe 5(3) de la LPRPDE (voir la note ci-dessus);
- Établissez une distinction claire entre les activités de collecte qui sont *essentielles* et celles qui ne le sont pas au chapitre de l'offre de biens ou de la prestation de services réelles demandées par les clients, comme le marketing de produits ou de services additionnels. Les clients devraient pouvoir choisir de renoncer à des fins non essentielles ou secondaires.

Documenter les fins

- Couchez clairement par écrit la liste de toutes les raisons pour lesquelles vous recueillez des renseignements personnels. Tenez cette liste à jour. En établissant votre liste :
  - indiquez précisément l'utilisation et la communication des renseignements personnels que vous prévoyez;
  - ne citez pas de fins générales, comme « servir le client »;
  - évitez les termes vagues ou généraux, comme « […] et d'autres utilisations appropriées »;
  - expliquez en des termes clairs, concrets et dénués d'ambiguïté pourquoi vous recueillez des renseignements personnels, pour que les clients puissent comprendre les façons précises dont votre organisation compte utiliser ou communiquer les renseignements qu'elle recueille auprès d'eux.
- Pour observer le principe de transparence, intégrez les fins documentées dans la documentation de votre organisation qui traite de la protection de la vie privée et dans tout autre document approprié (par exemple, les modalités de contrat, les formulaires de demande).

Indiquer les fins

- Chaque fois que cela est possible et raisonnable, informez les clients, verbalement ou par écrit, des raisons pour lesquelles vous recueillez des renseignements personnels, et ce, *avant* que vous ne les recueilliez;
- Quand il n'est pas possible ni raisonnable d'informer les clients au moment de la collecte ou avant, faites-le, verbalement ou par écrit, avant d'utiliser ou de communiquer les renseignements;
- En règle générale, n'informez les clients après la collecte que si les fins sont nouvelles (c'est-à-dire, si elles n'étaient pas encore déterminées au moment de la collecte);
- En général, avant l'obtention du consentement, faites tout effort raisonnable pour informer les clients des fins auxquelles votre organisation a l'intention d'utiliser ou de communiquer leurs renseignements personnels. Gardez à l'esprit que leur consentement explicite dépendra en fin de compte de leur compréhension de ce à quoi ils pourraient consentir;
- Informez les clients de toute utilisation ou communication prévues de leurs renseignements personnels auxquelles ils ne s'attendraient pas raisonnablement de la part de votre organisation dans le cadre de l'offre d'un bien ou de la prestation d'un service. Il peut par exemple s'agir de partage des renseignements personnels avec des tiers spécialistes du marketing.

Quand vous indiquez les fins verbalement

- Formez les employés qui recueillent les renseignements personnels pour qu'ils puissent expliquer les fins de manière exacte, claire et cohérente, et informez-les de toute nouvelle raison de procéder à une collecte;
- Remettez au personnel un scénario standard ou utilisez d'autres moyens pour vous assurer qu'il peut expliquer les fins aux clients de façon claire et cohérente;
- Si votre organisation enregistre des conversations téléphoniques avec des clients (par exemple, pour le contrôle de la qualité), informez le client au début de chaque appel de cette pratique et de ses objectifs. Reportez-vous au document du CPVP intitulé *Lignes directrices sur l'enregistrement des appels téléphoniques des clients*, accessible à l'adresse **http://www.privcom.gc.ca/**.

Quand vous indiquez les fins par écrit

- Si votre organisation informe les clients des fins par écrit :
  - fournissez au client des déclarations écrites des fins avant le moment ou de préférence au moment de la collecte des renseignements personnels du client, chaque fois que cela est possible;
  - fournissez au client des déclarations écrites des fins à l'endroit où se produit la collecte (par exemple, dans vos établissements, à la maison du client, ou sur votre site Web, selon que le client donne les renseignements en personne, par courrier ou par téléphone, ou de façon électronique), chaque fois que cela est possible;
  - rédigez des déclarations des fins facilement consultables par quelqu'un voulant se renseigner sur la question du consentement.
- Si vous utilisez des formulaires pour recueillir des renseignements personnels, expliquez sur les formulaires pourquoi vous recueilliez les renseignements;
- Pour tout document écrit servant à informer les clients, assurez-vous que les déclarations des fins sont en évidence et faciles à trouver, à lire et à comprendre. Utilisez des termes simples dans la mesure du possible.

Déterminer de nouvelles fins

- Si, quelque temps après la collecte, votre organisation a l'intention d'utiliser ou de communiquer les renseignements personnels d'un client à de nouvelles fins, qui n'avaient pas encore été déterminées :
  - demandez conseils auprès de votre responsable de la protection de la vie privée sur les conséquences possibles sur la protection de la vie privée;
  - déterminez et documentez la nouvelle fin, et expliquez-la au client;
  - obtenez le consentement du client relativement à la nouvelle fin, à moins que la *Loi* ne l'exige pas.

TROISIÈME PRINCIPE – CONSENTEMENT

Toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire.

Responsabilités de votre organisation en matière de protection de la vie privée

En vertu du principe de consentement, votre organisation doit :

- obtenir le consentement de la personne pour recueillir, utiliser ou communiquer des renseignements personnels, à moins qu'il ne soit pas approprié de le faire (par exemple, à des fins légales, médicales ou de sécurité), tel qu'il est précisé à l'article 7 de la LPRPDE. Documentez toutes les exceptions et indiquez les cas pour lesquels les renseignements peuvent être recueillis, utilisés ou communiqués sans le consentement de la personne. Lorsqu'il est inapproprié d'obtenir le consentement de la personne, une raison claire doit être documentée pour appuyer l'exception;
- s'assurer que la personne donne un consentement éclairé;
- faire un effort raisonnable pour s'assurer d'informer la personne des fins auxquelles les renseignements personnels seront utilisés ou communiqués;
- énoncer et expliquer les fins de façon à ce que la personne puisse raisonnablement comprendre de quelle manière les renseignements personnels seront utilisés ou communiqués;
- ne jamais exiger d'une personne, comme condition préalable à l'obtention d'un bien ou d'un service, qu'elle consente à la collecte, à l'utilisation ou à la communication de renseignements autres que ceux qui sont nécessaires aux fins explicitement indiquées et légitimes;
- tenir compte des attentes raisonnables de la personne au moment d'obtenir son consentement;
- ne jamais tenter d'obtenir un consentement par un subterfuge;
- tenir compte de la sensibilité des renseignements personnels au moment de déterminer la façon dont le consentement sera obtenu;
- permettre à la personne de retirer son consentement en tout temps, sous réserve des restrictions prévues par une loi ou par un contrat et d'un préavis raisonnable;
- informer le client des conséquences d'un tel retrait.

En vertu du principe de consentement, votre organisation devrait :

- tenter d'obtenir, au moment de recueillir les renseignements, le consentement de la personne pour des utilisations ou des communications subséquentes de ses renseignements personnels;
- traiter tout renseignement contenu dans un dossier médical, financier ou sur le revenu comme un renseignement sensible;
- garder à l'esprit que tout renseignement peut être sensible, selon le contexte;
- chercher à obtenir un consentement explicite lorsque cela est possible, et de façon systématique si les renseignements personnels sont susceptibles d'être considérés comme sensibles.

En vertu du principe de consentement, votre organisation peut :

- chercher à obtenir le consentement de la personne pour utiliser ou communiquer les renseignements personnels après les avoir recueillis, mais *avant* de les utiliser dans certains contextes (c'est-à-dire lorsque des renseignements personnels déjà recueillis sont utilisés à des fins non indiquées antérieurement);
- déterminer la forme que prendra le consentement selon le contexte et la nature et la sensibilité des renseignements;
- se fonder sur un consentement implicite uniquement si les renseignements personnels ne sont pas sensibles.

Comment atteindre ces objectifs

Répondre aux exigences en matière de connaissance

- Comprenez que la validité de tout consentement obtenu par votre organisation repose habituellement sur la connaissance que le client a des intentions de votre organisation au moment où vous lui demandez son consentement;
- Fournissez suffisamment d'information au client de sorte qu'il puisse donner un consentement valable. Pour ce faire, indiquez, documentez et précisez les fins, conformément au principe de détermination des fins de la collecte des renseignements (se reporter à la section précédente);
- Énoncez les fins de manière à permettre au client de comprendre de façon raisonnable les façons précises dont votre organisation prévoit utiliser ou communiquer les renseignements personnels;
- Prenez les mesures appropriées pour vous assurer que les efforts faits pour communiquer les fins au client seront jugés raisonnables.

Répondre aux exigences en matière de consentement

- Élaborez des politiques et des procédures claires en matière de consentement et veillez à ce que les employés qui recueillent les renseignements personnels comprennent le processus et puissent appliquer les procédures en tout temps;
- Tentez d'obtenir le consentement du client pour recueillir, utiliser ou communiquer ses renseignements personnels, sauf si une exception définie à l'article 7 de la LPRPDE s'applique. Consultez l'article 7 de la LPRPDE pour connaître les exceptions s'appliquant aux exigences en matière de consentement;
- Au moment de recueillir les renseignements, obtenez le consentement du client pour une utilisation ou une communication ultérieure et assurez-vous qu'en cas d'écart à cette règle, les attentes raisonnables du client sont quand même respectées;
- Si vous cherchez à obtenir le consentement du client après que les renseignements ont été recueillis à des fins d'utilisation ou de communication qui n'ont pas été indiquées précédemment, assurez-vous que le client est dûment informé des fins et obtenez son consentement avant toute nouvelle utilisation ou communication des renseignements;
- Avant de demander le consentement de tout client pour recueillir, utiliser ou communiquer ses renseignements personnels comme condition préalable à l'obtention d'un bien ou d'un service, veillez à respecter les points suivants :
  - Les fins sont légitimes (c'est-à-dire raisonnables);
  - Les fins précises sont communiquées au client de façon explicite;
  - Les renseignements recueillis, utilisés ou communiqués sont uniquement ceux nécessaires aux fins visées.

- N'utilisez pas un consentement à des fins secondaires, telles que des fins de marketing, comme condition préalable à la fourniture d'un bien ou à la prestation d'un service;
- Lorsqu'une fin est secondaire ou lorsque le consentement connexe ne peut pas être raisonnablement obtenu comme condition préalable à la fourniture d'un bien ou à la prestation d'un service, précisez que la fin et le consentement sont facultatifs et informez la personne de ses options;
- Consentement relatif à des renseignements obtenus avant l'entrée en vigueur de la LPRPDE : Pour plus d'information sur le consentement relatif à l'utilisation ou à la communication de renseignements personnels recueillis par votre organisation avant qu'elle doive se conformer à la LPRPDE, reportez-vous au document du CPVP intitulé *Pratiques exemplaires relatives au traitement des renseignements personnels avant l'entrée en vigueur de la LPRPDE (respect des droits acquis)*, accessible à l'adresse **http://www.privcom.gc.ca/**;
- Pour plus d'information sur le consentement relatif à l'enregistrement d'appels téléphoniques des clients, reportez-vous au document du CPVP intitulé *Lignes directrices sur l'enregistrement des appels téléphoniques des clients*, accessible à l'adresse **http://www.privcom.gc.ca/**.

Déterminer la forme de consentement appropriée

- Avant de déterminer la forme de consentement à utiliser dans une situation donnée (c'est-à-dire consentement explicite, implicite, actif ou refus), reportez-vous à la fiche d'information intitulée *Détermination de la forme de consentement appropriée aux termes de la* Loi sur la protection des renseignements personnels et les documents électroniques, accessible à l'adresse http://www.privcom.gc.ca/;
- Tenez compte de la sensibilité des renseignements personnels, des attentes raisonnables du client et du contexte;
- Utilisez le **consentement explicite (actif)** chaque fois que cela est possible et dans toute situation nécessitant des renseignements personnels, comme des dossiers médicaux ou financiers, qui sont susceptibles d'être considérés comme sensibles :
  - À titre de pratique exemplaire, utilisez la forme de consentement explicite (actif) pour toute communication prévue de renseignements personnels à des tierces parties ou pour toute autre fin secondaire à laquelle le client ne s'attendrait pas raisonnablement pour l'obtention d'un bien ou d'un service de votre organisation;
  - Si des fichiers témoins ou des technologies semblables sont utilisés dans le site Web de l'organisation, informez l'utilisateur de cette pratique et de la fin visée, et cherchez à obtenir son consentement explicite (actif).
- Ne comptez sur **un consentement implicite** que dans les situations où l'utilisation et la communication prévues des renseignements personnels sont évidentes compte tenu du contexte, et où votre organisation peut présumer de façon raisonnable que le client comprend, connaît ou accepte la situation.

