

Principes généralement reconnus en matière de protection des renseignements personnels

**Version destinée aux praticiens
CA ou CPA**

Août 2009



Protection des renseignements personnels



Remerciements :

L'AICPA et l'Institut Canadien des Comptables Agréés (ICCA) tiennent à souligner la contribution des bénévoles qui ont consacré beaucoup de temps et d'efforts à ce projet. Ils remercient également les organisations suivantes pour leur appui à l'égard de l'élaboration des principes généralement reconnus en matière de protection des renseignements personnels :

Information Systems Audit and Control
Association



The Institute of Internal Auditors



Avis au lecteur

La présente version destinée aux praticiens CA ou CPA est identique au document «Principes généralement reconnus en matière de protection des renseignements personnels», à l'exception de l'Annexe B, «Services de praticiens CA ou CPA fondés sur les principes généralement reconnus en matière de protection des renseignements personnels», et de l'Annexe C, «Modèles de rapports du vérificateur portant sur la protection des renseignements personnels». Ces annexes additionnelles visent principalement à aider les CPA et les CA en cabinet dans la prestation à leurs clients de services liés à la protection des renseignements personnels. La présente version s'applique à compter du 30 octobre 2009.

Copyright L'Institut Canadien des Comptables Agréés et l'American Institute of Certified Public Accountants, Inc., 2009.

Tous droits réservés. Les listes de contrôle et les modèles de documents peuvent être reproduits et distribués dans le cadre des services professionnels ou de la pratique professionnelle, pourvu que les documents reproduits ne soient d'aucune façon mis en vente directement. Pour obtenir des renseignements sur la procédure permettant d'obtenir la permission de faire des copies du présent document, en tout ou partie, veuillez visiter www.copyright.com ou composer le (978) 750-8400.

Avant-propos

L'Institut Canadien des Comptables Agréés (ICCA) et l'AICPA sont fermement convaincus de l'importance de la protection des renseignements personnels pour l'entreprise. En examinant les défis auxquels les organisations font face en matière de protection des renseignements personnels, nous avons rapidement constaté qu'elles n'avaient pas accès à un cadre de référence exhaustif pour gérer efficacement les risques qu'elles courent à cet égard. L'ICCA et l'AICPA ont déterminé qu'ils pourraient faire une différence importante en élaborant un cadre pour la protection des renseignements personnels qui répondrait aux besoins de toutes les parties concernées par les exigences ou les attentes en la matière. Le résultat a été un cadre nommé «Principes généralement reconnus en matière de protection des renseignements personnels». L'ICCA et l'AICPA assurent la diffusion la plus large possible de ces principes et critères à toutes les parties intéressées par la protection des renseignements personnels.

Ces principes et critères ont été élaborés et mis à jour par des bénévoles qui ont pris en compte la réglementation actuelle et les meilleures pratiques à l'échelle internationale en matière de protection des renseignements personnels. Ils ont été publiés suivant la procédure officielle de l'ICCA et de l'AICPA, qui comprend la publication pour commentaires. L'adoption de ces principes et critères est facultative.

Ces principes reposent sur le postulat qu'une protection des renseignements personnels efficace est bonne pour les affaires. L'existence de bonnes pratiques en la matière est un élément essentiel de la gouvernance d'entreprise et de la reddition de comptes. Aujourd'hui, la protection du caractère confidentiel des renseignements personnels qu'elles recueillent et conservent constitue un impératif pour les organisations. Les systèmes et les processus des entreprises gagnant en complexité et devenant de plus en plus perfectionnés, celles-ci recueillent toujours davantage de renseignements personnels. Étant donné la quantité croissante de données recueillies et conservées, le plus souvent sur support électronique, les renseignements personnels sont exposés à des risques divers : perte, utilisation abusive, accès non autorisé et communication non autorisée. Ces risques inquiètent les organisations, les gouvernements, les particuliers et le public en général.

Pour les organisations exerçant des activités dans plusieurs ressorts territoriaux, la gestion du risque lié à la protection des renseignements personnels peut poser un défi plus grand encore. L'observation des principes généralement reconnus en matière de protection des renseignements personnels ne garantit pas aux organisations qu'elles sont en conformité avec l'ensemble des textes légaux et réglementaires auxquels elles sont soumises. Elles doivent connaître les

principales exigences en la matière dans tous les ressorts territoriaux où elles font des affaires. Bien que le présent cadre de référence fournisse des lignes directrices sur la protection des renseignements personnels en général, les organisations devraient consulter leur propre conseiller juridique au sujet des textes légaux et réglementaires visant leur situation particulière.

Dans cette optique, l'ICCA et l'AICPA ont élaboré les principes généralement reconnus en matière de protection des renseignements personnels sous la forme d'un cadre d'exploitation destiné à aider la direction des organisations à gérer la protection des renseignements personnels en fonction des nombreuses exigences locales, nationales et internationales. L'objectif premier consiste à faciliter la conformité aux exigences et la gestion efficace dans ce domaine. Le second objectif est d'établir des critères valables permettant d'exécuter une mission d'attestation (habituellement appelée vérification) relative à la protection des renseignements personnels.

Les principes généralement reconnus en matière de protection des renseignements personnels, qui tiennent compte des besoins des organisations et de l'intérêt public, constituent l'apport de l'ICCA et de l'AICPA en vue d'aider les organisations à effectuer une gestion efficace du risque dans ce domaine. On trouvera d'autres informations sur l'élaboration des principes ainsi que des ressources additionnelles en ligne sur les sites Internet de l'[ICCA](http://www.icca.ca) et de l'[AICPA](http://www.aicpa.org) (www.icca.ca/prp et www.aicpa.org/privacy). Il est également possible d'y télécharger le document *Principes généralement reconnus en matière de protection des renseignements personnels*.

Comme le contexte de la protection des renseignements personnels est en constante mutation, il faut réviser de temps en temps les principes généralement reconnus en la matière. Nous vous saurions donc gré d'envoyer vos commentaires sur le présent document à l'ICCA (privacy@cica.ca) ou à l'AICPA (GAPP@aicpa.org).

AICPA

ICCA

Groupe de travail mixte AICPA – ICCA sur la protection des renseignements personnels

<p><u>Président</u> Everett C. Johnson, CPA <i>Deloitte & Touche LLP</i> <i>(retraité)</i></p> <p><u>Vice-président</u> Kenneth D. Askelson, CPA, CITP, CIA <i>JCPenney (retraité)</i></p> <p>Eric Federling <i>KPMG LLP</i></p> <p>Philip M. Juravel, CPA <i>Juravel & Company, LLC</i></p> <p>Sagi Leizerov, Ph.D., CIPP <i>Ernst & Young LLP</i></p> <p>Rena Mears, CPA, CITP, CISSP, CISA, CIPP <i>Deloitte & Touche LLP</i></p> <p>Robert Parker, FCA, CA.CISA, CMC <i>Deloitte & Touche LLP</i> <i>(retraité)</i></p> <p>Marilyn Prosch, Ph.D., CIPP <i>Arizona State University</i></p> <p>Doron M. Rotman, CPA (Israël), CISA, CIA, CISM, CIPP <i>KPMG LLP</i></p> <p>Kerry Shackelford, CPA <i>KLS Consulting LLC</i></p> <p>Donald E. Sheehy, CA•CISA, CIPP/C <i>Deloitte & Touche LLP</i></p>	<p><u>Permanents :</u></p> <p>Nicholas F. Cheung, CA, CIPP/C ICCA <i>Directeur de projets, Nouveaux services de certification</i></p> <p>Bryan Walker, CA ICCA <i>Directeur, Soutien aux praticiens</i></p> <p>Nancy A. Cohen, CPA, CITP, CIPP, AICPA <i>Senior Technical Manager, Specialized Communities and Practice Management</i></p> <p>James C. Metzler, CPA, CITP, AICPA <i>Vice President, Small Firms Interests</i></p> <p><i>L'Assurance Services Executive Committee de l'AICPA a approuvé les Principes généralement reconnus en matière de protection des renseignements personnels en août 2009.</i></p>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Table des matières

INTRODUCTION AUX PRINCIPES GÉNÉRALEMENT RECONNUS EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS	1
INTRODUCTION	1
<i>Importance de la protection des renseignements personnels pour l'entreprise</i>	2
QUESTIONS TOUCHANT LA PROTECTION DES RENSEIGNEMENTS PERSONNELS À L'ÉCHELLE INTERNATIONALE	3
<i>Externalisation et protection des renseignements personnels</i>	4
EN QUOI CONSISTE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS?	4
<i>Définition de la protection des renseignements personnels</i>	4
<i>Renseignements personnels</i>	5
<i>Protection des renseignements personnels ou confidentialité?</i>	6
PRINCIPES GÉNÉRALEMENT RECONNUS EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS – MISE EN CONTEXTE	7
OBJECTIF GÉNÉRAL DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS	7
PRINCIPES GÉNÉRALEMENT RECONNUS EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS	8
<i>Application des PPRP</i>	9
<i>Présentation des principes généralement reconnus et des critères en matière de protection des renseignements personnels</i>	13
PRINCIPES GÉNÉRALEMENT RECONNUS ET CRITÈRES EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS	14
GESTION	14
AVIS.....	27
CHOIX ET CONSENTEMENT	31
COLLECTE.....	36
UTILISATION, CONSERVATION ET SUPPRESSION	40
ACCÈS.....	44
COMMUNICATION À DES TIERS.....	50
SÉCURITÉ.....	55
QUALITÉ	66
SUIVI ET APPLICATION	69
ANNEXE A – GLOSSAIRE	76
ANNEXE B – SERVICES DE PRATICIENS CA OU CPA FONDÉS SUR LES PRINCIPES GÉNÉRALEMENT RECONNUS EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS	78
MISSIONS DE CONSEIL RELATIVES À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS	78
MISSIONS D'ATTESTATION ET DE CERTIFICATION RELATIVES À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS	78
<i>Missions de vérification relatives à la protection des renseignements personnels</i>	79
<i>Missions d'examen de la protection des renseignements personnels</i>	81
<i>Missions d'application de procédés de vérification spécifiés</i>	82
LIENS ENTRE LES PRINCIPES GÉNÉRALEMENT RECONNUS EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LES PRINCIPES ET CRITÈRES DES SERVICES TRUST	83
ANNEXE C – MODÈLES DE RAPPORTS DU VÉRIFICATEUR PORTANT SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS	85
MODÈLE N ^o 1 – RAPPORT SUR L'ASSERTION DE LA DIRECTION, ÉTABLI SELON LES NORMES D'ATTESTATION DE L'AICPA	86
EXEMPLE D'ASSERTION DE LA DIRECTION EN RAPPORT AVEC LE MODÈLE N ^o 1	88
MODÈLE N ^o 2 – RAPPORT PORTANT DIRECTEMENT SUR LES ÉLÉMENTS CONSIDÉRÉS, ÉTABLI SELON LES NORMES D'ATTESTATION DE L'AICPA	89
MODÈLE N ^o 3 – RAPPORT SUR L'ASSERTION DE LA DIRECTION, ÉTABLI SELON LES NORMES DE CERTIFICATION DE L'ICCA.....	91
EXEMPLE D'ASSERTION DE LA DIRECTION EN RAPPORT AVEC LE MODÈLE N ^o 3	93
MODÈLE N ^o 4 – RAPPORT PORTANT DIRECTEMENT SUR LES ÉLÉMENTS CONSIDÉRÉS, ÉTABLI SELON LES NORMES DE CERTIFICATION DE L'ICCA.....	94

Introduction aux principes généralement reconnus en matière de protection des renseignements personnels

Introduction

Pour nombre d'organisations, la gestion de la protection des renseignements personnels¹ au niveau local, national ou international comporte des défis. La plupart d'entre elles doivent mettre en application des lois et règlements variés en la matière.

Les principes généralement reconnus en matière de protection des renseignements personnels (PPRP) ont été élaborés selon le point de vue des entreprises, en fonction d'un certain nombre, mais en aucun cas de la totalité, des textes réglementaires importants en la matière à l'échelle locale, nationale et internationale. Les PRRP permettent de traduire des exigences complexes en un objectif unique de protection des renseignements personnels soutenu par dix principes. Chaque principe est étayé par des critères objectifs et mesurables qui constituent le fondement d'une gestion efficace des risques et de la conformité en matière de protection des renseignements personnels au sein d'une organisation. Des exemples ayant trait aux exigences, aux communications et aux contrôles, y compris à la surveillance des contrôles, sont fournis à l'appui des critères.

Toute organisation peut utiliser les PRRP dans le cadre de son programme de protection des renseignements personnels. Ces principes visent à permettre à la direction de mettre au point un programme efficace en la matière, qui prenne en compte les risques et les obligations rattachés à la protection des renseignements personnels ainsi que les occasions d'affaires. Ils peuvent également être utiles aux conseils d'administration et aux autres instances chargées de la gouvernance et exerçant une fonction de surveillance. L'introduction comporte une définition de la protection des renseignements personnels et une explication de l'importance que revêt cette question – qui ne se limite pas à la conformité – pour les entreprises. On y explique aussi comment les principes peuvent s'appliquer aux situations d'externalisation, et on présente les types d'initiatives pouvant être avantageuses pour les organisations et leurs clients.

¹ La première occurrence de chaque terme défini dans le Glossaire (Annexe A) est soulignée et reliée par hyperlien à sa définition dans le glossaire de la section d'introduction et dans les tableaux des principes généralement reconnus et des critères en matière de protection des renseignements personnels.

L'introduction ainsi que les principes de protection des renseignements personnels et les critères y afférents qui la suivent seront utiles aux personnes qui :

- assurent la surveillance et le suivi des programmes de protection des renseignements personnels et de sécurité;
- mettent en œuvre et gèrent les mesures de protection des renseignements personnels dans l'organisation;
- mettent en œuvre et gèrent les mesures de sécurité dans l'organisation;
- surveillent et gèrent les risques et la conformité dans l'organisation;
- évaluent la conformité et exécutent la vérification des programmes de protection des renseignements personnels et de sécurité;
- réglementent la protection des renseignements personnels.

Importance de la protection des renseignements personnels pour l'entreprise

Une protection des renseignements personnels efficace est bonne pour les affaires. L'existence de bonnes pratiques en la matière est un élément essentiel de la gouvernance d'entreprise et de la reddition de comptes. Aujourd'hui, la protection du caractère privé des renseignements personnels constitue un impératif pour les entreprises. Les systèmes et les processus des organisations gagnant en complexité et devenant de plus en plus perfectionnés, celles-ci recueillent toujours davantage de renseignements personnels. Des risques divers peuvent alors se poser quant à la protection de ces renseignements : perte, utilisation abusive, accès non autorisé et communication non autorisée. Ces risques suscitent des préoccupations pour les organisations, les gouvernements et le public en général.

Les organisations s'efforcent de parvenir à un juste équilibre entre la collecte adéquate de renseignements personnels concernant leurs clients et l'utilisation de ces renseignements. Les gouvernements, quant à eux, essaient de protéger l'intérêt public, tout en gérant leur propre stock de renseignements personnels recueillis auprès des citoyens. Les consommateurs ont de grandes inquiétudes à l'égard des renseignements personnels recueillis à leur sujet, et nombre d'entre eux estiment en avoir perdu la maîtrise. Qui plus est, le public s'inquiète considérablement des risques d'usurpation d'identité et d'accès abusif à des renseignements personnels, particulièrement aux dossiers financiers ou médicaux et aux renseignements sur les enfants.

Les individus s'attendent à ce que leur vie privée soit respectée et à ce que les organisations avec lesquelles ils font affaire protègent les renseignements personnels recueillis à leur sujet. Ils ne sont plus disposés à fermer les yeux lorsqu'une organisation n'a pas rempli ses obligations à ce chapitre. Dans la pratique, *toutes* les entreprises doivent donc traiter la protection des renseignements personnels comme un enjeu de la gestion des risques. Voici des risques précis découlant de politiques et procédures inadéquates en la matière :

dommages à la réputation de l'organisation, à sa marque ou à ses relations d'affaires;
responsabilité légale et sanctions infligées par le secteur d'activité ou les autorités de réglementation;
accusations de pratiques commerciales trompeuses;
perte de la confiance des clients ou des employés;
refus des individus de consentir à l'utilisation à des fins commerciales des renseignements personnels recueillis à leur sujet;
perte de clientèle ou de commandes et, partant, réduction des produits d'exploitation et de la part de marché;
perturbation des activités internationales de l'entreprise;
engagement de responsabilité à la suite d'un vol d'identité.

Questions touchant la protection des renseignements personnels à l'échelle internationale

Pour les organisations actives dans plusieurs pays, la gestion du risque lié à la protection des renseignements personnels peut poser de grands défis.

Par exemple, l'envergure mondiale d'Internet et des échanges commerciaux signifie que des mesures réglementaires prises dans un pays peuvent avoir une incidence sur les droits et obligations des utilisateurs et des consommateurs individuels partout dans le monde. De nombreux pays ont réglementé la circulation transfrontalière des données. Citons notamment les directives de l'Union européenne (UE) sur la protection des données et la protection des renseignements personnels, que les organisations doivent respecter pour pouvoir faire des affaires avec les pays membres de l'UE. Les organisations doivent donc se conformer à des exigences variables en matière de protection des renseignements personnels partout dans le monde. En outre, les philosophies à ce sujet diffèrent d'un pays à l'autre, ce qui rend la conformité à l'échelle internationale encore plus complexe. Par exemple, certains pays considèrent que les renseignements personnels appartiennent à la personne qu'ils concernent et que les entreprises ont une relation de type fiduciaire avec les gens lorsqu'elles recueillent et conservent de tels renseignements. À l'opposé, d'autres pays estiment que les renseignements personnels sont la propriété de l'entreprise qui les recueille.

Par ailleurs, les organisations sont mises au défi de demeurer au fait des plus récentes exigences de tous les pays où elles font affaire. L'adoption de normes mondiales rigoureuses comme celles dont fait état le présent document facilitera le respect des nombreux règlements en vigueur.