Méthodes utilisées pour obtenir un consentement

- Au moment d'utiliser un **formulaire de demande** pour l'obtention d'un consentement, assurez-vous que les fins auxquelles les renseignements sont recueillis sont clairement énoncées et placées bien en évidence sur le formulaire;
- Lorsque des cases à cocher sont utilisées pour l'obtention d'un consentement pour le partage de renseignements personnels avec d'autres organisations :
  - Indiquez le nom des autres organisations;
  - Énoncez clairement les fins;
  - Assurez-vous que la disposition des cases à cocher est claire et non ambiguë;
  - À titre de pratique exemplaire, n'utilisez qu'une case, « oui » ou « non »;
  - S'il s'agit de renseignements personnels sensibles ou si les autres organisations ne sont pas nommées, utilisez le consentement « actif » en n'utilisant qu'une case à cocher « oui ». Si le client ne coche pas la case, ne présumez pas que le client a donné son consentement;

  - N'utilisez le consentement négatif, ou « refus », (c'est-à-dire une case à cocher « non ») que s'il est possible de démontrer que les renseignements personnels ne sont pas sensibles (il s'agit généralement de renseignements accessibles au public);
  - Si les deux cases à cocher, « oui » et « non », sont utilisées, clarifiez la forme de consentement prévue en expliquant ce qui arrive si le client ne coche aucune case, et indiquez si votre organisation présume que le consentement est obtenu ou non;
  - Si les deux cases à cocher, « oui » ou « non », sont utilisées, et qu'il est question de renseignements personnels sensibles, utilisez le mécanisme de consentement « actif ». Si le client ne coche aucune des deux cases, il ne faut pas présumer avoir obtenu son consentement.
- Veillez à ce que les employés responsables de l'obtention du **consentement par téléphone** comprennent le processus et qu'ils puissent suivre en tout temps les procédures de l'organisation;
- Limitez la pratique qui consiste à **présumer que le client donne son consentement implicite** en raison de son utilisation du bien ou du service aux situations pour lesquelles un client s'attendrait de façon raisonnable à ce que ses renseignements personnels soient utilisés pour la fourniture du bien ou la prestation du service. En général, il ne faut pas présumer que le client donne son consentement implicite pour des fins secondaires s'ajoutant à celles pour lesquelles les renseignements personnels sont nécessaires pour qu'il obtienne le bien ou le service.

Offrir la possibilité de retirer le consentement

- Puisque le client a le droit de retirer son consentement en tout temps (sous réserve de restrictions prévues par une loi ou un contrat et d'un préavis raisonnable), offrez lui une façon pratique, facile et peu coûteuse de retirer son consentement, et appliquez ce retrait sans délai. Le retrait par téléphone au moyen d'un numéro sans frais est l'option privilégiée;
- Ajoutez de l'information sur les possibilités de retrait du consentement et le mécanisme connexe dans tous les documents publiés portant sur la détermination des fins et l'obtention du consentement. Si vous comptez sur un consentement négatif à des fins secondaires, assurez-vous de porter le mécanisme de retrait du consentement à l'attention du client au moment de présumer qu'il va donner son consentement;
- Avant toute demande de retrait du consentement ou au moment de cette demande, informez le client des conséquences d'un tel retrait. Le retrait du consentement pour des fins secondaires ne devrait pas entraîner de conséquences graves liées à la fourniture d'un bien ou à la prestation d'un service.

QUATRIÈME PRINCIPE – LIMITATION DE LA COLLECTE

L'organisation ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées et doit procéder de façon honnête et licite.

Responsabilités de votre organisation en matière de protection de la vie privée

En vertu du principe de limitation de la collecte, votre organisation doit :

- limiter la collecte des renseignements personnels (la quantité et la nature des renseignements) à ce qui est nécessaire aux fins déterminées;
- ne jamais recueillir des renseignements de façon arbitraire;
- recueillir des renseignements personnels de façon honnête et licite, sans induire la personne en erreur quant aux fins auxquelles les renseignements sont recueillis et sans obtenir le consentement de la personne par un subterfuge;
- préciser la nature des renseignements recueillis comme partie intégrante des politiques et pratiques de l'organisation concernant le traitement des renseignements, conformément au principe de transparence.

Comment atteindre ces objectifs

Vérifier les pratiques de collecte des renseignements personnels

- Vérifiez que votre organisation recueille en tout temps les renseignements personnels de façon honnête, licite et non arbitraire, et sans subterfuge quant aux fins et au consentement;
- Déterminez les raisons de recueillir des renseignements personnels, les quantités minimales et la nature des renseignements nécessaires pour réaliser les fins;
- Établissez une distinction claire entre les renseignements obligatoires et les renseignements facultatifs. Certains renseignements importants sont nécessaires pour fournir un service, tandis que d'autres peuvent être utiles, sans toutefois être nécessaires, par exemple, un numéro de permis de conduire pour un retour de bien. Précisez au client qu'il s'agit de renseignements qui pourraient être utiles, donc de renseignements facultatifs;
- Limitez la collecte de renseignements personnels de la part de votre organisation à la quantité nécessaire, et ne recueillez que ceux dont la nature sert aux fins déterminées. Les renseignements ne devraient pas être recueillis sous le prétexte qu'ils pourraient s'avérer utiles ultérieurement;
- Si possible, privilégiez l'utilisation des renseignements dépersonnalisés ou non personnels tels qu'un numéro de client au lieu d'un nom.

Documenter les pratiques de collecte

- Afin de communiquer avec les clients de façon conforme au principe de transparence, documentez les politiques et les pratiques de votre organisation en matière de collecte des renseignements et ajoutez cette information à votre documentation connexe. Indiquez clairement la nature des renseignements recueillis de même que les fins auxquelles ils sont recueillis;
- Déterminez les fins précises selon la nature des renseignements. Votre organisation doit aussi tenir compte des renseignements obtenus d'une source autre que le client (par exemple, une évaluation de crédit obtenue par un créancier d'une agence d'évaluation du crédit);
- Établissez des procédures de collecte des renseignements personnels. Assurez-vous que tous les membres du personnel comprennent et respectent les limitations de la collecte des renseignements personnels.

Renseignements obligatoires et renseignements facultatifs

- Au moment d'informer le client, que ce soit verbalement ou par écrit, des raisons pour lesquelles les renseignements sont recueillis, distinguez clairement les renseignements obligatoires des renseignements facultatifs. Les renseignements facultatifs sont simplement utiles, contrairement aux renseignements obligatoires, qui sont nécessaires, et ils comprennent tout renseignement recueilli uniquement à des fins secondaires;
- Si votre organisation demande un type de renseignement qui ne peut être considéré comme strictement nécessaire à une fin déterminée (par exemple, un numéro d'assurance sociale à des fins d'identification), informez le client au moment de la collecte que ce renseignement est facultatif;
- Si votre organisation recueille des numéros d'assurance sociale pour une fin quelconque, assurez-vous que la collecte ainsi que toute utilisation ou communication subséquente de ce renseignement sont conformes aux lignes directrices du CPVP, telles qu'elles sont décrites dans la fiche d'information intitulée *Pratiques exemplaires pour l'utilisation des numéros d'assurance sociale* dans le secteur privé (accessible à l'adresse **http://www.privcom.gc.ca/**). En général, le CPVP suggère de limiter l'utilisation des numéros d'assurance sociale aux utilisations prévues par la loi;
- Au moment d'informer le client des fins auxquelles les renseignements sont recueillis, indiquez clairement la nature des renseignements que votre organisation doit recueillir en vertu de la loi.

CINQUIÈME PRINCIPE – LIMITATION DE L'UTILISATION, DE LA COMMUNICATION ET DE LA CONSERVATION

Les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne l'exige. On ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins déterminées.

Responsabilités de votre organisation en matière de protection de la vie privée

En vertu du principe de limitation de l'utilisation, de la communication et de la conservation, votre organisation doit :

- ne jamais utiliser ou communiquer de renseignements personnels à des fins autres que celles pour lesquelles ils sont recueillis, à moins que la personne n'y consente ou que la loi ne l'exige;
- documenter toute nouvelle fin pour laquelle les renseignements personnels sont recueillis;
- conserver les renseignements personnels seulement aussi longtemps que cela est nécessaire pour les fins déterminées;
- conserver les renseignements personnels servant à prendre une décision au sujet d'une personne suffisamment longtemps pour permettre à la personne concernée d'exercer son droit d'accès aux renseignements après que la décision a été prise;
- élaborer des lignes directrices et des procédures pour le retrait des renseignements personnels.

En vertu du principe de limitation de l'utilisation, de la communication et de la conservation, votre organisation devrait :

- détruire, effacer ou dépersonnaliser les renseignements personnels qui ne sont plus nécessaires aux fins déterminées[3] ;
- élaborer des lignes directrices et appliquer des procédures pour la conservation des renseignements personnels;
- indiquer les périodes de conservation minimales et maximales dans ces lignes directrices.

Remarque

- Le principe des mesures de sécurité traite en outre de la destruction des renseignements personnels. Plus précisément, le principe 4.7.5 de l'annexe 1 stipule que :

  > *Au moment du retrait ou de la destruction des renseignements personnels, on doit veiller à empêcher les personnes non autorisées d'y avoir accès.*

  Il faut toutefois souligner que le simple recyclage de documents papier comprenant des renseignements personnels n'est pas l'équivalent d'une destruction des renseignement.

[3] À moins qu'une demande d'accès au renseignement n'ait été déposée. Dans un tel cas, le renseignement devrait être conservé aussi longtemps que nécessaire pour permettre à la personne d'épuiser ses recours, y compris les plaintes au CPVP et toute action en justice subséquente.

Comment atteindre ces objectifs

Limiter l'utilisation et la communication

- Utilisez ou communiquez les renseignements personnels seulement aux fins déterminées et documentées au moment de leur collecte;
- Si votre organisation souhaite utiliser ou communiquer des renseignements personnels à toute autre nouvelle fin qui n'était pas encore déterminée au moment de leur collecte, documentez la nouvelle fin, informez les personnes concernées et cherchez à obtenir leur consentement (à moins que la nouvelle utilisation ou communication ne soit exigée par la loi, ou sauf si une exception définie à l'article 7 de la LPRPDE s'applique);
- Assurez-vous que tous les membres du personnel responsables du traitement des renseignements personnels comprennent et respectent les limites relatives à l'utilisation et à la communication des renseignements.

Conservation et destruction

- Déterminez si tous les renseignements personnels détenus par votre organisation ont été recueillis à des fins précises et s'il est encore nécessaire de réaliser les fins auxquelles les renseignements ont été recueillis ou de se conformer aux exigences prévues par la loi;
- Si des renseignements personnels conservés ne servent plus à réaliser des fins précises ou s'ils ne sont plus nécessaires, prenez les mesures de sécurité appropriées pour les détruire, les supprimer ou les dépersonnaliser;
- Élaborez des lignes directrices et appliquez des procédures sûres pour la conservation et la destruction des renseignements personnels. Établissez des échéanciers de conservation et de destruction comprenant les périodes de conservation minimales et maximales, en tenant compte des exigences prévues par la loi qui s'appliquent à votre organisation;
- Lorsque des renseignements personnels sont utilisés pour prendre une décision sur une personne, déterminez une période de conservation qui laissera à la personne un délai raisonnable pour accéder aux renseignements après que la décision a été prise;
- Fondez les politiques et les pratiques de conservation de votre organisation en partant du principe que les renseignements ne devraient être conservés qu'aussi longtemps qu'il est nécessaire pour réaliser les fins auxquelles ils ont été recueillis;
- Effectuez des vérifications régulières ou ponctuelles des renseignements personnels détenus afin de vous assurer qu'ils ne sont pas conservés au-delà des délais fixés;
- Établissez des méthodes de sûres pour la destruction des renseignements qui ne sont plus utiles afin d'éviter toute communication inappropriée (par exemple, déchiquetez les dossiers papier ou supprimez de façon sécuritaire les fichiers électroniques). Tenez compte des risques associés à la mise au rebut d'ordinateurs dont le disque dur contient des renseignements personnels.
- Élaborez des politiques ou des contrats qui s'appliquent aux tierces parties participant à l'élimination des renseignements personnels pour le compte de votre organisation;
- Pour plus d'information sur la conservation des renseignements personnels recueillis par votre organisation avant qu'elle ne se conforme à la LPRPDE, reportez-vous au document du CPVP intitulé *Pratiques exemplaires relatives au traitement des renseignements personnels avant l'entrée en vigueur de la LPRPDE*, accessible à l'adresse **http://www.privcom.gc.ca/**.

SIXIÈME PRINCIPE – EXACTITUDE

Les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins auxquelles ils sont destinés.

Responsabilités de votre organisation en matière de protection de la vie privée

En vertu du principe d'exactitude, votre organisation doit :

- s'assurer que les renseignements personnels sont aussi exacts, complets et à jour que l'exigent les fins auxquelles ils sont destinés;
- systématiquement mettre à jour les renseignements personnels seulement si cela est nécessaire pour atteindre les fins auxquelles ils ont été recueillis;
- s'assurer que les renseignements sont suffisamment exacts, complets et à jour pour réduire au minimum la possibilité que des renseignements inappropriés soient utilisés pour prendre une décision au sujet de la personne;
- en déterminant le degré d'exactitude et de mise à jour ainsi que le caractère complet que les renseignements personnels nécessitent, tenir compte de l'usage auquel ils sont destinés et des intérêts de la personne.

En vertu du principe d'exactitude, votre organisation devrait :

- s'assurer que les renseignements personnels qui servent en permanence, y compris les renseignements qui sont communiqués à des tiers, sont exacts et à jour, à moins que des limites se rapportant à l'exactitude de ces renseignements ne soient clairement établies.

Comment atteindre ces objectifs

Déterminer les besoins en matière d'exactitude

- Analysez les raisons pour lesquelles votre organisation recueille des renseignements personnels, en tenant autant compte de l'usage auquel ils sont destinés que des intérêts du client;
- Les renseignements personnels ne doivent être systématiquement mis à jour que quand cela est exigé pour les fins auxquelles ils sont recueillis;
- Il est essentiel que les renseignements personnels soient exacts, complets et à jour lorsque l'utilisation de renseignements imprécis, incomplets ou désuets pourrait avoir une influence négative sur une décision à prendre concernant un client ou lui nuire de toute autre façon[4];
- Évaluez l'importance pour les renseignements d'être exacts, complets et à jour lorsqu'ils sont utilisés en permanence ou sont systématiquement communiqués aux tierces parties;
- Demandez-vous si vous pouvez raisonnablement attendre des clients qu'ils prennent eux-mêmes la responsabilité de corriger les renseignements ou de les mettre à jour, par exemple les avis de changement d'adresse pour des abonnements.

[4] Par exemple, en raison d'un renseignement financier désuet, une banque risque de refuser à un client un prêt ou un service.

Établir une politique d'exactitude

- Assurez-vous que votre cadre de gestion de la protection de la vie privée comprend des procédures prévoyant :
  - les types de renseignements personnels devant être systématiquement mis à jour pour demeurer exacts et complets;
  - au besoin, un échéancier et les procédures pour vérifier systématiquement l'exactitude des renseignements personnels et s'assurer qu'ils demeurent exacts et à jour;
  - une obligation d'enregistrer quand les renseignements personnels sont reçus ou mis à jour et que des mesures sont prises pour s'assurer qu'ils sont exacts, complets et à jour;
  - les moyens dont les clients disposent pour contester l'exactitude et l'intégralité des renseignements et y faire apporter les corrections appropriées, conformément au principe de l'accès aux renseignements personnels;
  - des limites clairement établies se rapportant à l'exactitude de ces renseignements et des justifications pour tout renseignement personnel que votre organisation :
    - utilise ou communique en permanence, mais n'a pas l'intention de mettre à jour, ou dont elle ne tient pas à s'assurer qu'ils demeurent exacts;
    - peut raisonnablement s'attendre à ce que les clients corrigent ou mettent à jour de leur propre initiative.

- Rendez accessible au public l'information sur les procédures d'exactitude de votre organisation, conformément au principe de transparence.

SEPTIÈME PRINCIPE – MESURES DE SÉCURITÉ

Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité.

Responsabilités de votre organisation en matière de protection de la vie privée

En vertu du principe des mesures de sécurité, votre organisation doit :

- protéger les renseignements personnels par des mesures de sécurité correspondant à leur degré de sensibilité;
- élaborer des mesures de sécurité pour protéger les renseignements personnels contre la perte ou le vol ainsi que contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées;
- protéger les renseignements personnels quelle que soit la forme sous laquelle ils sont conservés;
- sensibiliser le personnel à l'importance de protéger le caractère confidentiel des renseignements personnels;
- veiller à empêcher les personnes non autorisées d'avoir accès aux renseignements personnels au moment du retrait ou de la destruction des renseignements personnels.

En vertu du principe des mesures de sécurité, votre organisation devrait :

- mieux protéger les renseignements plus sensibles;
- inclure dans ses méthodes de protection :
  - des moyens matériels, par exemple le verrouillage des classeurs et la restriction de l'accès aux bureaux;
  - des mesures administratives, par exemple des autorisations sécuritaires et un accès sélectif;
  - des mesures techniques, par exemple l'usage de mots de passe et du chiffrement.

En vertu du principe des mesures de sécurité, votre organisation peut :

- prendre une variété de mesures de sécurité en fonction du degré de sensibilité des renseignements, de leur quantité, de leur répartition, de leur format et de la méthode de conservation utilisée.

Comment atteindre ces objectifs

Mettre en place une politique de sécurité des renseignements

- Examinez vos pratiques, vos politiques et vos systèmes de sécurité de l'information pour déterminer si votre organisation assume actuellement les responsabilités décrites ci-haut. Prenez les mesures appropriées ci-dessous recommandées pour combler toute lacune;
- Élaborez et mettez en œuvre une politique, ou mettez à jour vos procédures, pour consolider vos pratiques et vos procédures en matière de sécurité de l'information conformément au principe des mesures de sécurité. Établissez une obligation et des procédures connexes pour documenter les atteintes à la sécurité, faire un suivi connexe et informer les personnes touchées. Assurez-vous que votre politique tient compte des responsabilités suivantes le cas échéant.

Mesures de sécurité physiques

- Mettez en œuvre des mesures physiques au besoin pour assurer la sécurité des renseignements personnels que vous détenez, notamment :
  - le verrouillage des classeurs;
  - une politique en matière de rangement du bureau;
  - une restriction de l'accès aux renseignements personnels;
  - la sûreté des locaux;
  - des systèmes d'alarme.

- Assurez-vous que les mesures de sécurité physiques correspondent :
  - à la sensibilité des renseignements personnels (par exemple, meilleure protection des dossiers médicaux ou financiers);
  - à la quantité de renseignements en votre possession et à leur nature;
  - au type et au degré de répartition ou de transmission;
  - aux formats (par exemple, fichiers papier ou électroniques);
  - aux méthodes de conservation.

- Assurez-vous que les mesures de sécurité physiques sont suffisantes pour offrir une protection contre la perte ou le vol et contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées.

Mesures de sécurité administratives

- Mettez en œuvre des mesures administratives au besoin pour assurer la sécurité des renseignements personnels en votre possession, notamment :
  - une autorisation et un accès sélectif;
  - des autorisations sécuritaires et des classifications;
  - des ententes de confidentialité;
  - des procédures de sécurité spécifiques;
  - une formation sur la sécurité de l'information;
  - la surveillance interne régulière des systèmes de sécurité de l'information;
  - la surveillance et la vérification indépendantes régulières des systèmes de sécurité de l'information.

- Assurez-vous que vos mesures de sécurité administratives correspondent :
  - à la sensibilité des renseignements personnels (par exemple, meilleure protection des dossiers médicaux ou financiers);
  - à la quantité de renseignements que vous détenez;
  - au type et au degré de répartition ou de transmission;
  - aux formats (par exemple, documents papier ou fichiers électroniques);
  - aux méthodes de conservation.

- Assurez-vous que vos mesures de sécurité administratives sont suffisantes pour offrir une protection contre la perte ou le vol et contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées.

Mesures de sécurité technologiques

- Mettez en œuvre les mesures technologiques nécessaires afin d'assurer la sécurité des renseignements personnels que vous détenez, notamment :
  - des exigences en matière d'identification (particulièrement pour les opérations en ligne) afin d'établir l'identité de l'utilisateur légitime pour lui donner accès aux renseignements personnels;
  - une authentification (c'est-à-dire mots de passe ou autres identificateurs uniques pour s'assurer de l'accès autorisé aux renseignements personnels). Se reporter aux *Lignes directrices en matière d'identification et d'authentification* du CPVP, accessibles à l'adresse **http://wwwprivcom.gc.ca/**;
  - des mesures de contrôle de l'accès aux systèmes;
  - des voies de communication protégées pour la transmission de renseignements personnels;
  - le chiffrement des données sensibles à des fins de conservation et de transmission;
  - des pare-feux ainsi que des systèmes et des procédures de détection d'intrusion;
  - des pistes de vérification automatiques pour les systèmes de traitement des renseignements personnels;
  - des mesures de contrôle de la maintenance de la sécurité des systèmes, y compris des journaux;
  - des procédures pour les incidents en matière de sécurité et journaux connexes.

- Assurez-vous que les mesures de sécurité technologiques correspondent :
  - à la sensibilité des renseignements personnels (par exemple, meilleure protection des dossiers médicaux ou financiers);
  - à la quantité de renseignements que vous détenez et à leur nature;
  - au type et au degré de répartition ou de transmission.

- Assurez-vous que les mesures de sécurité technologiques (qu'une technologie avec ou sans fil soit utilisée ou non) suffisent à protéger les renseignements personnels contre la perte ou le vol ainsi que contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées;
- En communiquant des renseignements personnels, prenez les mesures correspondant au degré de sensibilité des renseignements et à la méthode de communication pour authentifier l'identité de la personne.

Conscientisation des employés

- Fixez des limites appropriées à l'accès par les employés aux renseignements personnels détenus par votre organisation et à l'utilisation qu'ils en font. En règle générale, accordez l'autorisation d'accès aux renseignements personnels de manière sélective (à savoir, les renseignements exigés pour accomplir des tâches de travail précises);
- Précisez qui est autorisé à avoir accès aux renseignements personnels détenus par votre organisation et à les traiter;
- Faites prendre conscience aux employés de l'importance du maintien de la sécurité et de la protection des renseignements personnels. Dans le cas de renseignements personnels sensibles ou quand les conséquences potentielles de communications inappropriées sont importantes, faites signer des ententes de confidentialité par les employés;
- Formez votre personnel sur les politiques et les procédures de votre organisation pour assurer la sécurité et la confidentialité des renseignements personnels;
- Sensibilisez et formez les employés régulièrement pour vous assurer d'une conscientisation continue et de la sécurité du traitement des renseignements.

Retrait sécuritaire

- Instituez des procédures pour le retrait ou la destruction sécuritaire des renseignements personnels, de l'équipement ou des appareils utilisés pour conserver les renseignements personnels;
- Durant le processus de retrait ou de destruction des renseignements personnels, prenez les mesures appropriées pour empêcher des parties non autorisées d'y avoir accès;
- Durant le processus de retrait de l'équipement ou des appareils utilisés pour conserver les renseignements personnels (comme des classeurs, des ordinateurs, des disquettes et des bandes audio), prenez les mesures appropriées pour exclure ou supprimer tout renseignement conservé ou pour empêcher des parties non autorisées d'y avoir accès.

Travail à domicile et travail à l'extérieur du bureau

- Élaborez des procédures officielles pour les employés emportant des renseignements personnels à l'extérieur de l'entreprise, notamment sur des assistants numériques personnels (ANP) ou des ordinateurs portables, et qui travaillent à l'extérieur du bureau ou à domicile. Analysez les risques de sécurité précis que ces situations créent et mettez au point des solutions pour limiter ces risques.

Sécuriser les transmissions par télécopie

- Pour les renseignements personnels transmis par télécopie, prenez les précautions de sécurité recommandées dans la fiche d'information du CPVP intitulée *Télécopieurs et renseignements personnels*, accessible à **http://www.privcom.gc.ca/**;
- Si vous devez envoyer des renseignements personnels sensibles, envisagez des solutions de remplacement plus sûres que la transmission par télécopie.

HUITIÈME PRINCIPE – TRANSPARENCE

Une organisation doit faire en sorte que des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels soient facilement accessibles à toute personne.

Responsabilités de votre organisation en matière de protection de la vie privée

En vertu du principe de transparence, votre organisation doit :

- faire preuve de transparence au sujet de ses politiques et de ses pratiques concernant la gestion des renseignements personnels;
- faire en sorte que l'information au sujet de ses politiques et de ses pratiques soit facilement accessible sous une forme généralement compréhensible par ses clients;
- communiquer l'information suivante :
  - le nom ou la fonction de même que l'adresse de la personne responsable de la politique et des pratiques de l'organisation en ce qui concerne la protection des renseignements personnels et à qui il faut acheminer les plaintes et les demandes de renseignements;
  - le moyen d'accès aux renseignements personnels que possède l'organisation;
  - le genre de renseignements personnels que possède l'organisation, y compris une explication générale de l'usage auquel ils sont destinés;
  - une copie de toute brochure ou autre document d'information expliquant les politiques, les normes ou les codes de l'organisation;
  - la définition de la nature des renseignements personnels communiqués aux organisations connexes (par exemple, les filiales).

En vertu du principe de transparence, votre organisation peut :

- rendre l'information accessible de diverses façons, est fonction de la nature des activités de l'organisation et d'autres considérations.

Comment atteindre ces objectifs

Créer de la documentation pour informer le public

- Créez de la documentation pour expliquer au public les politiques et les pratiques de gestion des renseignements personnels de votre organisation, conformément au principe de responsabilité. Peuvent figurer parmi ces documents des politiques, des formulaires de demande, des questionnaires, des formulaires d'enquête, des dépliants, des brochures, des sites Web, etc.;
- Cette documentation doit au moins comprendre :
  - le nom ou le titre et l'adresse du responsable de la protection de la vie privée désigné;
  - une indication précisant que le responsable de la protection de la vie privée est la personne à laquelle le public peut adresser ses plaintes ou ses demandes de renseignements concernant les pratiques de l'organisation en matière de gestion des renseignements;
  - les procédures à suivre par le public pour porter plainte auprès de votre organisation relativement à la protection de la vie privée;

- les procédures à suivre par les personnes pour avoir accès à leurs renseignements personnels détenus par votre organisation;
- une description de la nature des renseignements personnels que vous recueillez et que vous détenez;
- une description de la nature des renseignements personnels que vous communiquez à des tierces parties (y compris des filiales et des sociétés affiliées);
- une description de la raison pour laquelle vous utilisez ou communiquez des renseignements personnels;
- des explications concernant toute politique, toute norme ou tout code connexe.

- À titre de pratique exemplaire, indiquez de quelle manière les clients peuvent retirer leur consentement, dans tout document visant à les prévenir de fins secondaires facultatives;
- Assurez-vous que tous vos documents publics sur la façon dont vous traitez les renseignements personnels sont faciles à comprendre par le grand public.

Communiquer l'information

- Dans votre choix de méthodes et de formats pour communiquer l'information au public, rappelez-vous que vous devez permettre aux personnes d'obtenir l'information sans efforts déraisonnables;
- Selon la nature des activités de votre entreprise, communiquez l'information de plusieurs façons pour vous adapter autant que possible à vos clients. Le cas échéant, offrez des brochures dans votre établissement, postez des renseignements à vos clients, offrez l'accès en ligne ou établissez un numéro de téléphone sans frais. Assurez-vous que le message est cohérent peu importe le format;
- Si vous vous servez de documents écrits pour informer le public des fins de la collecte de renseignements et pour lui demander son consentement, faites en sorte que ces documents soient facilement accessibles à des fins de référence au cours du processus de consentement. À titre de pratique exemplaire, offrez ces documents directement et attirez l'attention des personnes sur les fins documentées et sur les clauses de consentement.