Même les organisations ayant une visibilité internationale limitée sont souvent confrontées à des questions de conformité aux normes de protection des

renseignements personnels dans d'autres pays. Bon nombre de ces organisations ne savent pas comment tenir compte de la réglementation étrangère souvent plus stricte. Cela accroît le risque qu'une organisation puisse commettre par inadvertance une infraction qui défraiera ensuite la chronique dans le pays hôte concerné.

Qui plus est, nombre d'instances locales (comme des États ou des provinces) et certains secteurs d'activité, comme la santé ou le secteur bancaire, ont des exigences particulières en matière de protection des renseignements personnels.

Externalisation et protection des renseignements personnels

L'externalisation accroît la complexité de la protection des renseignements personnels. Une organisation peut externaliser une partie de ses processus d'affaires et, de ce fait, un certain degré de responsabilité en matière de protection des renseignements personnels. Cependant, elle ne peut externaliser sa responsabilité ultime à l'égard de la protection des renseignements personnels inhérents à ses processus d'affaires. La complexité augmente lorsque les services externalisés sont confiés à une entité d'un autre pays qui peut être assujettie à une réglementation différente en la matière, s'il en est. Dans une telle situation, l'organisation qui externalise un processus doit s'assurer que la gestion de ses responsabilités en matière de protection des renseignements personnels est adéquate.

Les PPRP et leurs critères connexes peuvent aider les organisations à effectuer des évaluations (y compris des examens indépendants) ayant trait aux politiques, aux procédures et aux pratiques relatives à la protection des renseignements personnels de l'entité tierce fournissant les services externalisés.

L'application de ces principes et de ces critères à l'échelle mondiale peut rassurer les organisations qui externalisent quant au fait que les évaluations ayant trait à la protection des renseignements personnels peuvent être effectuées à l'aide d'une mesure uniforme fondée sur des pratiques loyales en matière d'information et reconnues à l'échelle internationale.

En quoi consiste la protection des renseignements personnels?

Définition de la protection des renseignements personnels

La protection des renseignements personnels correspond, selon la définition des principes généralement reconnus en la matière, aux «droits et obligations des individus et des organisations en ce qui concerne la collecte, l'utilisation, la conservation, la communication et la destruction des renseignements personnels».

Renseignements personnels

Les *renseignements personnels* (parfois appelés «renseignements personnalisés») concernent ou sont susceptibles de concerner un [individu](#) identifiable, ou sont reliés ou susceptibles d'être reliés à un individu identifiable. «Individu» s'entend, en l'occurrence, des clients et des salariés, passés, actuels ou pressentis ainsi que des autres personnes avec qui l'entité est en relation. Le terme «renseignements personnels» vise notamment tout renseignement pouvant être relié à un individu, ou pouvant être utilisé pour identifier directement ou indirectement un individu. La plupart des renseignements recueillis par une organisation au sujet d'un individu seront vraisemblablement considérés comme des renseignements personnels s'ils peuvent être attribués à un individu identifié. Voici des exemples de renseignements personnels :

- nom;
- adresse du domicile ou de courriel;
- numéro d'identification (le numéro d'assurance sociale ou de sécurité sociale, par exemple);
- caractéristiques physiques;
- historique des achats d'un consommateur.

Certains renseignements personnels sont considérés comme *sensibles*. Certains textes légaux et réglementaires précisent que les renseignements suivants constituent des [renseignements personnels sensibles](#) :

- renseignements sur l'état de santé;
- renseignements de nature financière;
- origine raciale ou ethnique;
- opinions politiques;
- convictions religieuses ou philosophiques;
- appartenance à un syndicat;
- préférences sexuelles;
- renseignements ayant trait à des infractions ou à des condamnations criminelles.

Les renseignements personnels sensibles commandent en général un degré de protection plus élevé et une obligation de diligence plus grande. Par exemple, il peut arriver que certains ressorts territoriaux exigent un consentement explicite plutôt qu'implicite préalablement à la collecte ou à l'utilisation d'informations sensibles.

Certains renseignements concernant des gens ne peuvent être associés à des individus en particulier. On les qualifie de *renseignements non personnels*. Il s'agit notamment de données statistiques ou de sommaires de renseignements personnels, à l'égard desquels soit l'identité de l'individu est inconnue, soit on a

supprimé le couplage avec l'individu. Dans de tels cas, il est impossible de déterminer l'identité de l'individu à partir des renseignements qui restent, puisque ceux-ci ont été dépersonnalisés ou désidentifiés. Les renseignements non personnels ne font habituellement pas l'objet d'une protection, parce qu'ils ne peuvent être reliés à un individu. Néanmoins, il peut arriver que certaines organisations aient tout de même des obligations au sujet de renseignements non personnels en raison d'autres textes réglementaires ou contractuels (par exemple, dans le cas de recherches cliniques ou d'études de marché).

Protection des renseignements personnels ou confidentialité?

Contrairement aux renseignements personnels, qui sont souvent définis dans les textes légaux ou réglementaires, il n'existe aucune définition unique et largement reconnue des renseignements confidentiels. Dans le cadre des activités de communication et d'affaires, deux parties échangent souvent des renseignements ou des données que l'une ou l'autre doit garder accessibles sur demande. Voici des exemples de renseignements pouvant faire l'objet d'une obligation de confidentialité :

- détails des opérations;
- plans d'ingénieur;
- plans d'affaires;
- renseignements bancaires au sujet des entreprises;
- disponibilité des stocks;
- prix proposés ou demandés;
- listes de prix;
- documents juridiques;
- chiffre d'affaires par client et par secteur.

De plus, à la différence des renseignements personnels, les droits d'accès aux renseignements confidentiels permettant de vérifier si ceux-ci sont exacts et complets ne sont pas définis clairement. En conséquence, les interprétations de ce que l'on considère comme des renseignements confidentiels peuvent varier considérablement d'une organisation à l'autre et sont, dans la plupart des cas, motivées par des ententes contractuelles. Pour un complément d'information sur les critères en matière de confidentialité, veuillez consulter les principes, critères et exemples des Services Trust de l'ICCA et de l'AICPA relatifs à la sécurité, à l'accessibilité, à l'intégrité du traitement, à la confidentialité et à la protection des renseignements personnels (voir www.aicpa.org/TrustServices ou www.webtrust.org).

Principes généralement reconnus en matière de protection des renseignements personnels – Mise en contexte

Les PPRP visent à aider la direction à mettre en place un programme efficace, qui tient compte des risques, des obligations et des occasions d'affaires propres à l'entité liés à la protection des renseignements personnels.

Les principes et les critères en matière de protection des renseignements personnels s'appuient sur des notions clés empruntées aux textes législatifs et aux lignes directrices d'importance à l'échelle locale, nationale et internationale² et sur les bonnes pratiques d'affaires. L'application des PPRP permet aux organisations de relever de façon proactive les défis importants que posent la mise en place des programmes de protection des renseignements personnels ainsi que la gestion de ces programmes et des risques connexes, du point de vue de l'entreprise. Les PPRP permettent également une simplification de la gestion des risques liés à la protection des renseignements personnels lorsque plusieurs ressorts territoriaux sont en cause.

Objectif général de la protection des renseignements personnels

Les principes de protection des renseignements personnels et les critères connexes sont fondés sur l'objectif suivant.

² Par exemple, l'Organisation de coopération et de développement économiques a publié des *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* et l'Union Européenne a publié la *Directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* (Directive 95/46/CE). D'autre part, les États-Unis ont adopté la loi Gramm-Leach-Bliley, la *Health Insurance Portability and Accountability Act* et la *Children's Online Privacy Protection Act*. Le Canada s'est doté de la *Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)*, tandis que l'Australie a adopté la loi de 1988 sur la protection des renseignements personnels (modifiée en 2001). On trouvera en ligne à l'adresse www.aicpa.org/privacy (en anglais) un tableau dressant une comparaison entre ces concepts internationaux de protection des renseignements personnels et les PPRP. Le respect de ces principes-ci et de leurs critères connexes ne vous met pas nécessairement en conformité avec les lois et règlements applicables en matière de protection des renseignements personnels; les entités devraient donc consulter un conseiller juridique compétent au sujet du respect de ces lois et règlements.

La collecte, l'utilisation, la conservation, la communication et la suppression des renseignements personnels se font en conformité avec les engagements énoncés dans l'avis sur la protection des renseignements personnels donné par l'entité et avec les critères établis dans le cadre des principes généralement reconnus en matière de protection des renseignements personnels publiés par l'ICCA et l'AICPA.

Principes généralement reconnus en matière de protection des renseignements personnels

Les principes de protection des renseignements personnels sont essentiels à la protection et à la gestion adéquates des renseignements personnels. Ces principes se fondent sur les pratiques loyales en la matière, reconnues à l'échelle internationale, qui sont énoncées dans de nombreux textes légaux et réglementaires de divers pays et sur des pratiques considérées comme bonnes.

Les dix principes sont les suivants :

1. **Gestion**. L'entité définit, consigne et diffuse ses politiques et procédures en matière de protection des renseignements personnels, et en confie la responsabilité à une personne ou à un groupe.
2. **Avis**. L'entité fait connaître, par un avis, ses politiques et procédures en matière de protection des renseignements personnels et indique les fins auxquelles les renseignements personnels sont recueillis, utilisés, conservés et communiqués.
3. **Choix et consentement**. L'entité décrit le choix offert à l'individu et obtient son consentement implicite ou explicite quant à la collecte, à l'utilisation et à la communication de renseignements personnels.
4. **Collecte**. L'entité ne recueille des renseignements personnels qu'aux fins mentionnées dans l'avis.
5. **Utilisation, conservation et suppression**. L'entité limite l'utilisation de renseignements personnels aux fins mentionnées dans l'avis, à l'égard desquelles l'individu a donné son consentement implicite ou explicite. L'entité ne conserve les renseignements personnels que pendant le temps nécessaire pour la réalisation des fins mentionnées ou selon les stipulations des textes légaux ou réglementaires, puis il les détruit de façon appropriée.
6. **Accès**. L'entité donne aux individus accès aux renseignements personnels les concernant, pour qu'ils puissent les examiner et les mettre à jour.

7. **Communication à des tiers**. L'entité ne communique des renseignements personnels à des tiers qu'aux fins mentionnées dans l'avis, et avec le consentement implicite ou explicite de l'individu.
8. **Sécurité**. L'entité protège les renseignements personnels contre tout accès non autorisé (aussi bien physique que logique).
9. **Qualité**. L'entité garde des renseignements personnels exacts, complets et pertinents, aux fins mentionnées dans l'avis.
10. **Suivi et application**. L'entité fait le suivi du respect de ses politiques et procédures en matière de protection des renseignements personnels, et a instauré des procédures pour le traitement des plaintes et des contestations relevant de cette question.

À chacun des dix principes relatifs à la protection des renseignements personnels sont associés des critères pertinents, objectifs, complets et mesurables qui visent à orienter l'élaboration et l'évaluation des politiques, des communications, des procédures et des contrôles d'une entité en la matière. Les *politiques de protection des renseignements personnels* sont des déclarations écrites exprimant l'intention de la direction, ses objectifs, ses exigences, ses responsabilités et ses normes. Les *communications* désignent les communications de l'organisation destinées aux individus, au [personnel interne](#) et aux [tiers](#) au sujet de l'avis sur la protection des renseignements personnels, des engagements qu'il contient et d'autres informations pertinentes. Quant aux *procédures* et aux *contrôles*, il s'agit des autres mesures que prend l'organisation pour satisfaire aux critères.

Application des PPRP

Les organisations peuvent utiliser les PPRP aux fins suivantes :

- conception, mise en œuvre et communication des politiques de protection des renseignements personnels;
- établissement et gestion de programmes de protection des renseignements personnels;
- surveillance et vérification des programmes de protection des renseignements personnels;
- mesure de la performance et étalonnage.

Les activités suivantes s'inscrivent dans le cadre de l'établissement et de la gestion d'un programme de protection des renseignements personnels :

Stratégie – planification stratégique et d'entreprise en matière de protection des renseignements personnels;

Diagnostic – analyse des faiblesses et des risques liés à la protection des renseignements personnels;

Mise en œuvre – élaboration, documentation, introduction et institutionnalisation du plan d'action du programme, y compris l'établissement de contrôles visant les renseignements personnels.

Soutien et gestion – suivi des activités liées à un programme de protection des renseignements personnels;

Vérification – évaluation du programme de protection des renseignements personnels d'une organisation par des vérificateurs internes ou externes.

Le tableau qui suit résume et illustre comment une organisation peut appliquer les PPRP dans le cadre de ces activités.

ACTIVITÉ	DISCUSSION GÉNÉRALE	APPLICATION POSSIBLE DES PRINCIPES GÉNÉRALEMENT RECONNUS EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS
Stratégie	<p>Vision. La stratégie d'une entité établit sa direction à long terme et vise sa prospérité. La vision définit la culture de l'entité et contribue à façonner et à déterminer la façon dont elle interagit avec son environnement externe, y compris ses clients, ses concurrents, ainsi que sa façon d'aborder les questions juridiques, sociales et éthiques.</p> <p>Planification stratégique. Il s'agit du plan directeur d'ensemble de l'entité, qui englobe son orientation stratégique. L'objectif du plan est de faire en sorte que tous les efforts de l'entité soient dirigés dans la même direction. Il énonce les objectifs à long terme de l'entité et les points clés à prendre en compte pour qu'elle devienne «conforme» en matière de protection des renseignements personnels.</p> <p>Affectation des ressources. Cette étape décrit les ressources humaines, financières et autres affectées pour atteindre les buts et les objectifs énoncés dans le plan stratégique ou le plan d'affaires.</p>	<p>Vision. Dans le cadre des efforts visant la protection des renseignements personnels, la détermination de la vision aide l'entité à intégrer ses préférences et à classer ses objectifs par ordre de priorité.</p> <p>Planification stratégique. Dans le cadre des travaux de l'organisation aux fins de la protection des renseignements personnels, les PPRP peuvent permettre de repérer des éléments importants devant être traités.</p> <p>Affectation des ressources. En se fondant sur les PPRP, l'entité identifie les gens qui s'occupent de la gestion des systèmes d'information ou des questions de protection des renseignements personnels et de sécurité, et précise les ressources allouées à ces activités.</p>

ACTIVITÉ	DISCUSSION GÉNÉRALE	APPLICATION POSSIBLE DES PRINCIPES GÉNÉRALEMENT RECONNUS EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS
		<p>Stratégie globale. Un document stratégique décrit les avancées attendues ou prévues. Les PPRP peuvent aider une entité à préciser ses plans concernant les systèmes à l'étude ou ses objectifs en matière de protection des renseignements personnels. Le plan décrit la marche à suivre pour atteindre les objectifs ainsi que les jalons. Il prévoit également un mécanisme de communication des éléments critiques de la mise en œuvre : détails sur les services, budgets, frais de développement, promotion, publicité relative à la protection des renseignements personnels, etc.</p>
Diagnostic	<p>Cette étape, souvent appelée la phase d'évaluation, comprend une analyse poussée de l'environnement de l'entité et l'identification des opportunités présentes là où il existe des faiblesses, une vulnérabilité et des menaces. Pour une organisation, le projet le plus courant est un diagnostic d'évaluation. Celui-ci vise à évaluer l'entité par rapport à ses buts et objectifs en matière de protection des renseignements personnels et à déterminer dans quelle mesure ceux-ci sont atteints.</p>	<p>Les PPRP peuvent aider l'entité à comprendre ses risques de haut niveau, ses opportunités, ses besoins, les politiques et pratiques en matière de protection des renseignements personnels, les pressions concurrentielles qu'elle subit, et les exigences des lois et règlements pertinents qu'elle doit respecter.</p> <p>Les PPRP constituent un point de référence juridiquement neutre permettant à l'entité d'évaluer le degré actuel de protection des renseignements personnels par rapport au degré de protection voulu.</p>
Mise en œuvre	<p>Cette étape consiste à arrêter un plan d'action, à mettre en œuvre une recommandation ou à faire les deux. La mise en œuvre implique l'élaboration et la documentation d'un programme et d'un plan d'action en matière de protection des renseignements personnels ainsi que l'exécution de toutes les tâches, planifiées et autres, nécessaires pour rendre le plan d'action opérationnel : déterminer qui exécutera quelle tâche,</p>	<p>Les PPRP peuvent aider l'entité à atteindre ses objectifs de mise en œuvre. Une fois cette phase terminée, l'entité devrait avoir élaboré ce qui suit :</p> <ul style="list-style-type: none"> systèmes, procédures et processus visant à satisfaire aux exigences concernant la protection des renseignements personnels; formulaires, dépliants et contrats mis à jour pour être conformes à la protection des

ACTIVITÉ	DISCUSSION GÉNÉRALE	APPLICATION POSSIBLE DES PRINCIPES GÉNÉRALEMENT RECONNUS EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS
	affecter les responsabilités, établir les calendriers et définir les jalons. Cela suppose la planification et la mise en œuvre d'une série de projets planifiés dans le but de donner à l'organisation des indications, une orientation, une méthodologie et des outils pour mettre ses initiatives au point.	renseignements personnels; programmes internes et externes de sensibilisation à la protection des renseignements personnels.
Soutien et gestion	Le soutien et la gestion demandent de surveiller le travail afin de repérer les cas où les progrès diffèrent du plan d'action à temps pour apporter des correctifs. La surveillance a trait aux politiques et aux processus de la direction ainsi qu'à la technologie connexe visant à assurer le respect des politiques et des procédures de l'organisation en matière de protection des renseignements personnels, et à la capacité de faire preuve de diligence raisonnable.	L'entité peut appliquer les PPRP, par exemple dans le cadre de l'élaboration de critères appropriés ayant trait à la présentation des résultats de la surveillance des demandes d'information, des sources utilisées pour compiler les renseignements et des renseignements communiqués. Les principes peuvent également servir à établir des procédures de validation visant à assurer que les tiers auxquels les renseignements sont communiqués sont autorisés à recevoir ces renseignements.
Vérification interne de la protection des renseignements personnels	Les vérificateurs internes fournissent des services objectifs qui donnent à l'entité une assurance sur le degré de maîtrise de ses opérations, apportent leurs conseils pour les améliorer, et contribuent à créer de la valeur ajoutée. Ils aident l'entité à atteindre ses objectifs en évaluant et en améliorant, suivant une approche systématique et méthodique, ses processus de gestion des risques, de contrôle et de gouvernance.	Les vérificateurs internes peuvent évaluer le programme et les contrôles de protection des renseignements personnels d'une entité en utilisant les PPRP comme point de référence, en plus de fournir des informations et des rapports utiles à la direction.
Vérification externe de la protection des renseignements personnels	Les vérificateurs externes, notamment les comptables agréés (CA) et les <i>certified public accountants</i> (CPA), peuvent fournir des services d'attestation et de certification. En général, ces services, qu'ils portent sur les informations financières ou non financières, inspirent confiance aux particuliers, à la direction, aux clients, aux partenaires d'affaires et aux autres utilisateurs.	Un vérificateur externe peut évaluer le programme et les contrôles de protection des renseignements personnels d'une entité en conformité avec les PPRP et produire des rapports utiles pour les particuliers, la direction, les clients, les partenaires d'affaires et les autres utilisateurs.