Information sur le Web

- Eu égard aux clients qui n'ont pas accès à un ordinateur ou à Internet, n'utilisez pas votre site Web comme unique moyen de communiquer au public votre information sur la protection de la vie privée. Exiger de tous vos clients qu'ils naviguent sur Internet pour trouver l'information sur vos politiques et vos pratiques de protection de la vie privée ne serait généralement pas considéré comme un effort raisonnable de diffusion de cette information;
- Si votre organisation dispose d'un site Web, affichez-y votre politique de protection de la vie privée. Assurez-vous qu'elle couvre tous les types de collecte, d'utilisation et de communication des renseignements personnels faits par l'intermédiaire de votre site Web;
- Prenez les mesures appropriées pour informer les utilisateurs du site Web de toutes les pratiques en ligne de votre organisation en matière de renseignements, notamment de l'utilisation de témoins ou d'autres moyens de suivi invisibles, et expliquez ces pratiques en des termes compréhensibles.

NEUVIÈME PRINCIPE – ACCÈS AUX RENSEIGNEMENTS PERSONNELS

Une organisation doit informer toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de l'usage qui en est fait et du fait qu'ils ont été communiqués à des tiers,et lui permettre de les consulter. Il sera aussi possible de contester l'exactitude et l'intégralité des renseignements et d'y faire apporter les corrections appropriées.

Responsabilités de votre organisation en matière de protection de la vie privée

En vertu du principe d'accès aux renseignements personnels et de l'article 8 de la LPRPDE, votre organisation doit :

- informer la personne qui en fait la demande par écrit de l'existence, de l'utilisation ou de la communication de ses renseignements personnels et lui fournir l'accès à ces renseignements, sous réserve des dispositions de l'article 9 de la LPRPDE;
- permettre à la personne de contester l'exactitude et l'intégralité des renseignements personnels et d'y faire apporter les corrections appropriées;
- sur demande écrite :
  - informer la personne du fait qu'elle possède des renseignements personnels à son sujet, le cas échéant;
  - fournir à la personne l'accès à ces renseignements;
  - indiquer comment les renseignements ont été utilisés ou seront utilisés;
  - informer la personne des tierces parties auxquelles les renseignements ont été communiqués.

  Remarque : Selon l'article 4.9 de la LPRPDE, dans certains cas, il peut être impossible à une organisation de communiquer tous les renseignements personnels qu'elle possède au sujet d'une personne, mais les exceptions en matière d'accès aux renseignements personnels devraient être restreintes et précises. La personne devrait également être informée des raisons pour lesquelles l'accès aux renseignements lui est refusé.
- fournir une liste des organisations auxquelles les renseignements auraient pu être communiqués lorsqu'il n'est pas possible de fournir une liste des organisations auxquelles les renseignements personnels ont effectivement été communiqués;
- fournir sur demande toute aide exigée par les personnes dans la préparation d'une demande d'accès;
- répondre à une demande d'accès en n'exigeant que des droits minimes à la personne;
- donner suite à une demande d'accès avec la diligence voulue et, en tout état de cause, dans les 30 jours suivant sa réception (nota : un accusé de réception ne constitue pas une réponse). Dans les 30 jours suivant la demande, vous devez fournir les renseignements demandés ou indiquer que vous n'avez pas les renseignements demandés;
- lorsqu'une prorogation du délai est nécessaire, envoyer un avis de prorogation au plus tard 30 jours après la date de la demande, avisant la personne du nouveau délai, des motifs de la prorogation et de son droit de déposer une plainte auprès du CPVP;
- fournir les renseignements demandés sous une forme généralement compréhensible (par exemple, expliquer toute abréviation ou tout code utilisé pour enregistrer les renseignements);
- en cas de refus d'accès aux renseignements, informer la personne par écrit des motifs du refus et de tout recours possible en vertu de la LPRPDE;
- conserver les renseignements personnels faisant l'objet d'une demande aussi longtemps que nécessaire afin de permettre à la personne d'épuiser ses recours en vertu de la LPRPDE;
- apporter les modifications nécessaires aux renseignements personnels lorsqu'une personne démontre qu'ils sont inexacts ou incomplets;

- s'il y a lieu, communiquer les renseignements modifiés aux tierces parties ayant accès aux renseignements en question;
- prendre note de l'objet de la contestation lorsqu'une contestation n'est pas réglée à la satisfaction de la personne concernée;
- informer, s'il y a lieu, les tierces parties ayant accès aux renseignements en question du fait que la contestation n'a pas été réglée.

En vertu du principe d'accès aux renseignements personnels, votre organisation devrait :

- donner des renseignements aussi précis que possible sur les tierces parties auxquelles les renseignements personnels de la personne ont été communiqués;
- si possible, indiquer la source des renseignements au moment d'informer la personne que vous possédez des renseignements personnels à son sujet.

En vertu du principe d'accès aux renseignements personnels et de l'article 8 de la LPRPDE, votre organisation peut :

- proroger le délai habituel de 30 jours d'une période maximale de 30 jours dans les cas où :
  - l'observation du délai entraverait gravement l'activité de l'organisation;
  - toute consultation nécessaire pour donner suite à la demande rendrait pratiquement impossible l'observation du délai;

- proroger le délai de 30 jours de la période nécessaire au transfert des renseignements visés sur un support de substitution[5];
- exiger des droits pour répondre à la demande uniquement si elle informe le demandeur du montant approximatif de ceux-ci et que celui-ci l'avise qu'il ne retire pas sa demande;
- décider que les renseignements médicaux seront communiqués par l'entremise d'un médecin;
- exiger que la personne concernée lui fournisse suffisamment de renseignements pour qu'il lui soit possible de la renseigner sur l'existence, l'utilisation et la communication de renseignements personnels. L'information ainsi fournie doit servir à cette seule fin.

Comment atteindre ces objectifs

Se préparer aux demandes d'accès

- Assurez-vous que votre cadre de gestion de la protection de la vie privée comprend des procédures pour traiter les demandes d'accès aux renseignements personnels. Tenez compte de toutes les responsabilités énumérées ci-dessus en vertu du principe d'accès aux renseignements personnels et de l'article 8 de la LPRPDE. Assurez-vous également que vous pouvez donner suite aux demandes de renseignements personnels dans un format de substitution;
- Tenez compte de toutes les exceptions qui s'appliquent à l'accès aux renseignements personnels définies à l'article 9 de la LPRPDE. Si votre organisation refuse l'accès aux renseignements, assurez-vous de pouvoir justifier le refus en raison d'une des exceptions définies à l'article 9;
- Assurez-vous que les systèmes d'information de votre organisation peuvent faciliter la récupération des renseignements personnels et la production de rapports connexes exacts, notamment les communications aux organisations tierces, et que les renseignements demandés peuvent être obtenus sans trop perturber les activités;

[5] Ces supports peuvent être des bandes sonores ou des documents en braille.

- Assurez-vous que les employés assignés au traitement des demandes d'accès connaissent les responsabilités de votre organisation liées au principe d'accès aux renseignements personnels, les procédures et les délais précis à respecter, de même que les exceptions définies à l'article 9 de la LPRPDE;
- Assurez-vous que les employés sont en mesure de reconnaître une demande d'accès à des renseignements personnels et qu'ils savent à qui celle-ci doit être transmise;
- Faites en sorte que l'information sur la façon de demander l'accès aux renseignements personnels auprès de votre organisation soit facilement accessible.

Traiter les demandes d'accès

- Aidez la personne à préparer une demande écrite d'accès aux renseignements personnels, au besoin. À la réception d'une demande d'accès qui nécessite des clarifications, demandez à la personne de fournir suffisamment d'information pour vous permettre de répondre à sa demande et n'utilisez cette information qu'à cette fin;
- À la réception d'une demande d'accès, consignez la date de réception et confirmez l'identité de la personne qui demande l'accès et son droit d'accéder aux renseignements;
- Donnez suite à une demande d'accès aussi rapidement que possible, au plus tard dans les 30 jours de la demande, et ce, sans frais ou à coût modique;
- Informez la personne des coûts approximatifs avant de traiter la demande et vérifiez avec celle-ci si elle souhaite toujours aller de l'avant avec la demande;
- Sur demande expresse :
  - Indiquez à la personne qui demande l'accès si votre organisation possède des renseignements à son sujet;
  - Informez-la de la source des renseignements personnels obtenus, si possible;
  - Expliquez-lui comment votre organisation a utilisé ou utilise les renseignements;
  - Fournissez-lui une liste de toutes les autres organisations auxquelles les renseignements ont été communiqués;
  - S'il n'est pas possible de lui fournir une liste des organisations auxquelles les renseignements ont effectivement été communiqués, fournissez-lui une liste de toutes les autres organisations auxquelles les renseignements ont pu être communiqués;
  - Donnez-lui l'accès aux renseignements;
  - Donnez-lui une copie des renseignements demandés;

- Veillez à ce que les renseignements fournis soient compréhensibles. Expliquez les acronymes, les abréviations et les codes.

Modifier les renseignements personnels

- Permettez à la personne qui demande l'accès aux renseignements de contester l'exactitude et l'intégralité des renseignements;
- Si la personne démontre que des renseignements personnels sont inexacts ou incomplets, apportez les modifications nécessaires à ces renseignements. Il peut s'agir de corriger, de supprimer ou d'ajouter des renseignements;
- Si les renseignements ont été communiqués à des tierces parties, fournissez les renseignements personnels modifiés à ces parties;
- Lorsqu'une contestation n'est pas réglée à la satisfaction de la personne concernée, prenez note de l'objet de la contestation et informez les tierces parties que la contestation n'est pas réglée.

Refuser l'accès

- Si votre organisation refuse de fournir l'accès aux renseignements personnels demandés :
  - Informez par écrit la personne qui demande des renseignements de votre refus dans les 30 jours suivant la réception de sa demande;
  - Expliquez-lui les raisons du refus et indiquez-lui toute exception pertinente définie à l'article 9 de la LPRPDE;
  - Informez-la de tout recours qui lui est possible (tel que son droit de déposer une plainte auprès du CPVP).

- Conservez les renseignements personnels faisant l'objet d'une demande aussi longtemps que nécessaire pour permettre à la personne qui demande l'accès aux renseignements d'épuiser ses recours en vertu de la LPRPDE.

Proroger le délai

- Faites tous les efforts raisonnables pour répondre à une demande d'accès dans le délai prévu de 30 jours. Ne recourez à une prorogation du délai que dans les cas suivants :

  1. Lorsqu'une réponse dans les 30 jours prévus entraverait gravement l'activité de votre organisation;
  2. Lorsqu'il faut prévoir du temps à des fins de consultations;
  3. Lorsque plus de temps est nécessaire pour transférer les renseignements sur un support de substitution.

- Lorsqu'une prorogation est justifiée, limitez cette prorogation à 30 jours supplémentaires dans le premier et le deuxième cas susmentionnés ou aussi longtemps que nécessaire dans le troisième cas susmentionné;
- Lorsqu'une prorogation est justifiée, informez-en par écrit la personne qui demande l'accès aux renseignements dans les 30 jours de la réception de la demande. Informez-la également des raisons de la prorogation et de son droit de déposer une plainte auprès du CPVP.

DIXIÈME PRINCIPE – POSSIBILITÉ DE PORTER PLAINTE À L'ÉGARD DU NON-RESPECT DES PRINCIPES

Toute personne doit être en mesure de se plaindre du non-respect des principes énoncés ci-dessus en communiquant avec le ou les personnes responsables de les faire respecter au sein de l'organisation concernée.

Responsabilités de votre organisation en matière de protection de la vie privée

En vertu du principe de possibilité de porter plainte à l'égard du non-respect des principes, votre organisation doit :

- permettre aux personnes de porter plainte à l'égard du non-respect des dix principes auprès de la personne désignée ou auprès des personnes chargées de voir à ce que l'organisation s'y conforme;
- instaurer des procédures pour recevoir les plaintes et les demandes d'information concernant les politiques et les pratiques de l'organisation en matière de gestion des renseignements personnels et pour y donner suite;
- établir des procédures simples et faciles d'accès pour le dépôt des plaintes;
- informer les personnes qui demandent de l'information ou les plaignants des procédures d'instruction des plaintes;
- examiner toutes les plaintes reçues;
- prendre les mesures correctives appropriées lorsqu'une plainte est fondée, par exemple, la modification des politiques et des pratiques, au besoin.

En vertu du principe de possibilité de porter plainte à l'égard du non-respect des principes, votre organisation devrait :

- s'assurer que ses procédures relatives aux demandes d'information et aux plaintes sont simples et faciles d'accès.