Présentation des principes généralement reconnus et des critères en matière de protection des renseignements personnels

Pour chaque principe, les critères sont présentés en trois colonnes. La première colonne renferme les critères de mesure. La deuxième colonne, qui contient des exemples de contrôles et de procédures, vise à faire mieux comprendre comment appliquer les critères. Les exemples ne se veulent pas exhaustifs, et aucun d'eux n'est indispensable pour qu'une entité satisfasse aux critères. Dans la troisième colonne, on trouvera des considérations additionnelles, notamment de l'information portant sur les bonnes pratiques et quelques exigences énoncées dans des textes légaux et réglementaires pouvant viser un secteur d'activité ou un pays donné.

Il peut arriver que certains des critères ne soient pas directement applicables à certaines organisations ou à certains processus. L'entité qui décide de considérer un critère comme non applicable devrait songer à justifier une telle décision dans la perspective d'une évaluation future.

Ces principes et critères constituent un fondement pour la conception, la mise en œuvre, l'application, l'évaluation et la vérification d'un programme de protection des renseignements personnels en vue de répondre aux besoins d'une entité.

Principes généralement reconnus et critères en matière de protection des renseignements personnels

Gestion

Section	Critères de gestion	Exemples de contrôles et de procédures	Autres considérations
1.0	L' entité définit, consigne et diffuse ses politiques et procédures en matière de protection des renseignements personnels , et en confie la responsabilité à une personne ou à un groupe.		
1.1	Politiques et communications		
1.1.0	<p>Politiques de protection des renseignements personnels</p> <p>L'entité définit et consigne ses politiques de protection des renseignements personnels à l'égard des aspects suivants :</p> <ul style="list-style-type: none"> a) avis (voir la section 2.1.0); b) choix et consentement (voir la section 3.1.0); c) collecte (voir la section 4.1.0); d) utilisation, conservation et suppression (voir la section 5.1.0); e) accès (voir la section 6.1.0); f) communication à des tiers (voir la section 7.1.0); g) sécurité des renseignements personnels (voir la section 8.1.0); h) qualité (voir la section 9.1.0); i) suivi et application (voir la section 10.1.0). 	Les politiques de protection des renseignements personnels sont consignées et peuvent facilement être consultées au besoin par le personnel interne et par les tiers.	
1.1.1	<p>Communication au personnel interne</p> <p>Les politiques de protection des renseignements personnels, et les</p>	L'entité : communique périodiquement au personnel interne (par le truchement, par exemple, d'un	Les politiques de protection des renseignements personnels (au sens où on l'entend ici) englobent les politiques de sécurité pertinentes pour la

Section	Critères de gestion	Exemples de contrôles et de procédures	Autres considérations
	<p>conséquences d'un manquement à ces politiques, sont communiquées au moins une fois l'an au personnel interne de l'entité à qui incombent la collecte, l'utilisation, la conservation et la communication des renseignements personnels. Lorsque des changements sont apportés à ces politiques, ils sont communiqués à ce personnel peu de temps après leur approbation.</p>	<p>réseau ou d'un site Web) l'information pertinente sur les politiques de l'entité en matière de protection des renseignements personnels. Les changements apportés à ces politiques sont communiqués peu après leur approbation; demande au personnel interne de confirmer (initialement puis à intervalles réguliers) qu'il comprend bien les politiques de l'entité en matière de protection des renseignements personnels et qu'il s'engage à s'y conformer.</p>	<p>protection de ces renseignements.</p>
1.1.2	<p>Responsabilité des politiques et reddition de comptes à cet égard Une personne ou un groupe est chargé d'élaborer, de consigner, de mettre en œuvre, de mettre en application, de surveiller et de mettre à jour les politiques de l'entité en matière de protection des renseignements personnels, et doit rendre des comptes à cet égard. Le nom de la personne ou du groupe est communiqué au personnel interne, de même que ses responsabilités.</p>	<p>L'entité confie la responsabilité des politiques de protection des renseignements personnels à une personne désignée. (Cette responsabilité pourra être confiée à des personnes différentes de celles qui sont responsables d'autres politiques, comme celles qui touchent la sécurité.)</p> <p>Les pouvoirs, les responsabilités et l'obligation de rendre compte de la personne ou du groupe désigné sont clairement consignés. Les responsabilités comprennent ce qui suit :</p> <ul style="list-style-type: none"> établir en collaboration avec la direction des normes pour le classement des renseignements personnels selon leur caractère sensible et pour la détermination du degré de protection nécessaire; formuler et maintenir les politiques de l'entité en matière de protection 	<p>La personne à qui l'on confie la responsabilité de la protection des renseignements personnels devrait faire partie du personnel interne de l'entité.</p>

Section	Critères de gestion	Exemples de contrôles et de procédures	Autres considérations
		<p>des renseignements personnels; surveiller et mettre à jour les politiques de l'entité en matière de protection des renseignements personnels; déléguer des pouvoirs concernant la mise en application des politiques de l'entité en matière de protection des renseignements personnels; surveiller la mesure dans laquelle les politiques sont respectées et prendre des mesures afin d'améliorer la formation ou de clarifier les politiques et pratiques.</p> <p>Un comité du conseil d'administration inclut périodiquement la protection des renseignements personnels dans son examen habituel de l'ensemble de la gouvernance.</p>	
1.2	Procédures et contrôles		
1.2.1	<p>Examen et approbation Les politiques et procédures relatives à la protection des renseignements personnels ainsi que les changements qui y sont apportés sont examinés et approuvés par la direction.</p>	<p>Les politiques et procédures relatives à la protection des renseignements personnels sont :</p> <ul style="list-style-type: none"> examinées et approuvées par la direction générale ou par un comité de gestion; examinées au moins une fois l'an et mises à jour au besoin. 	
1.2.2	<p>Conformité des politiques et procédures relatives à la protection des renseignements personnels avec les lois et règlements LES POLITIQUES ET PROCÉDURES SONT EXAMINÉES ET COMPARÉES AUX EXIGENCES DES LOIS ET RÈGLEMENTS</p>	<p>Le conseiller juridique de l'entité ou ses services juridiques :</p> <ul style="list-style-type: none"> déterminent les lois et règlements relatifs à la protection des renseignements personnels qui sont applicables dans les ressorts territoriaux où l'entité exerce ses activités; 	<p>En plus des exigences légales et réglementaires, des entités peuvent choisir de se conformer à certaines normes, comme les normes ISO, ou être tenues de se conformer à certaines normes, comme les normes du secteur des cartes de paiement (PCI), pour pouvoir faire des affaires. Les entités</p>

Section	Critères de gestion	Exemples de contrôles et de procédures	Autres considérations
	<p>APPLICABLES AU MOINS UNE FOIS L'AN, ET À CHAQUE MODIFICATION DE CES LOIS ET RÈGLEMENTS. LES POLITIQUES ET PROCÉDURES RELATIVES À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS SONT RÉVISÉES DE FAÇON À ÊTRE RENDUES CONFORMES AUX EXIGENCES DES LOIS ET RÈGLEMENTS APPLICABLES.</p>	<p>identifient les autres normes applicables à l'entité; révisent les politiques et procédures de l'entité pour s'assurer qu'elles sont conformes aux lois, aux règlements et aux normes appropriées applicables.</p>	<p>peuvent intégrer ces normes dans le processus décrit ci-contre.</p>
1.2.3	<p>Identification et classement des renseignements personnels Les types de renseignements personnels, sensibles et autres, ainsi que les processus, les systèmes connexes et les tiers qui traitent ces renseignements sont identifiés. Ces renseignements sont couverts par les politiques et procédures de l'entité en matière de protection des renseignements personnels et par les politiques et procédures de sécurité connexes.</p>	<p>L'entité s'est dotée à la fois de politiques et de processus de classement des renseignements, notamment :</p> <ul style="list-style-type: none"> ○ un processus de classement, qui permet d'identifier et de classer chaque renseignement dans l'une ou plusieurs de ces catégories : ○ confidentiels d'affaires, ○ renseignements personnels (sensibles et autres), ○ généraux d'affaires, ○ publics; <p>l'identification des processus, des systèmes et des tiers qui traitent des renseignements personnels; des politiques et des procédures de sécurité et de protection des renseignements personnels spécifiques pour chacune des catégories sus-définies.</p>	

Section	Critères de gestion	Exemples de contrôles et de procédures	Autres considérations
1.2.4	<p>Évaluation des risques Un processus d'évaluation des risques permet d'établir un scénario de risques de base et, au moins une fois par an, d'identifier l'évolution des risques ou les risques nouveaux auxquels sont exposés les renseignements personnels et de préparer et mettre à jour les réponses à ces risques.</p>	<p>On a mis en place un processus pour identifier périodiquement les risques auxquels sont exposés les renseignements personnels détenus par l'entité. De tels risques peuvent être externes (par exemple, perte de renseignements ou non-respect des exigences réglementaires par des fournisseurs) ou internes (par exemple, transmission électronique non sécurisée de renseignements sensibles). Lorsque des risques modifiés ou nouveaux sont identifiés, les stratégies d'évaluation des risques en matière de protection des renseignements personnels et les stratégies de réponses sont mises à jour.</p> <p>Le processus tient compte de facteurs comme l'expérience de la gestion des incidents touchant la protection des renseignements personnels, le processus de traitement des plaintes et de résolution des contestations ou le suivi des activités.</p>	<p>Idéalement, l'entité devrait intégrer l'évaluation des risques en matière de protection des renseignements personnels à celle des risques relatifs à la sécurité, et ce, dans le cadre de son programme global de gestion des risques. Le conseil d'administration ou l'un de ses comités devrait assurer la surveillance et la revue de l'évaluation des risques en matière de protection des renseignements personnels.</p>
1.2.5	<p>Conformité des engagements avec les politiques et procédures relatives à la protection des renseignements personnels Le personnel ou les conseillers de l'entité vérifient les contrats pour s'assurer de leur conformité avec les politiques et procédures relatives à la protection des renseignements personnels, et remédient à toute incompatibilité éventuelle.</p>	<p>Tant la direction que les services juridiques examinent tous les contrats et les ententes sur les niveaux de service pour s'assurer de leur conformité avec les politiques et procédures de l'entité relatives à la protection des renseignements personnels.</p>	

Section	Critères de gestion	Exemples de contrôles et de procédures	Autres considérations
1.2.6	<p>Gestion de l'infrastructure et des systèmes Les répercussions possibles sur la protection des renseignements personnels sont évaluées lors de la mise en place de nouveaux processus où entrent en jeu des renseignements personnels (y compris des activités sous-traitées par des tiers ou des collaborateurs externes) et les renseignements personnels continuent d'être protégés en application des politiques de protection des renseignements personnels. De ce point de vue, les processus où entrent en jeu des renseignements personnels englobent la conception, l'acquisition, le développement, la mise en place, la configuration, la modification et la gestion des éléments suivants :</p> <ul style="list-style-type: none"> infrastructure, systèmes, applications, sites Web, procédures, produits et services bases de données et dépôts de renseignements ordinateurs mobiles et autres appareils électroniques similaires <p>L'utilisation de renseignements personnels pour tester et développer les processus ou les systèmes est interdite à moins que ces renseignements ne soient désidentifiés ou autrement protégés selon les politiques et procédures de l'entité en</p>	<p>Les procédures ou contrôles suivants permettent de traiter les répercussions évoquées ci-contre :</p> <ul style="list-style-type: none"> la direction évalue les répercussions en matière de protection des renseignements personnels de l'apparition ou de la modification profonde de produits, de services, de processus d'affaires ou de l'infrastructure; l'entité utilise un processus documenté de développement de systèmes et de gestion du changement pour tous les systèmes d'information et les technologies connexes (y compris les procédures manuelles, les programmes d'application, l'infrastructure technologique, la structure organisationnelle et les responsabilités, tant des utilisateurs que des responsables du fonctionnement des systèmes) servant à recueillir, utiliser, conserver, communiquer et détruire des renseignements personnels; l'entité analyse l'effet potentiel des nouveaux systèmes et des modifications en projet sur la protection des renseignements personnels; en cas de modification, les composantes de systèmes sont soumises à des tests afin de réduire au minimum le risque d'effets néfastes sur la protection des renseignements personnels. Toutes les données utilisées pour ces tests 	<p>Dans certains ressorts territoriaux, il est interdit d'utiliser des renseignements personnels à des fins de test ou de développement à moins de les avoir désidentifiés ou autrement protégés au même degré exigé selon les politiques relatives à l'information de production.</p>

Section	Critères de gestion	Exemples de contrôles et de procédures	Autres considérations
	<p>matière de protection des renseignements personnels.</p>	<p>sont désidentifiées. On maintient une base de données test contrôlée, afin d'effectuer des tests complets de non-régression, permettant de s'assurer que les modifications apportées à un programme n'ont pas un effet négatif sur d'autres programmes qui traitent des renseignements personnels; des procédures assurent le maintien de l'intégrité et de la protection des renseignements personnels pendant les migrations vers de nouveaux systèmes ou des systèmes modifiés; le responsable de la protection des renseignements personnels, le responsable de la sécurité, le directeur de l'unité fonctionnelle et le responsable des TI doivent consigner et approuver les changements apportés aux systèmes et procédures liés au traitement de renseignements personnels, y compris les changements qui peuvent avoir une incidence sur la sécurité, avant leur mise en œuvre. Les changements urgents doivent se faire avec le même niveau de protection des renseignements personnels que les autres; ils peuvent toutefois être consignés et approuvés après coup.</p> <p>La fonction TI conserve une liste de tous les logiciels utilisés qui traitent des renseignements personnels, indiquant le niveau, la version ainsi que les correctifs qui ont été installés.</p>	

Section	Critères de gestion	Exemples de contrôles et de procédures	Autres considérations
		<p>Des procédures ont été mises en place pour faire en sorte que seules les modifications qui ont été autorisées, testées et consignées sont apportées aux systèmes.</p> <p>Lorsque des systèmes informatisés entrent en jeu, on suit des procédures appropriées, comme l'utilisation de bibliothèques séparées pour le développement, les tests et la production, afin de restreindre comme il convient l'accès aux renseignements personnels.</p> <p>Le personnel responsable de la conception ou de la mise en œuvre de nouveaux systèmes ou de modifications de systèmes ainsi que les utilisateurs d'applications ou de processus nouveaux ou révisés reçoivent des séances de formation et de sensibilisation ayant trait à la protection des renseignements personnels. Des rôles et des responsabilités spécifiques sont attribués au titre de la protection des renseignements personnels.</p>	
1.2.7	<p>Gestion des atteintes à la protection des renseignements personnels et des incidents qui s'y rapportent</p> <p>L'entité s'est dotée d'un programme de gestion des atteintes à la protection des renseignements personnels et des incidents qui s'y rapportent, qui comprend, sans toutefois s'y limiter, les éléments suivants :</p>	<p>Un programme structuré complet de gestion des atteintes à la protection des renseignements personnels (PRP) et des incidents qui s'y rapportent a été mis en œuvre, comprenant les points suivants :</p> <ul style="list-style-type: none"> les incidents et atteintes sont communiqués à un membre de l'équipe d'intervention en cas d'atteinte à la PRP; celui-ci 	<p>Il se peut que certaines entités adoptent une politique de notification des victimes d'une atteinte à la PRP pour l'ensemble des territoires où elles sont présentes. Forcément, une telle politique respectera, au minimum, les obligations juridiques du territoire imposant les règles les plus strictes.</p>

Section	Critères de gestion	Exemples de contrôles et de procédures	Autres considérations
	<p>des procédures d'identification, de gestion et de résolution des atteintes à la protection des renseignements personnels et des incidents s'y rapportant; des responsabilités définies; un processus d'identification de la gravité des incidents, définissant les réactions qui s'imposent et un ordre hiérarchique des interventions; un processus de conformité aux textes légaux et réglementaires visant les atteintes à la protection des renseignements personnels, y compris la notification des intéressés, le cas échéant; un processus de reddition de comptes des salariés ou des tiers responsables d'atteintes à la protection des renseignements personnels ou d'incidents s'y rapportant, comprenant des mesures correctives, des pénalités ou des mesures disciplinaires selon le cas; un processus de revue périodique (annuelle au moins) des incidents survenus afin d'identifier les mises à jour à apporter au programme, compte tenu notamment :</p> <ul style="list-style-type: none"> o des constantes et des causes profondes d'incidents, o des modifications de 	<p>apprécie si l'incident relève de la PRP, de la sécurité ou des deux, classe l'incident selon sa gravité, déclenche les actions requises et détermine, le cas échéant, les responsables de la PRP ou de la sécurité dont l'intervention s'impose; le responsable de la PRP est comptable de l'ensemble du programme. Il est appuyé par des comités directeurs de la PRP et de la sécurité et par une équipe d'intervention en cas d'atteinte à la PRP. Les incidents et les atteintes qui ne concernent pas les renseignements personnels relèvent du responsable de la sécurité; l'entité s'est dotée d'une politique de notification des atteintes à la PRP, reposant notamment sur :</p> <p>a) un processus d'identification des obligations de notification et autres imposées par les ressorts territoriaux dont relèvent, le cas échéant, les sujets visés, b) un processus permettant d'apprécier s'il faut ou non aviser les intéressés au sujet de l'atteinte, lorsque des textes légaux ou réglementaires ou encore la politique de l'entité l'imposent, c) un processus permettant de transmettre la notification en temps opportun. L'entité a conclu des contrats avec des</p>	