En vertu du principe de possibilité de porter plainte à l'égard du non-respect des principes, votre organisation peut :

- offrir diverses procédures pour le dépôt de plaintes, notamment la soumission des plaintes à l'égard des pratiques de gestion des renseignements personnels à l'organisme de réglementation lié à votre organisation

Comment atteindre ces objectifs

Mettre en œuvre des procédures de dépôt de plaintes à l'égard du non-respect des principes :

- Élaborez des procédures simples et faciles d'accès pour recevoir les plaintes et les demandes d'information sur les politiques et les pratiques de gestion des renseignements personnels de votre organisation et pour y donner suite;
- Assurez-vous que les employés de première ligne et les directeurs connaissent les politiques et les procédures, qu'ils savent distinguer une demande d'information d'une plainte en vertu de la *Loi* et qu'ils peuvent diriger la personne vers le responsable de la protection de la vie privée désigné ou un employé responsable de la gestion des demandes d'information ou des plaintes;

- Assurez-vous que les employés assignés à la gestion des demandes d'information et des plaintes concernant les politiques et les pratiques de gestion des renseignements personnels de votre organisation savent y donner suite en toute connaissance, avec équité et impartialité, et de façon rapide et efficace;
- Facilitez la démarche des personnes souhaitant demander de l'information ou déposer une plainte auprès de votre organisation. Suivez le principe de la transparence et publiez le nom ou le titre de la personne à laquelle les demandes d'information et les plaintes devraient être soumises (c'est à dire, le responsable de la protection de la vie privée), de même que son adresse professionnelle;
- Informez les personnes qui demandent de l'information ou qui déposent une plainte des procédures de votre organisation en matière de gestion des demandes d'information et de réception des plaintes. Informez-les également de tout autre recours possible auprès des associations industrielles et des organismes de réglementation liés à votre organisation;
- Assurez-vous que la direction s'engage à appuyer les conclusions et les recommandations découlant de l'examen d'une plainte et à corriger toute lacune démontrée dans les politiques et les pratiques de l'organisation en matière de gestion des renseignements personnels.

Recevoir les plaintes

- Consignez la date de réception de la plainte ainsi que sa nature (par exemple, un accès aux renseignements refusé, une réponse tardive à une demande d'accès, des renseignements incomplets ou inexacts au dossier, des mesures de sécurité inadéquates ou la collecte, l'utilisation, la communication et la conservation inappropriées);
- Accusez réception de la plainte sans délai;
- Communiquez avec le plaignant pour clarifier le problème, au besoin.

Examiner les plaintes

- Examinez toutes les plaintes reçues;
- Confiez le dossier à une personne possédant les compétences voulues pour examiner la plainte avec équité et impartialité et permettez à cette personne de consulter tous les dossiers, les employés ou les autres intervenants qui ont traité les renseignements personnels ou la demande d'accès;
- Procédez à l'examen sans tarder;
- Une fois l'examen terminé, informez clairement et rapidement la personne des résultats, des mesures pertinentes qui ont été prises et de tout autre recours dont elle dispose si elle n'est pas satisfaite des résultats;
- Lorsque les résultats de l'examen le justifient, accordez l'accès aux renseignements, corrigez tout renseignement inexact ou incomplet ou modifiez les politiques, les procédures et les pratiques problématiques de gestion des renseignements personnels;
- Assurez-vous que le personnel de votre organisation est au fait de toutes ces modifications;
- Consignez tous les résultats d'examen et toutes les mesures correctives prises pour vous assurer d'une application cohérente de la LPRPDE à l'avenir.

PARTIE 2 : LISTES DE CONTRÔLE DIAGNOSTIQUES

Quand votre cadre de protection de la vie privée aura été en œuvre depuis assez longtemps pour que son efficacité puisse faire l'objet d'une vérification, ces listes de contrôle vous permettront d'évaluer à quel point vous atteignez les objectifs définis à l'annexe 1 de la LPRPDE. Pour chaque question, vous devez décrire la preuve sur laquelle l'évaluation est fondée ainsi que toute circonstance atténuante pour les objectifs qui n'ont pas été « conformes ». La preuve devrait suffire à rendre l'évaluation significative. Vous devez décrire la façon dont vous gérez les renseignements personnels pour atteindre chaque objectif, que ce soit au moyen de politiques, de procédures, de processus ou de structures ou valeurs organisationnelles.

Deux critères permettent de juger du bon fonctionnement d'une mesure de protection de la vie privée :

1. La mesure de protection de la vie privée[6] doit avoir été conçue de manière appropriée pour répondre aux exigences de la loi;
2. La mesure de protection de la vie privée doit fonctionner comme prévu (les employés doivent suivre la politique).

Vous ne pouvez pas déterminer votre degré de conformité à la LPRPDE sans avoir évalué vos mesures de protection de la vie privée et leur efficacité réelle dans l'environnement d'entreprise.

Interpréter les résultats de l'autoévaluation

Avant de tirer les conclusions des résultats de l'autoévaluation, étudiez-les avec chaque unité fonctionnelle concernée. Notez toute circonstance atténuante liée à un mauvais résultat. Par exemple, les mauvais résultats relatifs aux formulaires de consentement remplis par les employés pendant deux mois pourraient s'expliquer par la présence temporaire d'un employé étudiant au service des Ressources humaines durant cette période. Les résultats pourraient être différents pour une autre période.

Un cadre de protection de la vie privée arrivé à maturité se caractérise par la diligence raisonnable et la documentation relative à l'acceptation du risque ou aux décisions d'atténuation du risque, ce qui devrait aider à fixer des priorités en matière de mesures correctives et à établir un échéancier réaliste.

Si votre organisation est incapable d'indiquer le degré d'atteinte des objectifs définis, elle risque de ne pas être conforme à la LPRPDE. Vous devriez prendre en compte les risques liés à chaque secteur pour lequel vous n'êtes pas conforme aux objectifs et combler en conséquence les lacunes de votre cadre de gestion de la protection de la vie privée. Rappelez-vous qu'une seule mesure corrective peut permettre d'atteindre plusieurs objectifs. Il est donc important de faire le suivi des mesures correctives et de chacune des conséquences positives pour les lacunes décelées.

L'étude des résultats de l'autoévaluation permettra à votre organisation de consacrer des ressources à l'amélioration des pratiques de protection de la vie privée dans les secteurs appropriés. Analysez les résultats de votre autoévaluation pour savoir si votre organisation affiche des faiblesses relativement à certains principes en particulier ou si elle n'a simplement pas atteint un certain niveau de maturité.

[6] Dans ce contexte, une « mesure de protection de la vie privée » peut être une politique ou un ensemble de procédures que vous avez mis en œuvre afin d'être conforme à chacun des dix principes.

Un programme de protection de la vie privée prend du temps avant d'arriver à maturité. L'évaluation de la conformité de votre organisation devrait donc se faire en tenant compte de cette courbe de maturité. Quand vous songez à une façon d'évaluer les résultats de votre programme en fonction d'objectifs de conformité et de pratiques exemplaires, choisissez une échelle pertinente à l'ensemble de votre organisation. L'échelle de maturité doit être assez souple pour s'appliquer aux diverses unités fonctionnelles et aux différents intervenants. Pour évaluer vos résultats totaux pour chaque principe, vous pouvez tenir compte de l'échelle de maturité suivante :

- **Niveau de maturité 1** – Maturité inexistante ou non développée (non-conformité aux exigences)
- **Niveau de maturité 2** – Maturité aux premières étapes de développement (conformité partielle aux exigences)
- **Niveau de maturité 3** – Maturité à une étape avancée (conformité à la plupart des exigences – améliorations possibles)
- **Niveau de maturité 4** – Pleine maturité (conformité aux exigences – seules de légères adaptations sont requises, voire aucune)

Plan d'action :

Les résultats de l'autoévaluation peuvent indiquer l'existence de risques au sein de votre organisation en matière de protection de la vie privée et de conformité. Le risque lié à la protection de la vie privée consiste en l'existence possible d'une menace en raison des vulnérabilités :

- du matériel contenant des renseignements personnels,
- d'un processus opérationnel dans le cadre duquel sont traités des renseignements personnels et qui pourrait provoquer un accès involontaire aux renseignements personnels ou les modifier, voire les endommager.

> **Les risques peuvent peser sur votre organisation, vos clients ou les deux.**

Les conséquences ou la gravité du risque sont proportionnelles à la probabilité que le risque se concrétise et à ses répercussions potentielles sur l'organisation et les personnes.

Une évaluation des facteurs relatifs à la vie privée consiste à déceler et à analyser les risques relatifs à la protection de la vie privée. Elle constitue le fondement des méthodes visant à gérer ces risques, y compris les mesures qu'il faudrait mettre en œuvre pour atténuer le risque jusqu'à ce qu'il atteigne un niveau acceptable.

Classez par importance les lacunes de votre programme de protection de la vie privée et élaborez un plan d'action. Les secteurs non conformes peuvent être classés au moyen d'un processus d'évaluation des risques de protection de la vie privée :

- Repérez toutes les réponses « non conforme » et « partiellement conforme » de votre autoévaluation et réservez-les pour un examen ultérieur;
- Imaginez les répercussions possibles de la non-conformité ou d'une conformité partielle aux exigences, par exemple :

Objectif/Critère :	Répercussions possibles :
Vous examinez toutes les plaintes que vous recevez sur vos politiques et vos pratiques de traitement des renseignements personnels.	Si vous ne le faites pas, le risque augmente que les problèmes sous-jacents en matière de protection de la vie privée ne soient pas cernés ni résolus en temps opportun, ce qui diminuera la satisfaction des clients.

Vérifiez si vous avez élaboré des mesures correctives pour atténuer les répercussions possibles d'un manquement à vos responsabilités en matière de conformité. En l'absence de mesures correctives, déterminez d'autres stratégies d'atténuation pour que vos pratiques se rapprochent de celles qui sont exigées et pour mieux gérer les risques relatifs à la protection de la vie privée décelés à l'étape précédente.

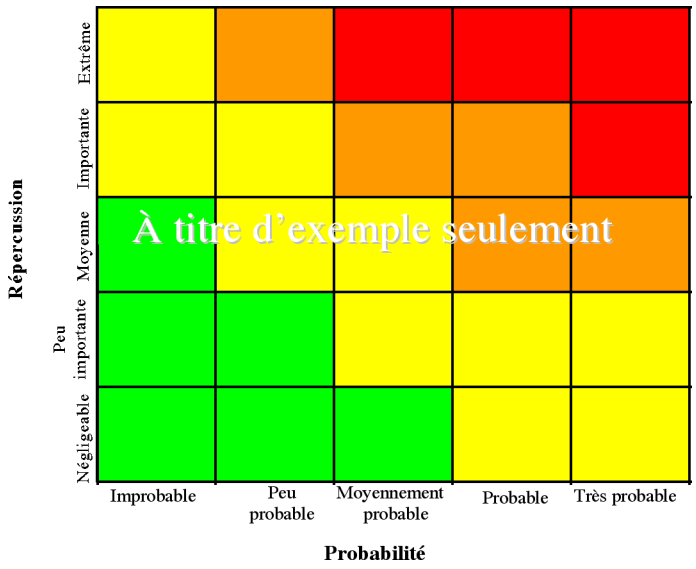
Que vous disposiez de mesures correctives partielles ou que vous n'en ayez aucune mise en place, utilisez les résultats de l'évaluation et votre connaissance de l'organisation pour déterminer les probabilités qu'un risque se concrétise et les conséquences qu'un tel événement pourrait entraîner. Vous pouvez utiliser un type d'échelle comme celui présenté au tableau suivant pour évaluer les probabilités qu'un risque se concrétise pour les cas de lacune en matière de conformité aux exigences :

PROBABILITÉS QU'UN RISQUE SE CONCRÉTISE		
NIVEAU	**DESCRIPTEUR**	**DESCRIPTION**
5	Très probable	Cet événement se produit régulièrement ici.
4	Probable	Cet événement s'est produit ici plus d'une fois ou se produit ailleurs dans des circonstances semblables.
3	Moyennement probable	Cet événement s'est déjà produit ici, ou a été observé dans des circonstances semblables.
2	Peu probable	Il est déjà arrivé que cet événement se produise ailleurs dans des circonstances semblables, mais pas ici.
1	Improbable	Cet événement ne s'est presque jamais produit; il se peut qu'il se produise, mais seulement dans des circonstances exceptionnelles.

RÉPERCUSSION		
NIVEAU	**DESCRIPTEUR**	**DESCRIPTION**
5	Extrême	Événement majeur pouvant empêcher, à long terme, que l'organisation atteigne ses objectifs. Les conséquences pourraient être de gros problèmes à long terme en matière de réglementation, de réputation, d'exploitation ou des problèmes financiers pour l'organisation, qui nécessiteraient l'intervention de la haute direction. Il pourrait également s'agir d'une nuisance sur les plans financier, émotionnel ou de la réputation pour une personne victime d'une atteinte à la vie privée.
4	Importante	Événement critique que l'organisation peut supporter si elle le gère bien. Les conséquences pourraient être de gros problèmes en matière de réglementation, de réputation, d'exploitation ou des problèmes financiers pour l'organisation, qui nécessiteraient l'intervention de la haute direction. Il pourrait également s'agir d'une nuisance sur les plans de la réputation, financier ou émotionnel pour une personne victime d'une atteinte à la vie privée.
3	Moyenne	Événement important pouvant être géré par l'organisation dans des circonstances normales. Les conséquences pourraient être des problèmes en matière de réglementation, de réputation, d'exploitation ou des problèmes financiers pour l'organisation, laquelle pourrait les gérer à l'interne. Sous cette catégorie, une personne pourrait aussi être touchée de façon modérée; certains de ses renseignements financiers pourraient être exposés, comme son salaire. Les conséquences sur la personne demeurent à l'intérieur de l'organisation et toute autre exposition est limitée.
2	Peu importante	Événement dont les conséquences peuvent être absorbées. La direction doit toutefois faire un effort pour les réduire au minimum. Les conséquences pourraient menacer les normes de l'organisation en matière de réglementation, de réputation ou d'exploitation, mais les problèmes seraient réglés à l'interne. Les conséquences seraient moindres pour l'organisation. Les conséquences sur la personne demeurent à l'intérieur de l'organisation et toute autre exposition est limitée.
1	Négligeable	Événement dont les conséquences peuvent être absorbées dans des circonstances normales. Les conséquences pourraient menacer les normes de l'organisation en matière de réglementation, de réputation ou d'exploitation, mais les problèmes seraient réglés à l'interne. Les conséquences seraient moindres pour l'organisation. Les conséquences sur la personne demeurent à l'intérieur de l'organisation et toute autre exposition est limitée.

Classez les résultats de votre évaluation du risque. S'il est probable qu'un événement défavorable se produise (par exemple, vous savez que votre organisation reçoit deux plaintes par mois et vous n'avez mis en place aucune mesure de sécurité pour les traiter) et que les répercussions soient également importantes (par exemple, vous croyez qu'un problème concernant une atteinte à votre crédibilité ou votre marque, ou concernant une plainte pourrait être soumis au CPVP), cet événement devrait être classé à un niveau plus élevé que les lacunes qui risquent moins de se produire et dont les répercussions sont moindres.

Reportez les résultats de ce classement sur un graphique des points chauds pour visualiser le classement relatif de vos lacunes. Voici un exemple de graphique des points chauds :



Adoptez des mesures précises visant à combler toute lacune en modifiant votre cadre de protection de la vie privée pour réduire la probabilité que l'événement défavorable se produise ou pour en atténuer les répercussions. Dans bien des cas, les mesures de contrôle que vous choisirez auront des incidences positives sur ces deux aspects du risque et pourraient combler de nombreuses lacunes.

Parcourez la liste des mesures que vous devez prendre pour combler les lacunes dans votre cadre de protection de la vie privée. Repérez les activités qui auront des répercussions sur plus d'un objectif. Vous pouvez aussi vous concentrer sur les mesures à prendre qui atténuent des risques plus élevés tout en étant relativement faciles à mettre en œuvre.

Déterminez les projets précis qui permettront d'améliorer les activités de protection de la vie privée. L'information que vous avez recueillie grâce au processus d'autoévaluation, y compris l'information concernant le risque, peut servir à rédiger une analyse de rentabilisation pour obtenir un budget et des ressources supplémentaires.

LISTE DE CONTRÔLE POUR LE PREMIER PRINCIPE – RESPONSABILITÉ

Énoncé	Évaluation			Preuve	Mesures
	Conforme	Non conforme	Partiellement conforme		
Vous avez analysé vos politiques de protection de la vie privée et trouvez qu'elles sont complètes et faciles à comprendre.					
Vous avez clairement déterminé qui, dans votre organisation, est responsable de la gouvernance et de la gestion de la protection de la vie privée.					
Vous avez des politiques et des pratiques de protection de la vie privée qui s'appliquent aux renseignements personnels de vos employés et de vos clients.					
Votre cadre de protection de la vie privée prévoit clairement que vous êtes responsable de tous les renseignements personnels que vous détenez ou gérez, y compris les renseignements transférés à une tierce partie à des fins de traitement.					
Vous avez nommé au moins une personne responsable de la conformité globale de votre organisation à la LPRPDE.					
Vous avez porté à la connaissance des employés les politiques et les procédures nécessaires et les avez formés pour qu'ils fournissent aux personnes en faisant la demande le nom, l'adresse et le numéro de téléphone de la personne-ressource en ce qui concerne la LPRPDE.					
Vous utilisez des ententes contractuelles avec les tierces parties auxquelles les renseignements sont communiqués aux fins de traitement pour vous assurer que leur niveau de protection de la vie privée est comparable au vôtre.					
Vous vous êtes assuré que les tierces parties ont mis en œuvre les mesures de contrôle de protection de la vie privée inscrites sur toutes les ententes contractuelles.					
Vous êtes responsable de la protection des renseignements personnels.					
Votre cadre de protection de la vie privée tient compte du principe de détermination des fins de la collecte de renseignements.					
Votre cadre de protection de la vie privée tient compte du principe de consentement relatif à la collecte de renseignements personnels.					
Votre cadre de protection de la vie privée tient compte du principe de limitation de la collecte des renseignements personnels.					
Votre cadre de protection de la vie privée tient compte du principe de limitation de l'utilisation, de la communication et de la conservation des renseignements personnels.					
Votre cadre de protection de la vie privée tient compte du principe d'exactitude des renseignements personnels.					
Votre cadre de protection de la vie privée tient compte du principe des mesures de sécurité relatives aux renseignements personnels.					

Énoncé	Évaluation			Preuve	Mesures
	Conforme	Non conforme	Partiellement conforme		
Votre cadre de protection de la vie privée tient compte du principe de transparence relative aux renseignements personnels.					
Votre cadre de protection de la vie privée tient compte du principe d'accès aux renseignements personnels.					
Votre cadre de protection de la vie privée tient compte du principe de possibilité de porter plainte à l'égard du non respect des principes relatifs aux renseignements personnels.					
Vous avez communiqué au personnel l'information liée aux politiques, aux procédures et aux pratiques de traitement des renseignements personnels.					
Vous avez formé votre personnel sur la protection des renseignements personnels en l'informant des politiques, des procédures et des pratiques exemplaires de votre organisation en matière de protection de la vie privée.					
Vous avez des moyens de déterminer quels membres de votre personnel devraient être formés sur la protection de la vie privée, qu'il s'agisse de former du nouveau personnel ou de renouveler la formation du personnel en place.					
Vous avez rédigé des documents pour expliquer vos politiques et vos procédures de protection des renseignements personnels à vos clients et au grand public.					

ÉVALUATION SUPPLÉMENTAIRE POUR LES ENTREPRISES FÉDÉRALES :

Énoncé	Évaluation			Preuve	Mesures
	Conforme	Non conforme	Partiellement conforme		
Vous avez mis à la disposition de vos employés de l'information expliquant les politiques et les procédures qui s'appliquent à leurs renseignements personnels.					

LISTE DE CONTRÔLE POUR LE DEUXIÈME PRINCIPE – DÉTERMINATION DES FINS DE LA COLLECTE DES RENSEIGNEMENTS

Énoncé	Évaluation			Preuve	Mesures
	Conforme	Non conforme	Partiellement conforme		
Vous indiquez les raisons pour lesquelles vous recueillez les renseignements personnels au moment de leur collecte ou avant.					
Vous avez documenté les fins de votre collecte de renseignements personnels.					
Vous avez prévenu vos clients des nouvelles fins auxquelles vous utiliserez les renseignements si vous ne l'avez pas fait au moment de leur collecte.					
Vous cherchez à obtenir le consentement des clients avant d'utiliser leurs renseignements pour toute nouvelle fin, le cas échéant.					
Vous avez prévenu vos clients des fins de la collecte de renseignements avant de les utiliser ou de les communiquer si vous n'avez pas pu le faire au moment de la collecte.					
Vous avez déterminé la quantité et la nature des renseignements nécessaires pour réaliser les fins auxquelles ils ont été recueillis.					
Vous avez déterminé les fins auxquelles vous recueillez les renseignements personnels, et que la quantité et la nature des renseignements personnels recueillis sont raisonnables dans des circonstances d'affaires normales.					
Vous avez établi une distinction entre les renseignements essentiels (exigés aux fins d'affaires principales) et les renseignements non essentiels (les renseignements volontairement donnés qui facilitent l'utilisation à des fins secondaires).					
Vous avez défini que les renseignements non essentiels étaient donnés volontairement et vous avez indiqué à votre personnel comment procéder quand les clients refusaient de les donner à des fins secondaires.					

LISTE DE CONTRÔLE POUR LE TROISIÈME PRINCIPE – CONSENTEMENT

Énoncé	Évaluation			Preuve	Mesures
	Conforme	Non conforme	Partiellement conforme		
Vous obtenez le consentement des clients pour toute collecte, utilisation ou communication de leurs renseignements personnels.					
Si vous n'obtenez pas le consentement des clients pour toute collecte, utilisation ou communication de leurs renseignements personnels, vous avez déterminé qu'il n'était pas exigé en vertu de l'article 7 de la LPRPDE.					
Vous faites des efforts raisonnables pour vous assurer que les clients sont prévenus des fins auxquelles les renseignements personnels seront utilisés ou communiqués.					
Vous n'exigez pas des clients qu'ils donnent leur consentement pour la collecte, l'utilisation ou la communication de renseignements personnels autres que ceux qui sont nécessaires pour réaliser les fins explicitement indiquées et limitées, pour le motif que vous fournissez un bien ou un service.					
Vous évaluez les fins et limitez la collecte, l'utilisation et la communication des renseignements personnels quand il s'agit d'une condition à la fourniture d'un bien ou à la prestation d'un service.					
Vous obtenez le consentement de façon honnête et licite.					
Vous permettez à un client de retirer son consentement à tout moment sous réserve de restrictions légales ou contractuelles et d'un préavis raisonnable.					
Vous informez vos clients des conséquences d'un retrait du consentement.					
Vous tenez compte de la sensibilité et de l'utilisation prévue des renseignements personnels ainsi que des attentes raisonnables des clients pour déterminer la forme de consentement (implicite ou explicite) que vous accepterez pour la collecte, l'utilisation et la communication des renseignements personnels.					

LISTE DE CONTRÔLE POUR LE QUATRIÈME PRINCIPE – LIMITATION DE LA COLLECTE

Énoncé	Évaluation			Preuve	Mesures
	Conforme	Non conforme	Partiellement conforme		
Vous limitez la quantité et la nature des renseignements personnels que vous recueillez à ce qui est nécessaire aux fins déterminées.					
Vous recueillez les renseignements seulement de façon honnête et licite.					
Vous avez documenté la nature précise des renseignements que vous recueillez ainsi que les fins de leur collecte.					
Vous avez documenté lorsque vous recueillez les renseignements de sources autres que la personne concernée.					
Vous établissez une distinction entre la collecte obligatoire et la collecte facultative de renseignements personnels.					
Vous limitez votre collecte du NAS aux fins légalement déterminées.					

LISTE DE CONTRÔLE POUR LE CINQUIÈME PRINCIPE – LIMITATION DE L'UTILISATION, DE LA COMMUNICATION ET DE LA CONSERVATION

Énoncé	Évaluation			Preuve	Mesures
	Conforme	Non conforme	Partiellement conforme		
Vous n'utilisez ni ne communiquez les renseignements à des fins autres que celles auxquelles ils ont été recueillis, sauf avec le consentement de la personne ou tel qu'il est exigé par la loi.					
Vous documentez les nouvelles fins déterminées après que les renseignements personnels ont été recueillis.					
Vous ne conservez les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins déterminées.					
Vous conservez les renseignements personnels utilisés pour prendre une décision au sujet d'une personne pendant un temps raisonnable. De cette façon, celle-ci peut y avoir accès.					
Votre cadre de gestion de la protection de la vie privée régit la destruction des renseignements personnels ainsi que le rôle des entités chargées de l'exécution de cette tâche.					

LISTE DE CONTRÔLE POUR LE SIXIÈME PRINCIPE – EXACTITUDE

Énoncé	Évaluation			Preuve	Mesures
	Conforme	Non conforme	Partiellement conforme		
Vous prenez des mesures raisonnables pour vous assurer que les renseignements personnels sont exacts, complets et à jour avant de les utiliser pour prendre des décisions.					
Vous ne mettez à jour les renseignements personnels que si ce processus est nécessaire pour les fins auxquelles les renseignements ont été recueillis.					
Votre cadre de gestion de la protection de la vie privée permet de veiller à ce que les renseignements personnels soient exacts, complets et à jour, notamment au moyen d'un processus grâce auquel les personnes peuvent contester l'exactitude des renseignements.					
Votre cadre de gestion de la protection de la vie privée précise quand les mises à jour sont appropriées en fonction des fins et des utilisations déterminées des renseignements ainsi que des intérêts de la personne.					
Vous consignez le moment et l'endroit où les renseignements principaux ont été recueillis, y compris les dates auxquelles ils ont été corrigés ou mis à jour.					
Vous contrôlez, évaluez ou vérifiez périodiquement les renseignements détenus et les bases de données pour vous assurer que les renseignements principaux sont exacts, complets et à jour.					

LISTE DE CONTRÔLE POUR LE SEPTIÈME PRINCIPE – MESURES DE SÉCURITÉ

Énoncé	Évaluation			Preuve	Mesures
	Conforme	Non conforme	Partiellement conforme		
Vous avez pris des mesures de sécurité physiques, techniques et administratives pour protéger les renseignements personnels contre la perte ou le vol, de même que contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées.					
Vous choisissez les mesures de sécurité en fonction du degré de sensibilité des renseignements et des méthodes utilisées pour les transmettre.					
Vous protégez les renseignements personnels quelle que soit la forme sous laquelle ils sont conservés.					
Vous sensibilisez le personnel à l'importance de protéger le caractère confidentiel des renseignements personnels.					
Vous avez mis en œuvre des processus pour empêcher les personnes non autorisées d'avoir accès aux renseignements personnels au moment du retrait ou de la destruction des renseignements.					
Vous avez mis en œuvre diverses politiques et pratiques de sécurité des renseignements et y adhérez.					
Vous avez établi une politique concernant l'atteinte à la sécurité des renseignements et vous vous engagez à examiner les causes fondamentales de telles atteintes.					
Vous avez élaboré et mis en œuvre des politiques et des pratiques comprenant des mesures de sécurité appropriées pour toutes les utilisations des renseignements personnels faites à l'extérieur de votre bureau.					