Section	Critères de gestion	Exemples de contrôles et de procédures	Autres considérations
	<p>l'environnement de contrôle interne ou des obligations externes (textes légaux ou réglementaires);</p> <p>des tests périodiques ou de cheminement (tous les ans au minimum) assortis des mesures correctives nécessaires.</p>	<p>sociétés tierces pour la gestion du processus de notification ainsi que la prestation de services de surveillance du dossier de crédit, en cas de besoin;</p> <p>un ordre hiérarchique clair des interventions, selon le type et/ou la gravité de l'incident en cause, remontant jusqu'à la haute direction, au conseiller juridique et au conseil d'administration;</p> <p>un processus d'alerte des autorités policières, réglementaires ou autres en cas de besoin;</p> <p>la formation des nouveaux employés ou membres des équipes ainsi que des activités de sensibilisation de l'ensemble du personnel, ayant lieu au moins une fois par an, chaque fois que le programme fait l'objet d'une modification importante et après tout incident majeur.</p> <p>Le programme de gestion des atteintes à la PRP et des incidents s'y rapportant prévoit également les mesures suivantes :</p> <p>après chaque incident majeur, la fonction d'audit interne ou des consultants externes procèdent à une évaluation formelle de l'incident;</p> <p>on effectue une revue trimestrielle des incidents survenus et on identifie les mises à jour qui s'imposent sur la base</p>	

Section	Critères de gestion	Exemples de contrôles et de procédures	Autres considérations
		<p>des éléments suivants :</p> <ul style="list-style-type: none"> o causes profondes, o constantes, o modifications de l'environnement de contrôle interne ou des textes légaux; <p>les résultats de ces revues sont communiqués au comité directeur de la PRP chaque trimestre, et au comité d'audit une fois par an;</p> <p>on a défini des indicateurs clés, dont l'évolution est suivie et communiquée à la haute direction chaque trimestre;</p> <p>le programme est testé au moins tous les six mois et peu après la mise en œuvre de modifications importantes des systèmes ou des procédures.</p>	
1.2.8	<p>Ressources d'appui L'entité fournit les ressources nécessaires à la mise en œuvre et à l'appui de ses politiques de protection des renseignements personnels.</p>	<p>La direction examine une fois l'an l'affectation du personnel, de ressources financières et d'autres ressources à son programme de protection des renseignements personnels.</p>	
1.2.9	<p>Compétences du personnel interne L'entité détermine les compétences requises chez le personnel responsable de la protection des renseignements personnels, et n'attribue des responsabilités en la matière qu'aux membres du personnel qui possèdent ces compétences et qui ont reçu la formation nécessaire.</p>	<p>On s'assure des compétences du personnel interne responsable de la protection des renseignements personnels au moyen de mesures comme les suivantes :</p> <ul style="list-style-type: none"> o définitions de poste officielles (faisant notamment état des responsabilités, des exigences en matière de formation et sur le plan professionnel ainsi que des rapports hiérarchiques dans le cas des postes 	

Section	Critères de gestion	Exemples de contrôles et de procédures	Autres considérations
		<p>clés au chapitre de la gestion des renseignements personnels); procédures d'embauche (y compris la vérification complète des titres de compétence, des références et des antécédents) et contrats de travail et ententes de confidentialité officiels; évaluations du rendement (effectuées par les supérieurs, y compris l'évaluation des activités de perfectionnement professionnel).</p>	
1.2.10	<p>Sensibilisation et formation en matière de protection des renseignements personnels L'entité offre un programme de sensibilisation à la protection des renseignements personnels et aux questions connexes ainsi qu'une formation spécifique tenant compte du rôle et des responsabilités de certains employés.</p>	<p>Tous les employés sont tenus de suivre chaque année un cours interactif en ligne sensibilisant à la PRP et à la sécurité. Les nouveaux employés, collaborateurs externes et autres sont tenus d'avoir effectué ce cours dans le mois qui suit leur engagement afin de pouvoir conserver leurs privilèges d'accès.</p> <p>L'entité offre une formation approfondie couvrant les politiques et procédures de PRP et de sécurité pertinentes, les questions légales et réglementaires, les réactions en cas d'incidents et les sujets connexes. Une telle formation est obligatoire une fois par an pour tous les employés ayant accès à des renseignements personnels ou responsables de la PRP; est adaptée aux responsabilités respectives des employés; est complétée par des séances de formation et des conférences extérieures.</p>	

Section	Critères de gestion	Exemples de contrôles et de procédures	Autres considérations
		<p>La participation aux cours de formation et de sensibilisation à la PRP offerts par l'entité fait l'objet d'un contrôle.</p> <p>Les cours de formation et de sensibilisation sont régulièrement revus et mis à jour en fonction des exigences légales, réglementaires et sectorielles et des politiques et procédures de l'entité.</p>	
1.2.11	<p>Modifications du cadre réglementaire et du cadre de l'entreprise</p> <p>Pour chacun des pays ou ressorts territoriaux dans lesquels l'entité exerce ses activités, on s'occupe de l'incidence, sur les obligations en matière de PRP, des changements touchant les aspects suivants :</p> <ul style="list-style-type: none"> l'encadrement légal et réglementaire; les contrats, y compris les ententes sur les niveaux de service; les exigences sectorielles; les activités et processus de l'entité; les personnes, les rôles et les responsabilités; la technologie. <p>LES POLITIQUES ET PROCÉDURES RELATIVES AUX RENSEIGNEMENTS PERSONNELS SONT MISES À JOUR POUR REFLÉTER L'ÉVOLUTION DES OBLIGATIONS.</p>	<p>L'entité a mis en place un processus continu permettant de surveiller et d'évaluer l'incidence, sur les obligations en matière de PRP, des changements touchant les aspects suivants :</p> <ul style="list-style-type: none"> le cadre légal et réglementaire; les exigences sectorielles (comme celles de la Direct Marketing Association); les contrats, y compris les ententes sur les niveaux de service conclus avec des tiers (les changements ayant pour effet de modifier les clauses contractuelles touchant la protection des renseignements personnels sont examinés et approuvés par le responsable de la protection des renseignements personnels ou par le conseiller juridique avant d'être effectués); les activités et processus de l'entité; les personnes assumant une responsabilité au chapitre de la PRP ou de la sécurité; la technologie (avant la mise en application). 	<p>Idéalement, ces procédures devraient être coordonnées avec le processus d'évaluation des risques.</p> <p>L'entité devrait également tenir compte des pratiques nouvelles ou des bonnes pratiques, comme la notification des atteintes à la PRP dans des pays ou des ressorts territoriaux où elle n'est pas obligatoire.</p>

Avis

Section	Critères relatifs aux avis	Exemples de contrôle et de procédures	Autres considérations
2.0	L'entité fait connaître, par un avis, ses politiques et procédures en matière de protection des renseignements personnels et indique les fins auxquelles les renseignements personnels sont recueillis, utilisés, conservés et communiqués.		
2.1	Politiques et communications		
2.1.0	Politiques de protection des renseignements personnels Les politiques de l'entité en matière de protection des renseignements personnels font état de l'avis devant être donné aux individus .		
2.1.1	Communication aux individus Un avis est donné aux individus au sujet des politiques suivantes relatives à la protection des renseignements personnels : <ul style="list-style-type: none"> a) fins auxquelles sont recueillis les renseignements personnels; b) choix et consentement (voir la section 3.1.1); c) collecte (voir la section 4.1.1); d) utilisation, conservation et suppression (voir la section 5.1.1); e) accès (voir la section 6.1.1); f) communication à des tiers (voir la section 7.1.1); g) sécurité des renseignements personnels (voir la section 8.1.1); h) qualité (voir la section 9.1.1); i) suivi et application (voir la section 10.1.1). Si des renseignements personnels sont	L'avis donné par l'entité : <ul style="list-style-type: none"> décrit les renseignements personnels recueillis ainsi que les sources auprès desquelles et les fins auxquelles ils sont recueillis; indique les fins auxquelles sont recueillis des renseignements personnels sensibles, en précisant si cela s'inscrit dans le cadre d'une obligation légale; décrit les conséquences qu'aurait le fait de ne pas fournir les renseignements demandés; indique que certains renseignements personnels pourraient être approfondis afin de mieux connaître les individus, par exemple leur profil d'achat; peut être donné de diverses façons (par exemple, lors d'une conversation en personne, d'une 	L'avis peut aussi décrire les situations dans lesquelles des renseignements personnels seront communiqués, par exemple : <ul style="list-style-type: none"> certaines utilisations à des fins de protection ou de défense de la population; certaines utilisations à des fins de santé ou de sécurité publique; communication autorisée ou exigée par la loi. Les fins décrites dans l'avis devraient être formulées de manière telle que l'individu puisse raisonnablement en comprendre la nature et comprendre comment les renseignements personnels seront utilisés. Ces fins doivent être compatibles avec l'activité de l'entité et ne pas être trop générales. Il y aurait lieu d'envisager la remise

Section	Critères relatifs aux avis	Exemples de contrôle et de procédures	Autres considérations
	recueillis auprès d'autres sources que l'individu, celles-ci sont décrites dans l'avis.	entrevue téléphonique, dans un formulaire de demande ou un questionnaire, ou encore par voie électronique). Toutefois, l'avis écrit est la méthode privilégiée.	d'un résumé de l'avis renfermant des liens avec les parties détaillées de la politique de protection des renseignements personnels.
2.2	Procédures et contrôles		
2.2.1	<p>Moment auquel l'avis est donné</p> <p>L'individu est avisé des politiques et procédures de l'entité en matière de protection des renseignements personnels, soit a) au moment où les renseignements personnels sont recueillis ou avant, ou dès que possible par la suite, soit b) au moment où l'entité modifie ses politiques et procédures relatives à la protection des renseignements personnels ou avant, ou dès que possible par la suite, soit c) avant que des renseignements personnels soient utilisés à des fins qui n'avaient pas été indiquées antérieurement.</p>	<p>L'avis sur la protection des renseignements personnels :</p> <ul style="list-style-type: none"> est aisément accessible et peut être consulté la première fois que des renseignements personnels sont recueillis auprès de l'individu; est donné en temps opportun (au moment où les renseignements personnels sont recueillis ou avant, ou dès que possible par la suite) de façon que les individus aient la possibilité de décider s'ils veulent donner des renseignements personnels à l'entité; est daté clairement, de façon que les individus puissent déterminer si l'avis a été modifié depuis la dernière fois qu'ils l'ont lu ou ont donné des renseignements personnels à l'entité. <p>De plus, l'entité :</p> <ul style="list-style-type: none"> fait le suivi de l'évolution de ses politiques et procédures relatives à la protection des renseignements personnels; informe les individus de tout changement apporté à un avis antérieurement diffusé au sujet de la protection des renseignements personnels, en en faisant état sur le 	<p>(Voir la section 3.2.2, «Consentement à de nouvelles fins et à de nouvelles utilisations»).</p> <p>Certaines dispositions légales énoncent qu'un avis sur la protection des renseignements personnels doit être donné à intervalles réguliers – par exemple, une fois l'an dans le cas de la Loi Gramm-Leach-Bliley (LGLB).</p>

Section	Critères relatifs aux avis	Exemples de contrôle et de procédures	Autres considérations
		<p>site Web de l'entité, en transmettant un avis écrit par voie postale ou en envoyant un courriel;</p> <p>tient des documents indiquant la communication aux individus des changements apportés aux politiques et procédures relatives à la protection des renseignements personnels.</p>	
2.2.2.	<p>Entités et activités visées</p> <p>L'avis diffusé par l'entité au sujet de la protection des renseignements personnels comprend une description objective des entités et des activités visées par les politiques et procédures.</p>	<p>L'avis sur la protection des renseignements personnels décrit les entités, les unités d'exploitation, les endroits et les types de renseignements visés, par exemple :</p> <ul style="list-style-type: none"> les territoires d'activité (sur les plans juridique et politique); les unités d'exploitation et les entités affiliées; les branches d'activité; les types de tiers (par exemple, sociétés de livraison et autres types de fournisseurs de services); les types de renseignements (par exemple, renseignements sur les clients et les clients potentiels); les sources d'information (par exemple, commande postale ou en ligne). <p>L'entité informe les individus qu'ils ne sont plus visés par les politiques et procédures relatives à la protection des renseignements personnels lorsqu'ils pourraient supposer le contraire (par exemple, s'ils accèdent à un site Web similaire à celui de l'entité ou s'ils utilisent des services fournis par des</p>	

Section	Critères relatifs aux avis	Exemples de contrôle et de procédures	Autres considérations
2.2.3	<p>Clarté et visibilité L'avis donné par l'entité au sujet de la protection des renseignements personnels est bien visible et rédigé en termes clairs.</p>	<p>tiers dans les installations de l'entité).</p> <p>L'avis sur la protection des renseignements personnels :</p> <ul style="list-style-type: none"> est rédigé en termes clairs et simples; est affiché d'une façon adéquate, est bien visible et n'est pas rédigé en caractères inhabituellement petits; est affiché sur le site Web, aux emplacements où les renseignements sont recueillis, ou fait l'objet d'un lien placé à ces emplacements; est fourni dans les différentes langues utilisées sur le site ou dans les langues rendues obligatoires par la loi. 	<p>Si l'on utilise plusieurs avis pour les différentes filiales ou les différents secteurs d'exploitation d'une entité, le recours à une présentation similaire est encouragé afin de ne pas semer la confusion chez les consommateurs et de leur permettre de noter les éventuelles différences entre les avis.</p> <p>Certains textes prévoient que l'avis doit comporter des informations bien précises.</p> <p>Des exemples d'avis existent dans bien des cas pour certains secteurs d'activité et certains types de collecte, d'utilisation, de conservation et de communication.</p>

Choix et consentement

Section	Critères relatifs au choix et au consentement	Exemples de contrôles et de procédures	Autres considérations
3.0	L'entité décrit le choix offert à l'individu et obtient son consentement implicite ou explicite quant à la collecte, à l'utilisation et à la communication de renseignements personnels.		
3.1	Politiques et communications		
3.1.0	Politiques de protection des renseignements personnels Les politiques de l'entité en matière de protection des renseignements personnels décrivent le choix offert aux individus et la nature du consentement à obtenir.		
3.1.1	Communication aux individus Les individus sont informés a) du choix qui leur est offert quant à la collecte, à l'utilisation et à la communication de renseignements personnels à leur sujet et b) du fait que leur consentement implicite ou explicite est nécessaire pour la collecte, l'utilisation et la communication de renseignements personnels, sauf dispositions légales ou réglementaires contraires.	L'avis donné par l'entité au sujet de la protection des renseignements personnels précise, d'une manière claire et concise, les points suivants : <ul style="list-style-type: none"> le choix offert à l'individu quant à la collecte, à l'utilisation et à la communication de renseignements personnels à son sujet; la marche à suivre par l'individu pour exercer ce choix (par exemple, cocher une case pour indiquer qu'il refuse de recevoir du matériel publicitaire); la capacité pour l'individu de modifier ses préférences et la marche à suivre; les conséquences si les renseignements personnels requis en lien avec une opération ou un service ne sont pas donnés. Les individus sont avisés des faits suivants :	Certaines dispositions légales et réglementaires (comme le principe 11, «Limites relatives à la communication de renseignements personnels», article 1 de la loi australienne de 1988 sur la protection des renseignements personnels) prévoient d'une manière spécifique des cas où l'entité n'est pas tenue d'obtenir le consentement de l'individu. Voici deux exemples : <ul style="list-style-type: none"> celui qui détient les renseignements estime, pour des motifs raisonnables, que l'utilisation des renseignements à une autre fin est nécessaire pour prévenir ou atténuer une menace sérieuse et imminente à la vie ou à la santé de l'individu concerné ou d'une autre personne; l'utilisation des renseignements à une autre fin est exigée ou autorisée par la loi.

Section	Critères relatifs au choix et au consentement	Exemples de contrôles et de procédures	Autres considérations
		<p>ils n'ont pas à donner les renseignements personnels non essentiels aux fins mentionnées dans l'avis sur la protection des renseignements personnels;</p> <p>il est possible de modifier ultérieurement les préférences exprimées et de retirer son consentement, sous réserve des restrictions légales ou contractuelles et d'un préavis raisonnable.</p> <p>Le type de consentement exigé dépend de la nature des renseignements personnels et de la méthode de collecte (par exemple, l'individu qui s'abonne à un bulletin consent implicitement à recevoir des communications de l'entité).</p>	
3.1.2	<p>Conséquences d'un refus ou d'un retrait de consentement</p> <p>Au moment de la collecte de renseignements, les individus sont informés des conséquences du refus de donner des renseignements, ainsi que du refus ou du retrait de consentement à l'utilisation de renseignements personnels aux fins mentionnées dans l'avis.</p>	<p>Au moment de la collecte, l'entité donne aux individus les informations suivantes :</p> <ul style="list-style-type: none"> les conséquences du refus de donner des renseignements (par exemple, des opérations pourraient ne pas être traitées); les conséquences du refus ou du retrait de consentement (par exemple, si on choisit de ne pas recevoir d'information sur des produits et services, on pourra ne pas être mis au courant des promotions de ventes); la manière dont ils seront touchés ou non, le cas échéant, s'ils ne donnent pas davantage de renseignements que le minimum demandé (par exemple, des services ou des 	

Section	Critères relatifs au choix et au consentement	Exemples de contrôles et de procédures	Autres considérations
		produits seront tout de même livrés).	
3.2	Procédures et contrôles		
3.2.1	<p>Consentement implicite ou explicite Le consentement implicite ou explicite de l'individu est obtenu au moment où les renseignements personnels sont recueillis ou avant, ou alors peu après. Les préférences exprimées par l'individu au moyen de son consentement sont confirmées et il y est donné suite.</p>	<p>L'entité :</p> <ul style="list-style-type: none"> obtient et consigne en temps opportun le consentement donné par l'individu (à savoir, au moment où les renseignements personnels sont recueillis ou avant, ou encore peu après); confirme (par écrit ou par voie électronique) les préférences exprimées par l'individu; consigne et gère les changements apportés aux préférences exprimées par un individu; veille à ce qu'il soit donné suite en temps opportun aux préférences exprimées par l'individu; règle les éventuelles contradictions existant dans les dossiers quant aux préférences exprimées par un individu par la mise en place d'un processus permettant aux utilisateurs de signaler et de contester l'interprétation de leurs préférences par un fournisseur; veille à ce que l'utilisation des renseignements personnels, au sein de l'entité et par des tiers, respecte les préférences exprimées par l'individu. 	
3.2.2	<p>Consentement à de nouvelles fins et à de nouvelles utilisations Si des renseignements antérieurement recueillis doivent être utilisés à des fins</p>	<p>Lorsqu'elle doit utiliser des renseignements personnels à des fins non mentionnées antérieurement, l'entité :</p>	

Section	Critères relatifs au choix et au consentement	Exemples de contrôles et de procédures	Autres considérations
	<p>qui n'étaient pas mentionnées dans l'avis sur la protection des renseignements personnels, ces nouvelles fins sont consignées, l'individu est avisé et son consentement implicite ou explicite est obtenu avant toute utilisation des renseignements à ces fins.</p>	<p>en avise l'individu et consigne les nouvelles fins; obtient et consigne le consentement ou le retrait du consentement à l'utilisation des renseignements personnels aux nouvelles fins; s'assure que les renseignements personnels sont utilisés en conformité avec les nouvelles fins ou que, si le consentement a été retiré, les renseignements ne sont pas utilisés à ces fins.</p>	
3.2.3	<p>Consentement explicite dans le cas des renseignements personnels sensibles Un consentement explicite est obtenu directement de l'individu lorsque des renseignements personnels sensibles sont recueillis, utilisés ou communiqués, sauf dispositions légales ou réglementaires spécifiques contraires.</p>	<p>L'entité recueille des renseignements sensibles seulement si l'individu donne un <i>consentement explicite</i>. Le consentement explicite suppose que l'individu accepte, par une action quelconque, l'utilisation ou la communication des renseignements sensibles. Le consentement explicite est obtenu directement auprès de l'individu et est consigné – par exemple, on exige de l'individu qu'il coche une case ou qu'il signe un formulaire. En anglais, on utilise parfois l'expression <i>opt-in</i>.</p>	<p>Selon l'article 4.3.6 de l'Annexe 1 de la <i>Loi sur la protection des renseignements personnels et les documents électroniques</i> (LPRPDE) du Canada, l'organisation doit en général chercher à obtenir un consentement explicite lorsque les renseignements sont susceptibles d'être considérés comme sensibles.</p> <p>Nombre de ressorts territoriaux interdisent la collecte de renseignements sensibles, à moins que ladite collecte soit expressément autorisée. Par exemple, l'article 7 de la <i>Loi sur la protection des individus à l'égard du traitement des données à caractère personnel</i> de la Grèce, État membre de l'UE, précise que la collecte et le traitement des données sensibles sont interdits. Toutefois, il est possible d'obtenir un permis pour recueillir et traiter des données sensibles.</p> <p>Certains ressorts territoriaux considèrent que les moyens</p>

Section	Critères relatifs au choix et au consentement	Exemples de contrôles et de procédures	Autres considérations
			d'identification d'origine gouvernementale (comme les numéros de sécurité sociale ou d'assurance sociale) constituent des renseignements sensibles.
3.2.4	<p>Consentement relatif au transfert en ligne de données à l'ordinateur (ou à un autre appareil électronique similaire) d'un individu ou à partir de celui-ci</p> <p>Le consentement est obtenu avant que des renseignements personnels soient transférés à l'ordinateur (ou à un autre appareil électronique similaire) d'un individu ou à partir de celui-ci.</p>	<p>L'entité demande au client la permission de stocker, de modifier ou de copier des renseignements personnels, autres que des témoins (<i>cookies</i>), dans l'ordinateur (ou un autre appareil électronique similaire) d'un client.</p> <p>Si le client a indiqué à l'entité qu'il ne voulait pas que des témoins soient utilisés, l'entité dispose de contrôles visant à faire en sorte que des témoins ne soient pas laissés dans l'ordinateur (ou un autre appareil électronique similaire) du client.</p> <p>Les entités ne téléchargent pas des logiciels servant à transférer des renseignements personnels sans avoir obtenu une permission à cette fin.</p>	Il y aurait lieu d'envisager d'empêcher ou de détecter l'introduction de logiciels conçus pour extraire des renseignements d'un ordinateur (ou d'un autre appareil électronique similaire) et qui peuvent par conséquent être utilisés pour extraire des renseignements personnels (les logiciels espions, par exemple).

Collecte

Section	Critères relatifs à la collecte	Exemples de contrôles et de procédures	Autres considérations
4.0	L'entité ne recueille des renseignements personnels qu'aux fins mentionnées dans l'avis.		
4.1	Politiques et communications		
4.1.0	Politiques de protection des renseignements personnels Les politiques de l'entité en matière de protection des renseignements personnels traitent de la collecte de renseignements personnels.		Certains ressorts territoriaux, comme certains pays d'Europe, exigent que les entités qui recueillent des renseignements personnels s'inscrivent auprès de leur organisme de réglementation.
4.1.1	Communication aux individus LES INDIVIDUS SONT INFORMÉS QUE LES RENSEIGNEMENTS PERSONNELS SONT UNIQUEMENT RECUEILLIS AUX FINS MENTIONNÉES DANS L'AVIS.	L'avis de l'entité sur la protection des renseignements personnels fait état des types de renseignements personnels recueillis, des sources et des méthodes utilisées pour les recueillir et il précise si des renseignements sont approfondis ou si des renseignements supplémentaires sont obtenus auprès de tiers, par exemple pour dresser leur profil d'achat.	
4.1.2	Types de renseignements personnels recueillis et méthodes de collecte Les types de renseignements personnels recueillis et les méthodes de collecte, y compris l'utilisation de témoins ou d'autres procédés de suivi similaires, sont consignés et décrits dans l'avis sur la protection des renseignements personnels.	Voici notamment les types de renseignements personnels recueillis : renseignements financiers (par exemple, relatifs à un compte financier); renseignements ayant trait à la santé (par exemple, relatifs à la santé physique ou mentale ou aux antécédents dans ces domaines); renseignements démographiques (ayant trait par exemple à l'âge, à la fourchette de revenu, aux codes de géographie sociale). Voici notamment quelles sont les méthodes de collecte et les sources	Certains ressorts territoriaux, comme ceux de l'Union européenne, exigent que les individus aient la possibilité de refuser l'utilisation de témoins.

Section	Critères relatifs à la collecte	Exemples de contrôles et de procédures	Autres considérations
		<p>tierces de renseignements personnels : agences d'évaluation du crédit; téléphone; Internet, à l'aide de formulaires, de témoins ou de pixels invisibles.</p> <p>L'avis de l'entité sur la protection des renseignements personnels indique si des témoins ou des pixels invisibles sont utilisés, et la façon dont ils le sont. L'avis décrit également les conséquences d'un refus du témoin.</p>	
4.2	Procédures et contrôles		
4.2.1	<p>Limitation de la collecte aux fins mentionnées</p> <p>La collecte de renseignements personnels est limitée à ce qu'exigent les fins mentionnées dans l'avis.</p>	<p>On a mis en place des systèmes et des procédures pour :</p> <ul style="list-style-type: none"> indiquer quels sont les renseignements personnels essentiels aux fins mentionnées dans l'avis et les distinguer des renseignements personnels facultatifs; revoir périodiquement la nécessité d'obtenir des renseignements personnels dans le cadre du programme ou du service de l'entité (par exemple, une fois tous les cinq ans ou lorsque des changements sont apportés au programme ou au service); obtenir un consentement explicite lorsque des renseignements personnels sensibles sont recueillis (voir la section 3.2.3, «Consentement explicite dans le cas des renseignements personnels sensibles»); vérifier que la collecte de renseignements personnels est 	

Section	Critères relatifs à la collecte	Exemples de contrôles et de procédures	Autres considérations
		limitée à ce qui est nécessaire aux fins mentionnées dans l’avis sur la protection des renseignements personnels, et que toutes les données facultatives sont indiquées comme telles.	
4.2.2	<p>Utilisation de moyens loyaux et conformes à la loi pour la collecte</p> <p>Les méthodes utilisées pour la collecte de renseignements personnels sont examinées par la direction avant d’être instaurées, dans le but de s’assurer que les renseignements personnels sont obtenus a) d’une manière loyale, sans intimidation ni tromperie et b) d’une manière conforme à la loi – dans le respect de toutes les règles de droit applicables concernant la collecte de renseignements personnels, qu’elles découlent d’un texte législatif ou de la common law.</p>	La direction, le responsable de la PRP et le conseiller juridique de l’entité vérifient les méthodes de collecte et les changements qui y sont apportés le cas échéant.	<p>Peuvent être considérées comme des pratiques trompeuses :</p> <ul style="list-style-type: none"> le fait d’utiliser des outils, tels que des témoins et des pixels invisibles, sur le site Web de l’entité afin de recueillir des renseignements personnels sans en aviser l’individu; le fait d’associer des renseignements recueillis lors de la visite d’un individu sur un site Web à des renseignements personnels provenant d’autres sources sans en aviser l’individu; le fait d’avoir recours à un <u>tiers</u> pour recueillir des renseignements de façon à éviter d’avoir à donner un avis aux individus. <p>Les entités devraient tenir compte des exigences légales et réglementaires en vigueur dans les ressorts territoriaux autres que celui où elles exercent leurs activités (par exemple, il se peut qu’une entité exploitée au Canada recueille des renseignements personnels au sujet d’Européens et doive se soumettre à certaines exigences légales en vigueur en Europe).</p> <p>L’examen des plaintes peut aider à déceler l’existence de pratiques déloyales ou non conformes à la loi.</p>

Section	Critères relatifs à la collecte	Exemples de contrôles et de procédures	Autres considérations
4.2.3	<p>Collecte de renseignements auprès de tiers La direction confirme que les tiers auprès desquels des renseignements sont recueillis (à savoir, des sources autres que l'individu concerné) sont des sources fiables qui recueillent des renseignements d'une manière loyale et conforme à la loi.</p>	<p>L'entité :</p> <ul style="list-style-type: none"> effectue les vérifications qui s'imposent avant d'établir une relation avec un tiers devant lui fournir des données; examine les politiques des tiers en matière de protection des renseignements personnels, leurs méthodes de collecte de renseignements et les types de consentements obtenus avant d'accepter des renseignements personnels de leur part. 	<p>Les contrats renferment des clauses selon lesquelles les renseignements doivent être recueillis auprès de sources fiables, d'une façon loyale et conforme à la loi.</p>
4.2.4	<p>Approfondissement des renseignements personnels L'entité informe les individus lorsqu'elle approfondit les renseignements qu'ils lui fournissent ou obtient des renseignements supplémentaires sur eux pour son propre usage.</p>	<p>L'avis sur la protection des renseignements personnels de l'entité indique que, s'il y a lieu, elle peut approfondir les renseignements fournis ou obtenir des renseignements supplémentaires auprès de sources tierces sur l'historique de navigation, de crédit, d'achat, etc. de l'individu.</p>	

Utilisation, conservation et suppression

Section	Critères relatifs à l'utilisation, à la conservation et à la suppression	Exemples de contrôles et de procédures	Autres considérations
5.0	L'entité limite l'utilisation de renseignements personnels aux fins mentionnées dans l'avis, à l'égard desquelles l'individu a donné son consentement implicite ou explicite. L'entité ne conserve les renseignements personnels que pendant le temps nécessaire pour la réalisation des fins mentionnées ou selon les dispositions légales ou réglementaires et elle les détruit ensuite de façon adéquate.		
5.1	Politiques et communications		
5.1.0	Politiques de protection des renseignements personnels Les politiques de l'entité en matière de protection des renseignements personnels traitent de l'utilisation, de la conservation et de la suppression des renseignements personnels.		
5.1.1	Communication aux individus Les individus sont informés que les renseignements personnels a) ne sont utilisés qu'aux fins mentionnées dans l'avis, et seulement si l'individu a donné son consentement implicite ou explicite, sauf dispositions légales ou réglementaires spécifiques contraires b) ne sont pas conservés plus longtemps qu'il n'est nécessaire pour la réalisation des fins mentionnées, ou que la période expressément prévue par une loi ou un règlement et c) sont détruits d'une façon qui empêche la perte, le vol, l'utilisation abusive ou l'accès non autorisé.	L'avis de l'entité relatif à la protection des renseignements personnels décrit les fins auxquelles sont utilisés les renseignements personnels, par exemple les suivantes : traitement des opérations commerciales (comme les réclamations et les garanties, la paie, les taxes, les avantages, les options sur actions, les primes et les autres formules de rémunération); traitement des demandes d'information ou des plaintes au sujet de produits ou de services, ou interaction lors de la promotion de produits ou de services; conception et développement de produits, ou acquisition de produits ou de services; participation à des activités de	

Section	Critères relatifs à l'utilisation, à la conservation et à la suppression	Exemples de contrôles et de procédures	Autres considérations
		<p>recherche scientifique ou médicale, commercialisation, sondages ou analyses de marché; personnalisation de sites Web ou téléchargement de logiciels; exigences légales; marketing direct.</p> <p>L'avis de l'entité relatif à la protection des renseignements personnels explique que les renseignements personnels ne seront conservés que pendant le temps nécessaire pour la réalisation des fins mentionnées, ou pendant la période expressément prévue par une loi ou un règlement et qu'ils seront ensuite détruits d'une manière sûre ou désidentifiés de façon à ne pouvoir être rattachés à aucun individu en particulier.</p>	
5.2	Procédures et contrôles		
5.2.1	<p>Utilisation des renseignements personnels Les renseignements personnels ne sont utilisés qu'aux fins mentionnées dans l'avis, et seulement si l'individu a donné son consentement implicite ou explicite, sauf dispositions légales ou réglementaires spécifiques contraires.</p>	<p>L'entité a mis en place des systèmes et procédures afin de s'assurer que les renseignements personnels sont utilisés :</p> <ul style="list-style-type: none"> conformément aux fins mentionnées dans l'avis de l'entité relatif à la protection des renseignements personnels; conformément au consentement donné par l'individu; dans le respect de toutes les lois et tous les règlements applicables. 	<p>Certains textes comme la LGLB, la <i>Health Insurance Portability and Accountability Act</i> (HIPAA) et la <i>Children's Online Privacy Protection Act</i> (COPPA) contiennent des dispositions portant spécifiquement sur l'utilisation des renseignements personnels.</p>
5.2.2	<p>Conservation des renseignements personnels Les renseignements personnels ne sont pas conservés plus longtemps qu'il</p>	<p>L'entité :</p> <ul style="list-style-type: none"> consigne ses politiques de conservation et de suppression des 	<p>Certaines lois précisent la durée de conservation des renseignements personnels. Ainsi, la HIPAA fixe des obligations de conservation en relation</p>

Section	Critères relatifs à l'utilisation, à la conservation et à la suppression	Exemples de contrôles et de procédures	Autres considérations
	<p>n'est nécessaire pour la réalisation des fins mentionnées, sauf dispositions légales ou réglementaires spécifiques contraires.</p>	<p>renseignements personnels; conserve, stocke et élimine les copies de fichiers archivées et de sauvegarde en conformité avec ses politiques de conservation; fait en sorte qu'aucun renseignement personnel ne soit conservé au-delà de la durée normale de conservation à moins que cela ne soit justifié pour un motif commercial ou légal.</p> <p>On tient compte des obligations contractuelles pour établir les pratiques de conservation lorsque celles-ci risquent de faire exception aux pratiques normales.</p>	<p>avec la responsabilité de fournir des renseignements personnels sur l'état de santé : trois ans dans le cas de dossiers de santé électroniques et six ans dans le cas de dossiers de santé non électroniques.</p> <p>D'autres textes législatifs peuvent prévoir des obligations de conservation; par exemple, il peut être nécessaire de conserver certaines données à des fins fiscales ou en vertu de la législation sur l'emploi.</p>
5.2.3	<p>Suppression, destruction et caviardage des renseignements personnels Les renseignements personnels qui cessent d'être conservés sont désidentifiés, supprimés ou détruits d'une manière qui empêche la perte, le vol, l'utilisation abusive et l'accès non autorisé.</p>	<p>L'entité efface ou détruit les dossiers selon ses politiques de conservation, quelle que soit la méthode de stockage (par exemple, média électronique, optique ou sur papier) détruit les originaux, les exemplaires archivés, en double et ponctuels ou personnels, conformément à ses politiques de conservation; consigne par écrit la suppression des renseignements personnels; dans les limites de la technologie, repère et supprime ou caviarde selon ce qui est obligatoire certains renseignements personnels au sujet d'un individu – par</p>	<p>Il faut envisager de faire appel aux services de sociétés spécialisées dans la destruction sûre des renseignements personnels. Certaines de ces sociétés peuvent fournir un certificat de destruction au besoin.</p> <p>Il peut arriver que certains supports d'archivage, tels que les DVD, les CD, les microfilms ou les microfiches ne permettent pas la suppression de dossiers individuels, sinon par la destruction de l'ensemble de la base de données contenue sur de tels supports.</p>