LISTE DE CONTRÔLE POUR LE HUITIÈME PRINCIPE – TRANSPARENCE

Énoncé	Évaluation			Preuve	Mesures
	Conforme	Non conforme	Partiellement conforme		
Vous mettez à la disposition des personnes l'information sur les politiques et les procédures liées à la gestion des renseignements personnels.					
Vous expliquez aux clients pourquoi vous recueillez leurs renseignements personnels, comment vous les utilisez et quand vous les communiquerez.					
Vous indiquez aux clients la personne qui dans l'organisation est responsable de traiter les questions ou les plaintes relatives à la gestion des renseignements personnels.					
Vous indiquez sur demande le nom ou la fonction de même que l'adresse de la personne responsable des politiques et des pratiques de l'organisation.					
Vous décrivez à vos clients comment ils peuvent obtenir l'accès à leurs renseignements personnels ou les corriger.					
Vous fournissez aux personnes une description des renseignements personnels que vous détenez et de ceux que vous communiquez à d'autres organisations.					

LISTE DE CONTRÔLE POUR LE NEUVIÈME PRINCIPE – ACCÈS AUX RENSEIGNEMENTS PERSONNELS

Énoncé	Évaluation			Preuve	Mesures
	Conforme	Non conforme	Partiellement conforme		
Vous avez adopté des politiques et des procédures pour répondre aux demandes de renseignements personnels en vertu de la LPRPDE.					
Vous avez informé le personnel de la nécessité d'adresser les demandes d'accès aux renseignements à l'employé responsable de traiter ces demandes.					
À la réception d'une demande écrite, vous informez les personnes de l'existence, de l'utilisation et de la communication de leurs renseignements personnels.					
À la réception d'une demande écrite, vous fournissez aux personnes l'accès aux renseignements personnels.					
Vous limitez le refus de fournir l'accès aux renseignements aux exceptions décrites à l'article 9 de la LPRPDE.					
Sur demande, vous fournissez un rapport sur les utilisations des renseignements.					
Vous fournissez une liste de toutes les tierces parties à qui les renseignements ont été communiqués (ou une liste des types de tierces parties à qui de tels renseignements sont généralement communiqués) à la réception d'une demande en ce sens.					
Vous prêtez assistance aux personnes qui déclarent avoir besoin d'aide pour remplir une demande de renseignements.					
Vous répondez à une demande de renseignements à un coût minimal ou nul pour la personne.					
Vous répondez à une demande de renseignements en 30 jours maximum, à moins que vous ne préveniez le demandeur durant cette période que vous devez proroger le délai fixé pour la réponse et que vous ne l'informiez de ce nouveau délai et de son droit de déposer une plainte auprès du CPVP.					
Vous ne comptez sur la prorogation du délai que dans les cas où répondre dans les 30 jours, tel qu'il est prévu au départ, nuirait gravement à vos activités, ou quand du temps supplémentaire est nécessaire pour procéder à des consultations ou pour transférer les renseignements personnels sur un support de substitution.					
À la demande d'une personne, vous fournissez l'accès aux renseignements dans un format qui est lisible, ainsi qu'une explication des abréviations ou des codes.					
Vous informez le demandeur des motifs pour lesquels l'accès lui est refusé ainsi que de tout recours possible.					
Vous permettez à une personne de contester l'exactitude des renseignements personnels et vous les corrigez quand elle démontre que ces renseignements sont inexacts ou incomplets.					
Vous transmettez les renseignements personnels corrigés aux tierces parties qui auraient reçu les renseignements originaux.					

LISTE DE CONTRÔLE POUR LE DIXIÈME PRINCIPE – POSSIBILITÉ DE PORTER PLAINTE À L'ÉGARD DU NON-RESPECT DES PRINCIPES

Énoncé	Évaluation			Preuve	Mesures
	Conforme	Non conforme	Partiellement conforme		
Vous permettez aux personnes de porter plainte à l'égard du non-respect des principes auprès de la personne désignée responsable de la conformité à la LPRPDE.					
Vous avez mis en place des politiques et des procédures pour recevoir les plaintes ou les demandes de renseignements sur vos politiques et vos pratiques de gestion des renseignements personnels et pour y donner suite.					
Vous informez les personnes ou les plaignants des procédures relatives aux plaintes, notamment de leur droit de porter plainte auprès d'un organisme de réglementation.					
Vous examinez toutes les plaintes que vous recevez relativement à vos politiques et à vos pratiques de gestion des renseignements personnels.					
Vous modifiez vos mesures si une plainte est appuyée par des preuves et prenez les mesures nécessaires pour réduire au minimum les probabilités que le problème se répète.					

ANNEXE A

APERÇU DE LA LPRPDE

Les organisations assujetties à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) doivent connaître cette loi. Cet outil d'autoévaluation devrait être utilisé de concert avec la *Loi*. Vous trouverez de l'information sur la LPRPDE sur le site Web du Commissariat à la protection de la vie privée (CPVP), à l'adresse **http://www.privcom.gc.ca/**.

Le but de la LPRPDE est d'appuyer et de promouvoir le commerce électronique en protégeant les renseignements personnels. La Partie 1 de la Loi établit les règles raisonnables pour la gouvernance de la collecte, de l'utilisation et de la communication des renseignements personnels de manière à respecter le droit des personnes à la protection de leur vie privée. D'autres parties de la *Loi* prévoient des solutions de rechange électroniques et facilitent l'utilisation des documents et des publications électroniques à différentes fins.

Les organisations visées par la *Loi* doivent obtenir le consentement de la personne concernée avant de recueillir, d'utiliser ou de communiquer ses renseignements personnels. Toute personne a le droit de consulter les renseignements personnels que détient une organisation à son sujet et, au besoin, d'en contester l'exactitude. Les renseignements personnels ne peuvent être utilisés qu'aux fins auxquelles ils ont été recueillis. L'organisation qui entend les utiliser à une autre fin doit obtenir un nouveau consentement. Les personnes devraient également avoir l'assurance que les renseignements qui les concernent seront protégés au moyen de mesures de sécurité précises, c'est-à-dire qu'ils seront, par exemple, conservés sous clé ou protégés au moyen de mots de passe ou du chiffrement des données.

Une organisation est responsable de la protection des renseignements personnels dont elle a la gestion et doit les traiter de façon équitable en tout temps, au sein même de l'organisation et dans le cadre de toute entente avec une tierce partie.

ORGANISATIONS VISÉES PAR LA LPRPDE

Dans le cadre des activités commerciales

Toute organisation qui recueille, utilise ou communique des renseignements personnels dans le cadre d'activités commerciales est visée par la LPRPDE. Selon la LPRPDE, une activité commerciale est définie comme suit :

> *Toute activité régulière ainsi que tout acte isolé qui revêtent un caractère commercial de par leur nature, y compris la vente, le troc ou la location de listes de donneurs, d'adhésion ou de collecte de fonds.*

Le terme « organisation » « s'entend notamment des associations, sociétés de personnes, personnes et organisations syndicales ». La définition est voulue vaste et inclusive.

Le gouvernement fédéral peut exclure des organisations ou des activités dans les provinces qui ont adopté une loi réputée être essentiellement similaire à la loi fédérale. Dans ces provinces, la LPRPDE continue de s'appliquer aux secteurs privés réglementés par le gouvernement fédéral, notamment les banques, les entreprises de transport aérien, les compagnies de téléphone, les entreprises de télédiffusion et les compagnies de chemin de fer, et aux renseignements personnels dans les transactions interprovinciales ou internationales, et ce, par toutes les organisations exerçant des activités commerciales. Jusqu'à maintenant, le Québec, la Colombie-Britannique, l'Alberta ainsi que, dans le domaine des soins de santé, l'Ontario, ont promulgué une loi réputée être essentiellement similaire à la loi fédérale.

Les municipalités, universités, écoles et hôpitaux

La *Loi constitutionnelle de 1867* confère aux provinces le pouvoir sur les institutions municipales, les écoles et les hôpitaux. La LPRPDE repose sur la compétence du gouvernement fédéral en matière de « réglementation du trafic et du commerce ».

Bien que les municipalités, les établissements d'enseignement et les hôpitaux puissent à l'occasion fournir des services moyennant des frais, ils ne font pas, dans l'ensemble, du commerce tel qu'il est énoncé dans la Constitution canadienne. De plus, ces institutions dépendent complètement ou partiellement des taxes et impôts levés par les municipalités ou les provinces ainsi que des subventions provinciales.

Par conséquent, le CPVP est d'avis qu'en règle générale, la LPRPDE ne s'applique pas aux activités essentielles des municipalités, des universités, des écoles et des hôpitaux. Par activités essentielles, on entend les activités qui sont au cœur du mandat et des responsabilités de ces institutions.

La prestation d'un service moyennant des frais n'entraîne pas nécessairement l'application de la *Loi* si le service s'inscrit dans les activités essentielles de l'institution. Par exemple, l'imposition de frais pour une chambre individuelle ou d'un supplément pour un plâtre en fibre de verre ne signifie pas automatiquement que l'hôpital ou la transaction même sont assujettis à la *Loi*. De même, une municipalité peut imposer des frais par sac pour la collecte des ordures ou imposer des frais pour l'utilisation d'un terrain de jeu ou d'un aréna sans être assujettie à la *Loi*.

Une municipalité, une université, une école ou un hôpital peuvent être assujettis à la *Loi* lorsqu'ils exercent une activité commerciale non essentielle, à moins qu'une loi réputée être essentiellement similaire à la loi fédérale ne s'applique. Par exemple, si une université vendait ou troquait une liste des anciens élèves, cette activité serait considérée comme une activité commerciale et cette transaction précise serait assujettie à la *Loi*. De plus, la collecte de renseignements personnels par une université ou un hôpital dans le cadre de l'exploitation d'un garage à étages serait probablement assujettie à la *Loi*, car cela ne serait pas considéré comme une activité essentielle.

Un café-restaurant dans un hôpital ou une université, un service de location de téléviseurs dans un hôpital, une librairie dans une université ou toute autre activité commerciale exercée par un tiers au sein d'un de ces établissements seraient assujettis à la *Loi*, tout comme le serait un café-restaurant dans un centre commercial, à moins qu'une loi essentiellement similaire à la loi fédérale ne s'applique.

La situation des établissements d'enseignement et des hôpitaux privés est différente. En général, plusieurs de ces établissements sont davantage engagés dans des activités commerciales et nous recommanderions qu'ils fonctionnent selon l'hypothèse de leur assujettissement à la LPRPDE, à moins qu'une loi provinciale réputée être essentiellement similaire ne s'applique.

Le secteur des soins de santé

Les activités essentielles des hôpitaux publics ou des établissements de soins prolongés financés par l'État ne sont pas assujetties à la LPRPDE. Cependant, les fournisseurs de soins de santé en cabinet privé comme les médecins, les dentistes et les chiropraticiens exercent une activité commerciale et sont donc assujettis à la *Loi*, à moins qu'une loi provinciale réputée être essentiellement similaire ne s'applique. Pour obtenir des renseignements additionnels sur l'application de la LPRPDE au secteur des soins de santé, prière de consulter le site suivant : **http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/h_gv00207f.html**. L'Alberta, la Saskatchewan, le Manitoba et l'Ontario ont adopté des lois surles renseignements personnels sur la santé qui s'appliquent au secteur des soins de santé, y compris aux hôpitaux. La *Loi sur les services de santé et les services sociaux* du Québec comporte aussi des dispositions importantes concernant les renseignements personnels sur la santé.

Les lois provinciales

Dans plusieurs provinces, les renseignements personnels recueillis par les municipalités, les universités, les écoles et les hôpitaux sont protégés par les lois provinciales. Habituellement, il s'agit d'une loi sur le secteur public, souvent une loi sur l'accès à l'information et la protection des renseignements personnels. Dans certains cas, des lois sur la protection des renseignements personnels sur la santé et des lois sur le secteur privé peuvent aussi s'appliquer. Pour de plus amples renseignements sur les lois provinciales applicables, consulter le site suivant : **http://www.privcom.gc.ca/prov/index_f.asp**.

Les territoires

La situation dans les trois territoires est un peu plus complexe. La LPRPDE s'applique aux entreprises fédérales et aux renseignements personnels de leurs employés. Une entreprise fédérale est une installation, un ouvrage, une entreprise ou un secteur d'activité qui relève de la compétence législative du Parlement.

Comme toutes les organisations des territoires sont considérées comme des entreprises fédérales, la LPRPDE s'applique aux renseignements relatifs aux employés des municipalités, des universités, des écoles et des hôpitaux dans les territoires.

Toutefois, la LPRPDE ne s'applique pas aux renseignements sur les patients ou les élèves des écoles ou des hôpitaux publics dans les territoires, car ces établissements n'exercent pas d'activité commerciale.

ANNEXE B

AUTOÉVALUATION DE LA PROTECTION DE LA VIE PRIVÉE

Qu'est-ce que l'autoévaluation de la protection de la vie privée?

Selon le CPVP, l'autoévaluation de la protection de la vie privée est un processus qui permet à une organisation d'amorcer une évaluation afin de mettre à l'essai ses propres systèmes et pratiques de protection de la vie privée et de les améliorer. L'autoévaluation comprend l'évaluation de l'organisation en fonction d'un ensemble de critères établis afin de déterminer le degré de conformité de l'organisation à ces critères. L'évaluation de la conformité permet de relever les lacunes et les risques pour prendre les bonnes mesures correctives et en assurer le suivi.