Section	Critères relatifs à l'utilisation, à la conservation et à la suppression	Exemples de contrôles et de procédures	Autres considérations
		<p>exemple, le numéro de carte de crédit une fois l'opération effectuée; détruit, efface ou désidentifie à intervalles réguliers et systématiquement les renseignements personnels qui ne sont plus nécessaires pour la réalisation des fins mentionnées ou dont la conservation n'est plus exigée par une loi ou un règlement.</p> <p>On tient compte des obligations contractuelles pour établir les pratiques de suppression, de destruction et de caviardage lorsque celles-ci risquent de faire exception aux politiques normales de l'entité.</p>	

Accès

Section	Critères relatifs à l'accès	Exemples de contrôles et de procédures	Autres considérations
6.0	L'entité donne aux individus accès aux renseignements personnels les concernant, pour qu'ils puissent les examiner et les mettre à jour.		
6.1	Politiques et communications		
6.1.0	Politiques de protection des renseignements personnels Les politiques de l'entité en matière de protection des renseignements personnels font état de la nécessité de donner aux individus accès aux renseignements personnels les concernant.		
6.1.1	Communication aux individus Les individus sont informés de la façon dont ils peuvent avoir accès aux renseignements personnels les concernant afin de les examiner, de les mettre à jour et de les rectifier.	L'avis de l'entité relatif à la protection des renseignements personnels : explique la façon dont les individus peuvent avoir accès aux renseignements personnels les concernant ainsi que les coûts à engager à cet égard le cas échéant; décrit la façon dont les individus peuvent mettre à jour et rectifier les renseignements personnels les concernant (par exemple, par écrit, par téléphone, par courriel ou par le truchement du site Web de l'entité); explique comment il est possible de régler les désaccords survenant au sujet de renseignements personnels.	
6.2	Procédures et contrôles		
6.2.1	Accès des individus aux renseignements personnels les concernant	L'entité a mis en place des procédures pour : déterminer si elle détient des	Certains textes légaux et réglementaires : contiennent des dispositions et des

Section	Critères relatifs à l'accès	Exemples de contrôles et de procédures	Autres considérations
	<p>Les individus peuvent vérifier si l'entité possède des renseignements personnels à leur sujet et peuvent, sur demande, avoir accès à ces renseignements.</p>	<p>renseignements personnels sur un individu ou exerce un contrôle à leur égard; communiquer la marche à suivre pour avoir accès aux renseignements personnels; répondre en temps utile à la demande d'un individu; fournir sur demande une copie des renseignements personnels sur un support papier ou électronique qui est pratique pour l'individu comme pour l'entité; consigner les demandes d'accès et les réponses, y compris les refus et les plaintes et contestations non résolus.</p>	<p>exigences quant à l'accès aux renseignements personnels (c'est notamment le cas de la HIPAA); précisent que les demandes d'accès à des renseignements personnels doivent être présentées par écrit.</p>
6.2.2	<p>Confirmation de l'identité d'un individu On contrôle l'identité des individus qui demandent accès aux renseignements personnels les concernant avant d'accéder à leur demande.</p>	<p>Les employés reçoivent une formation adéquate pour être en mesure de contrôler l'identité des individus avant de leur accorder les possibilités suivantes :</p> <ul style="list-style-type: none"> accès aux renseignements personnels les concernant; modification de renseignements sensibles ou d'autres renseignements personnels (par exemple, mise à jour de l'adresse ou des coordonnées bancaires). <p>L'entité :</p> <ul style="list-style-type: none"> n'utilise, pour effectuer le contrôle d'identité, aucun identificateur émanant des pouvoirs publics (numéros d'assurance sociale ou de sécurité sociale, par exemple); ne poste l'information sur une 	<p>La rigueur du contrôle d'identité est fonction du type de renseignements personnels auxquels accès est donné ainsi que de leur sensibilité. Différentes techniques peuvent être envisagées selon les différents canaux, notamment :</p> <ul style="list-style-type: none"> Web; système de réponse vocale interactive; centre d'appels; en personne.

Section	Critères relatifs à l'accès	Exemples de contrôles et de procédures	Autres considérations
		<p>demande de changement qu'à l'adresse figurant au dossier ou, dans le cas d'un changement d'adresse, la poste à l'ancienne et à la nouvelle;</p> <p>exige que l'accès en ligne à des renseignements sur un compte utilisateur nécessite l'emploi d'un identificateur d'utilisateur et d'un mot de passe (ou l'équivalent) uniques.</p>	
6.2.3	<p>Compréhensibilité des renseignements personnels, délai de communication et coût</p> <p>Les renseignements personnels sont donnés à l'individu sous une forme compréhensible, dans un délai raisonnable et gratuitement ou à un coût raisonnable.</p>	<p>L'entité :</p> <ul style="list-style-type: none"> donne les renseignements personnels à l'individu sous une forme compréhensible (par exemple, pas sous forme de code ou de série de nombres, ni dans une langue abusivement technique ou un jargon quelconque) et sur un support qui est pratique pour l'individu comme pour l'entité; fait des efforts raisonnables pour localiser les renseignements personnels demandés et, si elle est incapable de trouver des renseignements personnels, conserve des pièces suffisantes pour prouver que des recherches raisonnables ont été effectuées; prend des précautions raisonnables pour s'assurer que les renseignements personnels communiqués ne révèlent pas, directement ou indirectement, l'identité d'une autre personne; donne accès aux renseignements personnels dans un délai semblable 	<p>Les entités peuvent donner aux individus accès aux renseignements personnels les concernant, gratuitement ou à un coût minime, pour en tirer potentiellement des avantages sur le plan de la relation qu'elles entretiennent avec leur clientèle, ainsi que pour avoir l'opportunité d'accroître la qualité des renseignements qu'elles détiennent.</p>

Section	Critères relatifs à l'accès	Exemples de contrôles et de procédures	Autres considérations
		<p>au délai normal de réponse de l'entité dans le cas d'autres opérations commerciales, ou selon ce que la loi autorise ou exige;</p> <p>donne accès à des renseignements personnels contenus dans des systèmes et supports d'archives ou de sauvegarde;</p> <p>informe les individus du coût de l'accès au moment où la demande d'accès est présentée, ou dès que possible par la suite;</p> <p>exige de l'individu, pour l'accès aux renseignements personnels, une somme qui n'est pas excessive par rapport au coût engagé par l'entité pour donner cet accès, ou le lui donne gratuitement;</p> <p>met à la disposition de l'individu un lieu physique adéquat où il pourra examiner les renseignements personnels.</p>	
6.2.4	<p>Refus d'accès</p> <p>Les individus sont informés, par écrit, de la raison pour laquelle une demande d'accès aux renseignements personnels les concernant a été refusée, de la source du droit de l'entité de refuser cet accès, le cas échéant, et du droit de l'individu, éventuellement, de contester ce refus, selon ce qui est expressément permis ou exigé par une loi ou un règlement.</p>	<p>L'entité :</p> <p>expose brièvement les raisons pour lesquelles elle peut refuser l'accès à des renseignements personnels;</p> <p>consigne tous les refus d'accès ainsi que les plaintes et contestations non résolus;</p> <p>donne à l'individu un accès partiel aux renseignements dans les cas où elle peut à bon droit lui refuser l'accès à certains renseignements personnels le concernant;</p> <p>explique par écrit à l'individu les raisons pour lesquelles on lui refuse l'accès à des renseignements</p>	<p>Certaines lois et certains règlements (par exemple, dans la loi australienne de 1988 sur la protection des renseignements personnels, le principe 5 énoncé au point 2, et dans la LPRPDE, les paragraphes 8. (4), 8. (5) et 8. (7), et les articles 9, 10 et 28) indiquent les cas dans lesquels l'individu peut se voir refuser l'accès aux renseignements, la marche à suivre (par exemple, informer le client par écrit du refus d'accès dans les trente jours suivant la demande), et les pénalités et sanctions potentielles auxquelles s'expose l'entité qui ne se</p>

Section	Critères relatifs à l'accès	Exemples de contrôles et de procédures	Autres considérations
		<p>personnels; prévoit une procédure hiérarchique officielle (et une possibilité d'appel) lorsque l'accès aux renseignements personnels est refusé; fait état des droits conférés à l'entité par la loi ainsi que du droit de l'individu de contester le refus, le cas échéant.</p>	<p>conforme pas à ces dispositions.</p>
6.2.5	<p>Mise à jour ou rectification de renseignements personnels Les individus peuvent mettre à jour ou rectifier les renseignements personnels détenus par l'entité. Si la chose est possible sur les plans économique et pratique, l'entité fournit les renseignements ainsi mis à jour ou rectifiés aux tiers à qui des renseignements personnels concernant l'individu avaient été antérieurement fournis.</p>	<p>L'entité :</p> <ul style="list-style-type: none"> décrit la marche à suivre par l'individu qui veut mettre à jour ou rectifier des dossiers de renseignements personnels (par exemple, par écrit, par téléphone, par courriel ou en utilisant le site Web de l'entité); s'assure que les renseignements personnels mis à jour ou modifiés par un individu sont exacts et complets (par exemple, par des contrôles de modification et de validation, et au moyen de champs dont la saisie est obligatoire); consigne la date, l'heure et l'identité de la personne qui effectue le changement, si un employé de l'entité effectue le changement pour le compte d'un individu; avise les tiers à qui des renseignements personnels ont été communiqués des modifications, suppressions ou blocages de renseignements personnels, si la chose s'avère possible et raisonnable. 	<p>Certaines lois (par exemple, la LPRPDE, articles 4.5.2 et 4.5.3 de l'Annexe 1) interdisent la suppression de renseignements personnels, l'entité étant cependant tenue de cesser tout traitement de ces renseignements.</p>

Section	Critères relatifs à l'accès	Exemples de contrôles et de procédures	Autres considérations
6.2.6	<p>Déclaration de désaccord Les individus sont informés, par écrit, de la raison pour laquelle leur demande de rectification de renseignements personnels a été refusée, ainsi que de la façon dont ils peuvent faire appel de ce refus.</p>	<p>En cas de désaccord entre un individu et une entité sur le caractère complet et exact de renseignements personnels, l'individu peut demander à l'entité d'accepter une déclaration dans laquelle il fait valoir que les renseignements personnels ne sont pas complets et exacts.</p> <p>L'entité :</p> <ul style="list-style-type: none"> consigne en dossier les cas où un individu et elle ne sont pas du même avis au sujet du caractère complet et exact des renseignements personnels; informe l'individu, par écrit, de la raison pour laquelle une demande de rectification de renseignements personnels est refusée, en faisant état du droit d'appel dont dispose l'individu; informe l'individu, lorsque l'accès aux renseignements personnels est demandé ou lorsqu'il est donné, que la déclaration de désaccord peut comporter des précisions sur la nature du changement souhaité par l'individu et mentionner la raison pour laquelle l'entité refuse de l'effectuer; si la chose est indiquée, avise du désaccord, en en précisant la nature, les tiers à qui les renseignements personnels ont été communiqués antérieurement. 	<p><u>VOIR LES SECTIONS 10.1.1, «COMMUNICATION AUX INDIVIDUS», 10.2.1, «PROCESSUS APPLICABLE À L'ÉGARD DES DEMANDES D'INFORMATION, DES PLAINTES ET DES CONTESTATIONS», ET 10.2.2, «RÈGLEMENT DES CONTESTATIONS ET RECOURS».</u></p> <p>Certaines lois (dont la HIPAA) établissent des exigences spécifiques au chapitre des refus de changement et des mesures à prendre à l'égard des désaccords exprimés par des individus.</p> <p>Si une contestation n'est pas réglée d'une façon jugée satisfaisante par l'individu, l'existence de cette contestation, lorsque cela est opportun, est communiquée aux tiers ayant accès aux renseignements en cause.</p>

Communication à des tiers

Section	Critères relatifs à la communication à des tiers	Exemples de contrôles et de procédures	Autres considérations
7.0	L'entité ne communique des renseignements personnels à des tiers qu'aux fins mentionnées dans l'avis, et avec le consentement implicite ou explicite de l'individu.		
7.1	Politiques et communications		
7.1.0	Politiques de protection des renseignements personnels Les politiques de l'entité en matière de protection des renseignements personnels traitent de la communication des renseignements personnels à des tiers.		
7.1.1	Communication aux individus Les individus sont informés que des renseignements personnels ne sont communiqués à des tiers qu'aux fins mentionnées dans l'avis, et qu'avec le consentement implicite ou explicite de l'individu, sauf dispositions légales ou réglementaires spécifiques contraires.	L'avis de l'entité relatif à la protection des renseignements personnels : <ul style="list-style-type: none"> décrit, le cas échéant, les pratiques en matière de partage des renseignements personnels avec des tiers et les raisons motivant ce partage; identifie les tiers ou les catégories de tiers auxquels des renseignements personnels sont communiqués; informe les individus que des renseignements personnels sont communiqués à des tiers seulement aux fins : 1) qui sont mentionnées dans l'avis et 2) à l'égard desquelles l'individu a donné son consentement implicite ou explicite, ou selon ce qui est expressément autorisé ou exigé par une loi ou un règlement. 	L'avis de l'entité relatif à la protection des renseignements personnels peut indiquer : <ul style="list-style-type: none"> le processus par lequel on assure la confidentialité et la sécurité des renseignements personnels qui ont été communiqués à un tiers; comment les renseignements personnels partagés avec un tiers seront mis à jour, de façon que les renseignements périmés ou incorrects partagés avec un tiers soient modifiés si l'individu a apporté des modifications aux renseignements le concernant.
7.1.2	Communication des politiques aux	Avant de partager des renseignements	

Section	Critères relatifs à la communication à des tiers	Exemples de contrôles et de procédures	Autres considérations
	<p>tiers Les politiques de protection des renseignements personnels ou d'autres instructions ou obligations spécifiques relatives au traitement des renseignements personnels sont communiquées aux tiers à qui des renseignements personnels sont communiqués.</p>	<p>personnels avec des tiers, l'entité leur communique ses politiques de PRP ou d'autres instructions ou obligations spécifiques relatives au traitement des renseignements personnels et obtient d'eux l'assurance écrite que leurs pratiques de PRP à l'égard de la communication des renseignements personnels respectent ces politiques ou obligations.</p>	
7.2	Procédures et contrôles		
7.2.1	<p>Communication de renseignements personnels Les renseignements personnels ne sont communiqués à des tiers qu'aux fins mentionnées dans l'avis et à l'égard desquelles l'individu a donné son consentement implicite ou explicite, sauf dispositions légales ou réglementaires spécifiques contraires.</p>	<p>L'entité a mis en place des systèmes et des procédures pour :</p> <ul style="list-style-type: none"> empêcher la communication de renseignements personnels à des tiers, à moins qu'un individu n'ait donné son consentement implicite ou explicite à cet égard; consigner en dossier la nature et l'étendue des renseignements personnels communiqués à des tiers; s'assurer que la communication à des tiers se fait en conformité avec les politiques et procédures de l'entité en matière de protection des renseignements personnels, ou selon ce qui est expressément autorisé ou exigé par une loi ou un règlement; consigner toute communication à un tiers en vertu de dispositions légales. 	<p>Les renseignements personnels peuvent être communiqués aux autorités policières ou à des organismes de réglementation suivant divers processus légaux.</p> <p>Certaines lois et certains règlements renferment des dispositions spécifiques traitant de la communication des renseignements personnels et permettent la communication de renseignements personnels sans le consentement de l'individu, alors que d'autres exigent un consentement vérifiable.</p>
7.2.2	<p>Protection des renseignements personnels L'entité ne communique des renseignements personnels qu'à des</p>	<p>Lorsqu'elle fournit des renseignements personnels à des tiers, l'entité conclut avec eux une entente visant à garantir un niveau de protection des</p>	<p>L'entité assume la responsabilité des renseignements personnels dont elle a la possession ou la garde, y compris les renseignements qui ont été transmis à</p>

Section	Critères relatifs à la communication à des tiers	Exemples de contrôles et de procédures	Autres considérations
	<p>tiers ayant conclu avec elle des ententes visant à protéger les renseignements personnels en conformité avec les aspects pertinents des politiques de PRP de l'entité ou d'autres instructions ou obligations spécifiques. L'entité s'est dotée de procédures lui permettant d'apprécier si les tiers ont des contrôles efficaces pour satisfaire aux conditions de l'entente, aux instructions ou aux obligations.</p>	<p>renseignements personnels équivalent à celui qu'elle assure. Ce faisant, l'entité restreint l'utilisation par le tiers des renseignements personnels aux fins nécessaires à l'exécution du contrat; communique au tiers les préférences exprimées par l'individu; soumet à un cadre désigné, comme le responsable de la protection des renseignements personnels, toutes les demandes d'accès ou plaintes touchant les renseignements personnels transmis par l'entité; précise de quelle manière et à quel moment les tiers doivent éliminer ou restituer les renseignements personnels communiqués par l'entité.</p> <p>L'entité évalue le respect d'une telle entente par le tiers en utilisant une ou plusieurs des méthodes suivantes afin d'obtenir un degré croissant d'assurance, proportionné à son évaluation des risques :</p> <ul style="list-style-type: none"> le tiers répond à un questionnaire sur ses pratiques; le tiers atteste, sur la base de rapports d'audit interne ou d'autres procédures, que ses pratiques satisfont aux exigences de l'entité; l'entité procède à une inspection chez le tiers; l'entité obtient un audit ou un rapport similaire auprès d'un auditeur indépendant. 	<p>un tiers.</p> <p>Certains règlements (émanant par exemple des organismes fédéraux américains de réglementation financière) exigent que l'entité prenne des mesures raisonnables de surveillance des fournisseurs de services en faisant preuve de la diligence voulue dans la sélection de ces fournisseurs.</p> <p>Des ressorts territoriaux, comme certains pays d'Europe, exigent que les entités qui transfèrent des renseignements personnels s'inscrivent auprès de leur organisme de réglementation avant de procéder au transfert.</p> <p>La LPRPDE exige un degré de protection comparable lorsque des renseignements sont traités par un tiers.</p> <p>Selon l'article 25 de la directive européenne, le transfert de tels renseignements ne peut avoir lieu que si un niveau de protection adéquat est assuré par le tiers.</p>
7.2.3	Nouvelles fins et nouvelles utilisations	L'entité a mis en place des systèmes et des procédures pour :	Parmi les autres types de transferts à une autre entité ou à un autre

Section	Critères relatifs à la communication à des tiers	Exemples de contrôles et de procédures	Autres considérations
	<p>L'entité ne communique des renseignements personnels à des tiers à de nouvelles fins ou pour de nouvelles utilisations que si l'individu a antérieurement donné son consentement implicite ou explicite à cet égard.</p>	<p>aviser les individus et obtenir leur consentement avant de communiquer des renseignements personnels à un tiers à des fins non mentionnées dans l'avis relatif à la protection des renseignements personnels; établir des documents indiquant si l'entité a avisé l'individu et reçu son consentement; s'assurer que des renseignements personnels ne sont communiqués à des tiers qu'aux fins mentionnées dans l'avis relatif à la protection des renseignements personnels.</p>	<p>organisme, il y a les transferts à des tiers :</p> <ul style="list-style-type: none"> qui sont des filiales ou des entités affiliées; qui fournissent un service demandé par l'individu; qui sont des autorités policières ou des organismes de réglementation; qui sont dans un autre pays et qui peuvent être assujettis à d'autres exigences.
7.2.4	<p>Utilisation abusive de renseignements personnels par un tiers L'entité prend des mesures correctives lorsqu'un tiers fait une utilisation abusive de renseignements personnels qu'elle lui a transférés.</p>	<p>L'entité :</p> <ul style="list-style-type: none"> examine les plaintes pour repérer toute indication d'une utilisation abusive de renseignements personnels par des tiers; prend des mesures chaque fois qu'elle apprend qu'un tiers utilise ou communique des renseignements personnels d'une façon non conforme aux politiques et procédures de l'entité en matière de protection des renseignements personnels, ou à une entente contractuelle; limite, dans la mesure du possible, tout préjudice causé par l'utilisation ou la communication de renseignements personnels par le tiers en violation des politiques et procédures de l'entité en matière de protection des renseignements personnels (par exemple, informer les individus touchés, tenter de 	

Section	Critères relatifs à la communication à des tiers	Exemples de contrôles et de procédures	Autres considérations
		<p>recupérer les renseignements communiqués, annuler les numéros affectés et en générer de nouveaux);</p> <p>prend des mesures correctives lorsqu'un tiers a fait une utilisation abusive de renseignements personnels (par exemple, des clauses contractuelles traitent des conséquences de l'utilisation abusive de renseignements personnels).</p>	

Sécurité

Section	Critères relatifs à la sécurité	Exemples de contrôles et de procédures	Autres considérations
8.0	L'entité protège les renseignements personnels contre tout accès non autorisé (aussi bien physique que logique).		
8.1	Politiques et communications		
8.1.0	<p>Politiques de protection des renseignements personnels</p> <p>Les politiques de l'entité en matière de protection des renseignements personnels (y compris ses politiques de sécurité pertinentes) traitent de la sécurité des renseignements personnels.</p>	<p>Les politiques traitent adéquatement des mesures de sécurité propres à assurer la protection des renseignements personnels, qu'ils soient conservés sur support électronique, sur support papier ou sous une autre forme. Les mesures de sécurité correspondent au degré de sensibilité des renseignements personnels.</p>	<p>Les renseignements personnels se trouvant dans tout lieu sous le contrôle de l'entité, ou réputé être sous son contrôle, doivent être protégés.</p>
8.1.1	<p>Communication aux individus</p> <p>Les individus sont informés des précautions prises pour assurer la protection des renseignements personnels.</p>	<p>L'avis de l'entité relatif à la protection des renseignements personnels décrit les types généraux de mesures au moyen desquelles on protège les renseignements personnels concernant l'individu. Voici des exemples :</p> <ul style="list-style-type: none"> les employés sont autorisés à avoir accès aux renseignements personnels en fonction des responsabilités rattachées à leur poste; on a recours à l'authentification pour empêcher tout accès non autorisé aux renseignements personnels stockés sur un support électronique; on assure la sécurité physique des renseignements personnels stockés 	<p>LES UTILISATEURS, LA DIRECTION, LES FOURNISSEURS ET LES AUTRES INTÉRESSÉS DEVRAIENT S'EFFORCER DE METTRE AU POINT ET D'ADOPTER DE BONNES PRATIQUES EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS, ET DE PROMOUVOIR DES COMPORTEMENTS TÉMOIGNANT DE LA RECONNAISSANCE DES BESOINS RELATIFS À LA SÉCURITÉ ET DU RESPECT DES INTÉRÊTS LÉGITIMES D'AUTRES PERSONNES.</p> <p>L'entité devrait envisager d'indiquer dans l'avis sur la protection des renseignements personnels les obligations des individus en matière de sécurité, par exemple l'obligation de</p>

Section	Critères relatifs à la sécurité	Exemples de contrôles et de procédures	Autres considérations
		<p>sous forme de copie papier, et on a recours au chiffrement pour empêcher tout accès non autorisé aux renseignements personnels transmis par Internet;</p> <p>des mesures de sécurité supplémentaires sont prises à l'égard des renseignements personnels sensibles.</p>	<p>garder confidentiels les identificateurs d'utilisateur et les mots de passe et celle de signaler les cas où la sécurité des renseignements personnels les concernant est compromise.</p> <p>L'entité devrait envisager de limiter la communication de renseignements détaillés sur les mesures de sécurité qu'elle a prises de façon à ne pas compromettre sa sécurité interne.</p>
8.2	Procédures et contrôles		
8.2.1	<p>Programme de sécurité de renseignements personnels</p> <p>Un programme de sécurité a été élaboré, consigné en dossier, approuvé et instauré. Ce programme comprend des mesures de protection de nature administrative, technique et physique destinées à protéger les renseignements personnels contre les risques de perte, d'utilisation abusive, d'accès non autorisé, de communication, de modification et de destruction. Le programme de sécurité devrait couvrir, sans toutefois s'y limiter, les éléments suivants³ dans la mesure où ils se rapportent à la sécurité des renseignements personnels :</p> <p>a) évaluation et traitement des risques [1.2.4];</p>	<p>Le programme de sécurité de l'entité traite des points suivants, au chapitre de la protection des renseignements personnels :</p> <ul style="list-style-type: none"> évaluations périodiques des risques; identification de tous les types de renseignements personnels, des processus et systèmes connexes ainsi que des tiers qui participent à la manipulation des renseignements personnels; détermination et documentation des exigences imposées aux utilisateurs en matière de sécurité; façon dont on accorde l'accès, nature de cet accès et personne qui l'autorise; nécessité d'empêcher tout accès non autorisé au moyen de contrôles efficaces d'accès logique et 	<p>Les mesures de protection utilisées peuvent prendre en compte la nature et la sensibilité des renseignements, ainsi que l'importance et la complexité des activités de l'entité. Par exemple, l'entité peut protéger les renseignements personnels et d'autres renseignements sensibles dans une plus grande mesure que les autres types de renseignements.</p> <p>Certains textes (dont la HIPAA) sont plus détaillés et donnent davantage d'indications sur les mesures de sécurité spécifiques qui devraient être envisagées et mises en œuvre.</p> <p>Certaines règles touchant la sécurité (par exemple, les règles relatives à la LGLB visant la sauvegarde des</p>

³ Ces éléments sont tirés de la norme ISO/IEC 27002:2005, *Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour la gestion de la sécurité de l'information*, avec la permission de l'American National Standards Institute (ANSI) agissant au nom de l'Organisation internationale de normalisation (ISO). On peut acheter des exemplaires de la norme ISO/IEC 27002 auprès de l'ANSI aux États-Unis, sur le site <http://webstore.ansi.org/> ou au Canada auprès du Conseil canadien des normes à l'adresse www.standardsstore.ca/eSpecs/index.jsp. Il n'est pas nécessaire de remplir tous les critères de la norme ISO/IEC 27002:2005 pour satisfaire au critère 8.2.1 des Principes généralement reconnus en matière de protection des renseignements personnels (PPRP). Les renvois dont est suivi chaque élément indiquent les critères des PPRP les plus pertinents aux fins de l'élément en question.

Section	Critères relatifs à la sécurité	Exemples de contrôles et de procédures	Autres considérations
	<ul style="list-style-type: none"> b) politiques de sécurité [8.1.0]; c) organisation de la sécurité des renseignements [sections 1, 7 et 10]; d) gestion des actifs [section 1]; e) sécurité des ressources humaines [section 1]; f) sécurité physique et environnementale [8.2.3 et 8.2.4]; g) gestion des communications et des activités [sections 1, 7 et 10]; h) contrôle des accès [sections 1, 8.2 et 10]; i) acquisition, développement et maintien de systèmes d'information [1.2.6]; j) gestion des incidents touchant la sécurité des renseignements [1.2.7]; k) gestion de la continuité de l'entreprise [section 8.2]; l) conformité [sections 1 et 10]. 	<p>physique;</p> <p>procédures selon lesquelles on ajoute de nouveaux utilisateurs, on modifie les niveaux d'accès d'utilisateurs actuels et on exclut des utilisateurs qui n'ont plus besoin d'avoir accès aux renseignements personnels;</p> <p>attribution de la responsabilité et de l'obligation de rendre compte en matière de sécurité;</p> <p>attribution de la responsabilité et de l'obligation de rendre compte à l'égard de l'entretien du système et des changements qui y sont apportés;</p> <p>protection du système d'exploitation et du logiciel de réseau ainsi que des fichiers système;</p> <p>protection des outils et des informations de chiffrement;</p> <p>implémentation des mises à niveau des logiciels d'exploitation et des correctifs;</p> <p>essai, évaluation et autorisation des composantes du système avant l'implémentation;</p> <p>façon dont sont résolues les plaintes et les demandes concernant des problèmes de sécurité;</p> <p>façon dont on remédie aux erreurs et omissions, aux atteintes à la sécurité et aux autres incidents de nature similaire;</p> <p>procédures utilisées pour déceler les attaques ou intrusions visant les systèmes ainsi que les tentatives en ce sens, et pour mettre à l'épreuve</p>	<p>renseignements) imposent les obligations suivantes :</p> <p>que le conseil d'administration (ou un comité, ou une personne nommée par le conseil) approuve et surveille le programme de l'entité en matière de sécurité des renseignements personnels;</p> <p>que les entités prennent des mesures raisonnables pour surveiller les fournisseurs de services concernés :</p> <ul style="list-style-type: none"> - en faisant preuve de la diligence requise dans la sélection des fournisseurs de services, - en obligeant par contrat les fournisseurs de services à mettre en œuvre et à maintenir des mesures de protection appropriées à l'égard des renseignements personnels en cause. <p>Le secteur des cartes de paiement (<i>PCI</i>) impose des obligations spécifiques de sécurité et de protection des renseignements personnels en ce qui concerne les renseignements sur les titulaires de cartes de certaines marques.</p>

Section	Critères relatifs à la sécurité	Exemples de contrôles et de procédures	Autres considérations
		<p>d'une manière proactive les procédures de sécurité (par exemple, tests de pénétration);</p> <p>affectation de ressources dans le domaine de la formation et d'autres domaines, à l'appui des politiques de sécurité;</p> <p>façon dont sont abordées les exceptions et les situations qui ne sont pas visées d'une manière spécifique dans les politiques de l'entité sur l'intégrité des processus système et les politiques connexes sur la sécurité du système;</p> <p>plans de gestion de la continuité de l'entreprise et de reprise après sinistre et tests connexes;</p> <p>mesures prises pour repérer les lois et règlements applicables, les engagements, les ententes sur les niveaux de service et autres contrats, et pour s'assurer que l'entité s'y conforme;</p> <p>obligation pour les utilisateurs, la direction et les tiers de confirmer (initialement et une fois l'an) qu'ils comprennent les politiques et procédures de l'entité relatives à la protection des renseignements personnels, et qu'ils s'engagent à s'y conformer;</p> <p>procédures d'annulation des privilèges d'accès et de restitution des ordinateurs et autres appareils utilisés pour consulter ou stocker des renseignements personnels lorsqu'il est mis fin à l'emploi d'un salarié.</p>	

Section	Critères relatifs à la sécurité	Exemples de contrôles et de procédures	Autres considérations
		<p>Le programme de sécurité de l'entité empêche l'accès aux renseignements personnels se trouvant dans des ordinateurs, sur des supports de données et des supports papier qui ne sont plus couramment utilisés par l'organisation (par exemple, des renseignements se trouvant dans des ordinateurs, sur des supports de données ou des supports papier qui sont entreposés, vendus ou éliminés de toute autre manière).</p>	
8.2.2	<p>Contrôles d'accès logique L'accès logique aux renseignements personnels est restreint par des procédures portant sur les aspects suivants :</p> <ul style="list-style-type: none"> a) autorisation et enregistrement des membres du personnel interne et des individus; b) identification et authentification des membres du personnel interne et des individus; c) modification et mise à jour des profils d'accès; d) octroi des privilèges et des permissions d'accès aux composantes de l'infrastructure informatique et aux renseignements personnels; e) dispositifs empêchant les individus d'avoir accès à d'autres renseignements que les renseignements personnels ou sensibles les concernant; f) dispositifs limitant l'accès aux 	<p>L'entité a mis en place des systèmes et des procédures pour :</p> <ul style="list-style-type: none"> établir le niveau et la nature de l'accès qui sera donné aux utilisateurs en fonction de la sensibilité des données et du besoin légitime de l'utilisateur d'avoir accès aux renseignements personnels dans le cadre de ses fonctions; authentifier les utilisateurs, par exemple au moyen d'un nom d'utilisateur et d'un mot de passe, de certificats, de jetons externes ou de moyens biométriques, avant de leur donner accès à des systèmes où sont traités des renseignements personnels; exiger des mesures de sécurité accrues pour l'accès à distance : mots de passe additionnels ou dynamiques, procédures de rétro-appels, certificats 	<p>Les processus relatifs à l'autorisation de l'utilisateur prennent en compte les éléments suivants :</p> <ul style="list-style-type: none"> le mode d'accès aux données (réseau interne ou externe) ainsi que les supports de données et la plate-forme technologique de stockage; l'accès aux documents papier et aux supports de sauvegarde contenant des renseignements personnels; le refus de donner accès aux comptes joints sans l'utilisation d'autres méthodes pour authentifier les véritables individus. <p>Certains pays ou ressorts territoriaux imposent le chiffrement (ou toute autre forme de brouillage) des données stockées (au repos).</p>

Section	Critères relatifs à la sécurité	Exemples de contrôles et de procédures	Autres considérations
	<p>renseignements personnels aux membres autorisés du personnel interne, en fonction du rôle et des responsabilités qui leur sont attribués;</p> <p>g) remise des sorties d'ordinateur limitée aux membres autorisés du personnel interne;</p> <p>h) limitation de l'accès logique au stockage hors-ligne, aux données de sauvegarde, aux systèmes et aux supports de données;</p> <p>i) limitation de l'accès aux configurations de système, à la fonctionnalité de superutilisateur, aux mots de passe maîtres, aux utilitaires puissants et aux dispositifs de sécurité (les coupe-feu, par exemple);</p> <p>j) dispositifs empêchant l'introduction de virus, de programmes malveillants et de logiciels non autorisés.</p>	<p>numériques, cartes d'identification sécurisées, réseau privé virtuel (RPV), coupe-feu adéquatement installés, etc.;</p> <p>mettre en œuvre des systèmes de détection des intrusions et de surveillance.</p>	
8.2.3	<p>Contrôles d'accès physique</p> <p>L'accès physique aux renseignements personnels, quelle qu'en soit la forme (y compris les composantes du ou des systèmes de l'entité qui contiennent ou protègent des renseignements personnels) est restreint.</p>	<p>L'entité a mis en place des systèmes et des procédures pour :</p> <ul style="list-style-type: none"> gérer l'accès logique et physique aux renseignements personnels, y compris en ce qui concerne les supports papier, les archives et les copies de sauvegarde; enregistrer et surveiller l'accès à des renseignements personnels; empêcher toute destruction ou perte non autorisée ou accidentelle de renseignements personnels; 	<p>Parmi les mesures de protection physique, on peut citer l'utilisation de classeurs verrouillés, les systèmes de contrôle des accès par carte, les clés physiques, les fichiers des entrées avec signature, et d'autres techniques permettant de contrôler l'accès aux bureaux, aux centres de données ainsi qu'à d'autres lieux où des renseignements personnels sont traités ou stockés.</p>

Section	Critères relatifs à la sécurité	Exemples de contrôles et de procédures	Autres considérations
		<p>enquêter sur les intrusions et les tentatives d'obtenir un accès non autorisé;</p> <p>communiquer les résultats des enquêtes au responsable de la protection des renseignements personnels;</p> <p>exercer un contrôle physique sur la diffusion de rapports contenant des renseignements personnels;</p> <p>éliminer d'une façon sûre les déchets contenant des renseignements confidentiels (au moyen du déchiquetage, par exemple).</p>	
8.2.4	<p>Mesures de protection contre les risques liés à l'environnement</p> <p>Les renseignements personnels, quelle qu'en soit la forme, sont protégés contre une communication accidentelle due à une catastrophe naturelle ou aux risques liés à l'environnement.</p>	<p>La direction applique des mesures de protection contre les facteurs environnementaux (incendie, inondation, poussière, panne d'électricité, chaleur et humidité excessives...) sur la base de son évaluation des risques. Les zones contrôlées de l'entité sont protégées contre les incendies au moyen de détecteurs de fumée et d'un système d'extinction.</p> <p>En outre, l'entité maintient des dispositifs physiques et autres moyens pour empêcher la communication accidentelle de renseignements personnels en cas d'incident environnemental.</p>	<p>Certains règlements, tels que les directives européennes, exigent que les renseignements personnels soient protégés contre la destruction illégale, la perte accidentelle, les catastrophes naturelles et les risques liés à l'environnement, en plus d'être protégés des communications accidentelles.</p>
8.2.5	<p>Transmission de renseignements personnels</p>	<p>L'entité a mis en place des systèmes et des procédures pour :</p>	<p>Certains textes (par exemple, la HIPAA) contiennent des dispositions portant</p>