Une organisation peut procéder à de telles évaluations de trois façons différentes :

1. L'unité fonctionnelle analyse et évalue son propre degré de conformité avec les normes de protection de la vie privée. On appelle communément cette façon de faire « autoévaluation », car ce sont les chefs de l'exploitation qui s'en chargent. L'autoévaluation peut être faite avec l'aide d'un facilitateur;

2. Une autre partie de l'organisation, indépendante de l'unité fonctionnelle faisant l'objet de l'examen, est sollicitée pour évaluer la conformité de l'organisation avec les normes (par exemple, un vérificateur interne). Il est possible de combiner ces deux premières façons de faire;

3. Une tierce partie externe procède à une évaluation indépendante (par exemple, un vérificateur externe).

Une organisation peut en outre adopter différentes approches tant en matière de portée que de fréquence d'évaluation. Peu importe l'approche adoptée, nous conseillons de planifier une autoévaluation continue et régulière. Les approches consistent à :

- effectuer une seule évaluation dans l'ensemble de l'organisation à un moment donné. Cette approche peut s'avérer des plus efficaces si votre organisation est relativement petite;
- créer un échéancier selon lequel les unités fonctionnelles les plus à risque sont évaluées en priorité (par exemple, évaluer d'abord les unités qui recueillent, conservent et traitent un grand volume de renseignements financiers ou médicaux);
- d'abord effectuer un projet pilote auprès d'une petite unité afin de valider et, au besoin, adapter l'approche avant d'évaluer les unités plus importantes et plus à risque.

Avantages de l'autoévaluation

Selon le CPVP, les organisations devraient se montrer proactives quant à leur conformité aux lois sur la protection des renseignements personnels. Entre autres caractéristiques (comme une politique sur la protection de la vie privée), l'autoévaluation reflète une culture responsable de gestion de la protection de la vie privée au sein d'une organisation. Finalement, la saine gestion d'une organisation en matière de cycle de vie des renseignements personnels est intimement liée à sa réputation, à sa marque, à ses relations d'affaires, à sa responsabilité juridique, à la fidélité de ses clients et à sa croissance. Procéder à une autoévaluation est dans l'intérêt de toute organisation.

Il est important de se rappeler qu'un outil d'autoévaluation devrait être appliqué dans le cadre d'un programme de protection de la vie privée bien structuré. Les autoévaluations effectuées régulièrement constituent de précieux outils qui permettent à une organisation de faire face à des facteurs de changement de leur environnement, facteurs qui peuvent l'empêcher d'atteindre les objectifs définis.

Au cours de ses recherches pour la rédaction de ce guide, le CPVP a appris l'existence de certains outils d'évaluation et de gestion du risque en matière de protection de la vie privée utilisés dans certaines organisations comme IBM Canada et la Commission de la sécurité professionnelle et de l'assurance contre les accidents du travail. Il existe des modèles d'outils, et l'autoévaluation est bel et bien possible. Plus important encore, l'existence de ces modèles indique que l'autoévaluation est une façon constructive de changer les comportements et d'accroître la conscientisation en matière de protection de la vie privée. En outre, ils peuvent présenter un avantage pour l'entreprise sur le plan du diagnostic des processus administratifs. L'autoévaluation permet également de répartir les responsabilités en matière de protection de la vie privée et peut mettre en valeur le rôle du responsable de la protection de la vie privée.

Préparation d'une autoévaluation

Cet exercice de conformité permet non seulement de s'assurer que des mesures de contrôle en matière de protection ont été mises au point, mais également de recueillir des preuves de leur mise en œuvre. Par exemple, pour vérifier la mise en œuvre réussie d'une politique selon laquelle le consentement explicite est nécessaire pour recueillir des renseignements personnels, une preuve de l'obtention de ce consentement devrait être recueillie auprès d'un échantillon. Plus nombreuses sont les preuves de la conformité de votre organisation, plus vous serez en mesure de relever et d'évaluer les risques liés à la protection de la vie privée.

Les évaluations doivent être planifiées soigneusement pour être efficaces. Il faut y investir du temps et des ressources. Plus important encore, l'organisation doit être prête à donner suite aux résultats d'évaluation et à investir dans les mesures appropriées pour éliminer les risques inacceptables et renforcer sa capacité de gestion de la protection de la vie privée. L'autoévaluation est inutile si les lacunes (faiblesses) relevées ne font pas l'objet d'un plan d'action de gestion dont la direction fait le suivi.

Quelques activités préparatoires sont nécessaires avant de commencer l'exercice d'autoévaluation. Toutes ces activités, en soi, contribueront à réduire le nombre de lacunes sur le plan de l'information pendant l'évaluation. Ces activités comprennent l'élaboration d'un plan d'évaluation, l'inventaire des renseignements personnels, et l'inventaire et l'examen des politiques et des procédures.

Élaboration d'un plan d'évaluation

Élaborez un plan qui décrit les secteurs à évaluer dans l'entreprise, les services offerts par ces secteurs, les principes en fonction desquels ils seront évalués et l'échéancier d'évaluation. Pour chaque secteur, déterminez si vous voulez évaluer ce qui suit :

- « conception réussie » des mesures de contrôle en matière de protection de la vie privée, pour savoir si elles sont conçues pour atteindre les objectifs définis;
- « mise en œuvre réussie », pour savoir si ces mesures ont été mises en œuvre comme elles le devraient;
- « fonctionnalité réussie », pour savoir si ces mesures ont été mises en œuvre et si elles sont fonctionnelles pendant une période déterminée.

Afin de vérifier si la conception d'une mesure de contrôle en matière de protection de la vie privée est réussie, vous devez connaître le besoin pour lequel la mesure a été conçue. Par exemple, si une politique générale de protection de la vie privée doit décrire l'engagement de l'organisation à se conformer aux dix principes de la LPRPDE, cette politique devrait être évaluée afin de déterminer si elle répond à ce besoin. Si elle y répond effectivement, c'est qu'elle a été conçue correctement. Pour savoir si la mise en œuvre d'une mesure est réussie, l'organisation doit d'abord connaître l'objectif visé par la mesure. Si les mesures concernant une application en matière de contrôle d'accès sécuritaire automatisé ont été conçues pour limiter la communication de renseignements personnels, vous devrez peut-être faire quelques tests pour déterminer si l'accès aux renseignements personnels est exclusivement réservé aux personnes qui en ont besoin.

Si le plan d'évaluation comporte l'évaluation de tous ces aspects de votre politique, de vos procédures, de vos processus et de vos structures de gouvernance de protection de la vie privée, prévoyez y consacrer assez de temps, selon le volume des documents à examiner et à analyser.

Inventaire des renseignements personnels

Un inventaire général doit être effectué par chaque secteur de l'entreprise qui participera à l'exercice d'évaluation. Utilisez un tableau ou un chiffrier pour dresser l'inventaire des renseignements personnels de votre organisation, en fonction de leur nature et de l'endroit où ils sont conservés. Prenons par exemple un inventaire auquel figurent le nom d'une application (par exemple, PeopleSoft) et les documents papier ou les fichiers électroniques liés à l'application (par exemple, les fichiers de dotation en ressources humaines, les fichiers de la paie et des avantages sociaux, les fichiers d'évaluation). L'inventaire doit comprendre, de manière plus générale, la nature des renseignements personnels (par exemple, renseignements médicaux, financiers, sur les ressources humaines) et la façon dont ils sont recueillis, utilisés, communiqués, conservés, retirés ou archivés.

Selon le nombre de processus administratifs et de systèmes d'information de votre organisation qui sont nécessaires à la collecte, à l'utilisation ou à la communication des renseignements personnels, cette tâche peut se révéler de taille. Un projet pilote de plus petite envergure peut être plus facile à réaliser dans ces situations. Une autre façon de connaître les renseignements personnels détenus par une organisation est de tracer des diagrammes des processus administratifs pour les principales activités organisationnelles évaluées, qui indiqueraient la circulation générale des renseignements personnels tout au long de leur cycle de vie.

Bien qu'il s'agisse d'une tâche importante à des fins de protection de la vie privée, elle est également précieuse pour la sécurité et les activités de l'organisation. En effet, un contrôle collectif de la nature des renseignements personnels recueillis, des raisons de les obtenir, de les conserver, de les transmettre, de les utiliser et de les retirer, ainsi que de la façon de le faire, répond souvent à un besoin crucial pour l'entreprise. Les renseignements personnels font partie des actifs d'une entreprise, et bien souvent, ce sont des actifs déterminants.

Pour dresser un inventaire efficace des renseignements personnels, utilisez les questions suivantes à titre de guide :

- Qu'entend la LPRPDE par « renseignements personnels » et comment cette définition s'applique-t-elle dans le contexte de votre organisation?
- Quelle est la nature des renseignements personnels que votre organisation recueille?
- De quelles façons votre organisation recueille-t-elle des renseignements personnels et dans quelles circonstances?
- Pour quelles raisons votre organisation recueille-t-elle des renseignements personnels?
- Quelles personnes de l'organisation utilisent les renseignements personnels?
- Quelles personnes ont accès aux renseignements personnels?
- Où votre organisation conserve-t-elle les renseignements personnels?

- Dans quels formats les renseignements personnels sont-ils conservés (par exemple, fichiers électroniques, documents papier, bandes sonores)?
- De quelle façon les renseignements personnels sont-ils protégés?
- Quels renseignements personnels votre organisation communique-t-elle à d'autres organisations? Pour quelles raisons?
- À quelles autres organisations votre organisation communique-t-elle des renseignements personnels? De quelles façons?
- Pendant combien de temps votre organisation conserve-t-elle les renseignements personnels?
- Pendant combien de temps votre organisation doit-elle conserver les renseignements personnels?
- Quand et comment votre organisation retire-t-elle les renseignements personnels qu'elle détient?

Remarque : L'utilisation du terme « raisonnable » dans la LPRPDE signifie que les renseignements personnels sont utilisés « à des fins qu'une personne raisonnable estimerait acceptables ».

Inventaire des politiques et des procédures

Dressez une liste des politiques et des procédures pertinentes à la gestion des renseignements personnels. Il s'agit des politiques et des procédures de protection de la vie privée, mais aussi des politiques et des procédures de sécurité, de gestions des dossiers et des renseignements, de gestion des données et de confidentialité. Vous pouvez distinguer les politiques et procédures qui s'appliquent à l'ensemble de l'organisation de celles qui sont propres au processus de l'unité fonctionnelle ou au processus administratif.

Il existe de nombreuses façons de mettre en œuvre un processus d'autoévaluation. Selon la portée de l'évaluation, le plan peut être appliqué à l'aide :

- d'une structure de comité d'évaluation de la conformité en matière de protection de la vie privée. Compte tenu de la nature complexe du concept de la vie privée et de ses multiples facettes, un comité peut être nécessaire pour veiller à ce que les enjeux en matière de protection de la vie privée soient analysés en profondeur. Par exemple, les membres du comité pourraient représenter les différentes unités fonctionnelles de l'organisation, comme les technologies de l'information, les services juridiques et les communications ou le marketing;
- d'un facilitateur principal qui soutient les équipes chargées de l'évaluation des unités fonctionnelles;
- d'un directeur du projet d'évaluation de la conformité aux normes de protection de la vie privée et d'une équipe permanente chargée de l'évaluation de la conformité.

Une fois l'étape de planification terminée, il est important de vérifier le plan avec la direction. Le soutien continu et tangible de la direction est un facteur de réussite essentiel de l'évaluation. Un plan de communication qui indique la façon dont les résultats de chaque évaluation seront vérifiés avec l'unité fonctionnelle, la façon dont le rapport global sera présenté et les principaux messages à communiquer au cours du projet devrait également être mis sur pied.

ANNEXE C

AUTRES DIRECTIVES DISPONIBLES AUPRÈS DU CPVP

Cet outil d'autoévaluation a principalement été conçu pour les moyennes et les grandes organisations. Le CPVP a conçu un outil d'apprentissage en ligne qui pourrait être utile aux petits commerces de détail. Ces outils sont accessibles sur le site Web du CPVP, à l'adresse **http://www.privcom.gc.ca/**.

Voici des directives et des fiches d'information qui pourraient vous être utiles et qui accompagnent l'outil d'autoévaluation :

- Cadre de conformité à la LPRPDE du CPVP
- Lignes directrices en cas d'atteintes à la vie privée
- Questions et réponses concernant l'application de la LPRPDE
- Détermination de la forme de consentement appropriée aux termes de la LPRPDE
- Télécopieurs et renseignements personnels
- Pratiques exemplaires relatives au traitement des renseignements personnels avant l'entrée en vigueur de la LPRPDE (respect des droits acquis)
- Pratiques exemplaires pour l'utilisation des numéros d'assurance sociale dans le secteur privé
- Lignes directrices sur l'enregistrement des appels téléphoniques des clients
- Guide à l'intention des organisations au regard des enquêtes sur les plaintes aux termes de la LPRPDE
- Application de la LPRPDE aux œuvres de charité et aux organismes sans but lucratif
- Application de la LPRPDE aux dossiers du personnel
- La protection des renseignements personnels au travail
- Se conformer à la LPRPDE
- Questionnaire sur la protection des renseignements personnels
- Un aperçu de la LPRPDE à l'intention des entreprises et des organismes
- LPRPDE pour les organisations du secteur de la santé

Vous pouvez également vous reporter aux enquêtes sur des plaintes publiées par le CPVP dans ses rapports annuels ou à l'adresse **http://www.privcom.gc.ca/**.