Section	Critères relatifs à la sécurité	Exemples de contrôles et de procédures	Autres considérations
	<p>Les renseignements personnels sont protégés lorsqu'ils sont transmis par la poste ou par d'autres moyens physiques. Les renseignements personnels recueillis et transmis par Internet, par des réseaux publics non sécurisés ou par des réseaux sans fil sont protégés au moyen d'une technologie de chiffrement normalisée pour le transfert et la réception des renseignements personnels.</p>	<p>définir les niveaux minimums de chiffrement et de contrôles; utiliser une technologie normalisée (par exemple, la transmission par réseau privé virtuel selon le protocole Transport Layer Security à 128 bits) pour le transfert et la réception de renseignements personnels; approuver les connexions de réseau externe; protéger les renseignements personnels, tant sur support papier qu'électronique, transmis par la poste, par messagerie ou par un autre moyen physique. chiffrer les renseignements personnels recueillis et transmis sans fil et protéger les réseaux sans fil contre les accès non autorisés.</p>	<p>spécifiquement sur la transmission électronique et l'authentification des signatures dans le cas des dossiers médicaux (en association avec les transactions standard).</p> <p>Certains émetteurs de cartes de crédit ont publié des exigences minimales pour la sécurisation des données relatives au détenteur, dont l'obligation d'employer des techniques de chiffrement pour la transmission et le stockage des données liées aux cartes et aux opérations.</p> <p>Au fur et à mesure de l'évolution de la technologie, du marché et de la réglementation, de nouvelles mesures deviendront sans doute nécessaires pour atteindre des niveaux de protection adéquats (par exemple, le protocole de sécurité TLS à 128 bits, avec identification d'utilisateur et mots de passe).</p> <p>Il se peut que la transmission vocale par appareil sans fil (par exemple, téléphone cellulaire) de renseignements personnels ne soit pas chiffrée.</p>
8.2.6	<p>Renseignements personnels sur supports portatifs Les renseignements personnels stockés sur des supports ou des appareils portatifs sont protégés contre les accès non autorisés.</p>	<p>Les politiques et procédures interdisent le stockage de renseignements personnels sur des supports ou des appareils portatifs à moins que les besoins d'affaires ne l'imposent et qu'un tel stockage ne soit approuvé par la direction.</p> <p>Des politiques, des systèmes et des</p>	<p>Il faudrait songer à la nécessité de protéger les renseignements personnels fournis, par exemple, aux autorités de réglementation ou aux auditeurs.</p>

Section	Critères relatifs à la sécurité	Exemples de contrôles et de procédures	Autres considérations
		<p>procédures ont été mis en place afin de protéger les renseignements personnels consultés ou stockés par les moyens suivants :</p> <ul style="list-style-type: none"> ordinateurs portables, assistants numériques personnels (PDA), téléphones intelligents et appareils similaires; ordinateurs et autres appareils utilisés par le personnel en déplacement ou travaillant de la maison; clés USB, CD, DVD, bandes magnétiques et autres supports portatifs. <p>De tels renseignements sont chiffrés, protégés par mot de passe et physiquement et couverts par les politiques de l'entité en matière d'accès, de conservation et de destruction.</p> <p>Des contrôles encadrent la création, la transmission, le stockage et la suppression des copies de sauvegarde contenant des renseignements personnels.</p> <p>Des procédures sont prévues pour la déclaration de la perte ou d'une utilisation abusive potentielle de supports contenant des renseignements personnels.</p> <p>Lorsque l'emploi d'un salarié ou le contrat d'un collaborateur extérieur prend fin, des procédures prévoient la restitution ou la destruction des</p>	

Section	Critères relatifs à la sécurité	Exemples de contrôles et de procédures	Autres considérations
		supports et des appareils portatifs utilisés pour consulter ou stocker des renseignements personnels ainsi que de toute copie, imprimée ou autre, de ces renseignements.	
8.2.7	<p>Vérification des mesures de sécurité On effectue au moins une fois l'an des tests sur l'efficacité des principales mesures de protection administratives, techniques et physiques concernant les renseignements personnels.</p>	<p>L'entité a mis en place des systèmes et procédures pour :</p> <ul style="list-style-type: none"> tester régulièrement l'efficacité des principales mesures de protection administratives, techniques et physiques concernant les renseignements personnels; faire procéder périodiquement à des vérifications indépendantes des contrôles de sécurité en ayant recours à des vérificateurs internes ou externes; tester au moins une fois l'an les systèmes d'accès par carte et les autres dispositifs de sécurité physique; consigner et tester au moins une fois l'an les plans de reprise après sinistre et les plans de secours pour s'assurer de leur viabilité; effectuer périodiquement des tests sur les menaces et les vulnérabilités, y compris les contrôles touchant la sécurité face aux tentatives de pénétration ainsi que la vulnérabilité et la résistance à l'égard du Web; apporter périodiquement les modifications requises aux politiques et aux procédures de sécurité, en tenant compte des résultats des tests effectués ainsi que de l'évolution des menaces et des 	<p>La fréquence et la nature des tests sur les mesures de sécurité varieront selon la taille et la complexité de l'entité, la nature et l'étendue de ses activités et enfin la sensibilité des renseignements personnels.</p> <p>Certains règlements ayant trait à la sécurité (par exemple, les règles liées à la LGLB au sujet de la sauvegarde des renseignements) obligent les entités :</p> <ul style="list-style-type: none"> à faire effectuer régulièrement des tests des principaux contrôles, systèmes et procédures par des tiers indépendants ou par des membres du personnel indépendants de ceux qui élaborent ou gèrent les mesures de sécurité (ou, du moins, à soumettre les résultats des tests à ces personnes indépendantes); au moins une fois l'an, à évaluer et, le cas échéant, à corriger les mesures de sécurité en matière de renseignements personnels.

Section	Critères relatifs à la sécurité	Exemples de contrôles et de procédures	Autres considérations
		vulnérabilités; rendre compte régulièrement des résultats des tests de sécurité à la direction.	

Qualité

Section	Critères relatifs à la qualité	Exemples de contrôles et de procédures	Autres considérations
9.0	L'entité garde des renseignements personnels exacts, complets et pertinents, aux fins mentionnées dans l'avis.		
9.1	Politiques et communications		
9.1.0	Politiques de protection des renseignements personnels Les politiques de l'entité en matière de protection des renseignements personnels traitent de la qualité de ces renseignements.		
9.1.1	Communication aux individus Les individus sont informés qu'il leur incombe de donner à l'entité des renseignements personnels exacts et complets, et de communiquer avec l'entité lorsque des rectifications s'imposent.	L'avis de l'entité relatif à la protection des renseignements personnels explique la nécessité de fournir des renseignements exacts et à jour, dans le cas seulement où la relation entre l'individu et l'entité est durable.	
9.2	Procédures et contrôles		
9.2.1	Caractère exact et complet des renseignements personnels Les renseignements personnels sont exacts et complets au regard des fins auxquelles ils doivent être utilisés.	L'entité a mis en place des systèmes et des procédures pour : <ul style="list-style-type: none"> modifier et valider les renseignements personnels à mesure qu'ils sont recueillis, créés, gardés et mis à jour; consigner la date à laquelle les renseignements personnels ont été obtenus ou mis à jour; préciser à partir de quel moment les renseignements personnels ne sont plus valides; préciser à quel moment et de quelle manière les renseignements personnels doivent être mis à jour, 	

Section	Critères relatifs à la qualité	Exemples de contrôles et de procédures	Autres considérations
		<p>et quelle est la source de cette mise à jour (par exemple, la confirmation annuelle des renseignements détenus et les méthodes selon lesquelles les individus peuvent mettre à jour d'une façon proactive les renseignements personnels les concernant);</p> <p>indiquer comment vérifier l'exactitude et le caractère complet des renseignements personnels obtenus directement d'un individu, reçus d'un tiers (voir la section 4.2.3, «Collecte de renseignements auprès de tiers») ou communiqués à un tiers (voir la section 7.2.2, «Protection des renseignements personnels»);</p> <p>s'assurer que les renseignements personnels utilisés d'une façon continue sont suffisamment exacts et complets pour permettre la prise de décisions, à moins que des limites claires soient posées quant à la nécessité de l'exactitude;</p> <p>s'assurer qu'on ne procède pas d'une façon machinale à la mise à jour de renseignements personnels, à moins que cela ne soit nécessaire pour la réalisation des fins auxquelles les renseignements doivent être utilisés.</p> <p>L'entité effectue des évaluations périodiques pour vérifier l'exactitude des dossiers de renseignements personnels et y apporter les corrections nécessaires, afin qu'ils remplissent leur</p>	

Section	Critères relatifs à la qualité	Exemples de contrôles et de procédures	Autres considérations
		objet.	
9.2.2	<p>Pertinence des renseignements personnels Les renseignements personnels sont pertinents à l'égard des fins auxquelles ils doivent être utilisés.</p>	<p>L'entité a mis en place des systèmes et des procédures pour :</p> <ul style="list-style-type: none"> s'assurer que les renseignements personnels ont une pertinence suffisante à l'égard des fins auxquelles ils doivent être utilisés, et pour réduire au minimum la possibilité que des renseignements non pertinents soient utilisés pour prendre des décisions commerciales au sujet de l'individu; évaluer périodiquement la pertinence des dossiers de renseignements personnels et les corriger, au besoin, afin de réduire au minimum l'utilisation de données non pertinentes dans la prise de décisions. 	

Suivi et application

Section	Critères relatifs au suivi et à l'application	Exemples de contrôles et de procédures	Autres considérations
10.0	L'entité fait le suivi du respect de ses politiques et procédures en matière de protection des renseignements personnels, et a instauré des procédures pour le traitement des demandes d'informations, des plaintes et des contestations relevant de cette question.		
10.1	Politiques et communications		
10.1.0	Politiques de protection des renseignements personnels Les politiques de l'entité en matière de renseignements personnels traitent du suivi et de l'application des politiques et procédures dans ce domaine.		
10.1.1	Communication aux individus Les individus sont informés de la façon dont les plaintes, les demandes d'informations et les contestations peuvent être communiquées à l'entité.	L'avis de l'entité relatif à la protection des renseignements personnels : indique de quelle façon les individus peuvent communiquer à l'entité les plaintes (par exemple, numéro de téléphone, lien de courriel sur le site Web de l'entité); indique à qui l'individu peut s'adresser pour l'acheminement de plaintes (par exemple, nom, numéro de téléphone, adresse postale, adresse électronique de la personne ou du bureau chargé de recevoir les plaintes).	
10.2	Procédures et contrôles		
10.2.1	Processus applicable à l'égard des demandes d'informations, des plaintes et des contestations On a mis en place un processus pour le traitement des demandes d'informations, des plaintes et des	Le responsable de la protection des renseignements personnels ou la personne désignée est autorisé à s'occuper des plaintes, des contestations et de tout autre problème relevant de la protection des	

Section	Critères relatifs au suivi et à l'application	Exemples de contrôles et de procédures	Autres considérations
	contestations.	<p>renseignements personnels.</p> <p>L'entité a mis en place des systèmes et des procédures indiquant :</p> <ul style="list-style-type: none"> la marche à suivre pour communiquer et régler les plaintes au sujet de l'entité; les mesures qui seront prises au sujet des renseignements en cause jusqu'à ce que la plainte ait été réglée d'une manière satisfaisante; les recours possibles en cas d'utilisation abusive de renseignements personnels, et la façon de communiquer cette information à un individu; les recours et la procédure hiérarchique officielle pour l'examen et l'approbation de tout recours offert aux individus; la personne avec qui communiquer et les procédures à suivre à l'égard de tout service de règlement des contestations par un tiers ou service similaire (quand ils sont offerts). 	
10.2.2	<p>Règlement des contestations et recours</p> <p>Toute plainte fait l'objet d'un examen, et la conclusion est consignée et communiquée à l'individu.</p>	<p>L'entité a mis en place une procédure consignée en bonne et due forme pour :</p> <ul style="list-style-type: none"> assurer la formation des employés responsables du traitement des plaintes et des contestations individuelles sur les processus de règlement et la procédure hiérarchique; consigner par écrit toute plainte et y répondre en temps utile; examiner périodiquement les 	<p>Certains textes (notamment la HIPAA et la COPPA) prévoient des procédures et des exigences spécifiques à cet égard.</p> <p>Certaines lois (par exemple, la LPRPDE) permettent les recours juridiques jusqu'au plus haut échelon de la hiérarchie judiciaire.</p>

Section	Critères relatifs au suivi et à l'application	Exemples de contrôles et de procédures	Autres considérations
		<p>plaintes et les contestations en suspens pour faire en sorte de les régler en temps utile;</p> <p>transmettre les plaintes et les contestations en suspens par la voie hiérarchique pour examen par la direction;</p> <p>déceler des tendances et l'éventuelle nécessité d'apporter des changements aux politiques et procédures de l'entité en matière de protection des renseignements personnels;</p> <p>avoir recours aux services désignés de règlement des contestations par un tiers indépendant ou aux autres procédures dictées par les organismes de réglementation lorsque l'individu n'est pas satisfait du règlement proposé par l'entité, et que de tels tiers se sont engagés à s'occuper de tels recours.</p> <p>Si l'entité offre un processus de règlement des contestations par un tiers à l'égard des plaintes ne pouvant être réglées directement avec elle, on explique à l'individu comment il peut se prévaloir de ce processus.</p>	
10.2.3	<p>Contrôle de conformité</p> <p>Le respect des politiques et procédures en matière de protection des renseignements personnels, des engagements ainsi que des lois et règlements applicables, des ententes sur les niveaux de service et des autres contrats fait l'objet d'un contrôle et est consigné, et les</p>	<p>L'entité a mis en place des systèmes et des procédures pour :</p> <p>contrôler une fois l'an le respect des politiques et procédures en matière de renseignements personnels, des engagements ainsi que des lois et règlements applicables, des ententes sur les niveaux de service, des normes</p>	<p>En plus de leurs obligations légales, réglementaires et contractuelles, il se peut que des entités choisissent de se conformer à certaines normes, comme celles publiées par l'ISO, ou qu'elles soient tenues de se conformer à certaines, par exemple celles du secteur des cartes de paiement (<i>PCI</i>), pour pouvoir exercer des activités.</p>

Section	Critères relatifs au suivi et à l'application	Exemples de contrôles et de procédures	Autres considérations
	<p>résultats de ces contrôles sont transmis à la direction. Si des problèmes ont été décelés, on élabore un plan de mesures correctives et on le met en œuvre.</p>	<p>adoptées par l'entité et des autres contrats; documenter les contrôles périodiques, les plans de vérification interne, les rapports de vérification, les listes de contrôle de conformité et les approbations signées par la direction; signaler à la direction les résultats du contrôle de conformité et les améliorations recommandées, et mettre en œuvre un plan de mesures correctives; faire le suivi du règlement des problèmes et des vulnérabilités relevés lors du contrôle de conformité pour assurer la prise en temps utile des mesures correctives appropriées (les politiques et procédures en matière de protection des renseignements personnels sont revues au besoin).</p>	
10.2.4	<p>Cas de non-conformité Les cas de non-conformité avec les politiques et procédures en matière de protection des renseignements personnels sont consignés et signalés et, au besoin, des mesures correctives ou disciplinaires sont prises en temps utile.</p>	<p>L'entité a mis en place des systèmes et des procédures pour : aviser les employés de la nécessité de signaler en temps utile les atteintes à la protection des renseignements personnels et les vulnérabilités sur le plan de la sécurité; informer les employés des voies par lesquelles devraient être signalées les vulnérabilités sur le plan de la sécurité et les atteintes à la protection des renseignements personnels; consigner les cas de non-conformité aux politiques et</p>	

Section	Critères relatifs au suivi et à l'application	Exemples de contrôles et de procédures	Autres considérations
		<p>procédures en matière de protection des renseignements personnels;</p> <p>faire le suivi de la correction des vulnérabilités sur le plan de la sécurité et des atteintes à la protection des renseignements personnels, de façon à s'assurer que les mesures correctives appropriées ont été prises en temps utile;</p> <p>prendre les mesures disciplinaires qui s'imposent à l'encontre des employés ou des autres personnes à l'origine d'atteintes à la protection des renseignements personnels ou d'incidents s'y rapportant;</p> <p>limiter, dans la mesure du possible, tout préjudice causé par l'utilisation ou la communication de renseignements personnels par le tiers en violation des politiques et procédures de l'entité en matière de protection des renseignements personnels (par exemple, informer les individus touchés, tenter de récupérer les renseignements communiqués, annuler les numéros de compte affectés et en générer des nouveaux);</p> <p>déceler les tendances susceptibles de nécessiter la révision des politiques et procédures en matière de protection des renseignements personnels.</p>	
10.2.5	<p>Suivi continu</p> <p>Des procédures de suivi continu sont</p>	L'entité utilise les moyens suivants : rapports sur les contrôles	L'ouvrage <i>Guidance on Monitoring Internal Control Systems</i> , publié par le

Section	Critères relatifs au suivi et à l'application	Exemples de contrôles et de procédures	Autres considérations
	<p>mises en œuvre pour surveiller l'efficacité des contrôles sur les renseignements personnels en fonction de l'évaluation des risques [1.2.4] et, le cas échéant, prendre en temps utile les mesures correctives nécessaires.</p>	<p>analyse des tendances assiduité aux formations et évaluations règlement des plaintes examens internes réguliers rapports d'audit interne rapports d'audit indépendants couvrant les contrôles des sociétés de services autres éléments probants de l'efficacité des contrôles</p> <p>Le choix des contrôles à surveiller et la fréquence à laquelle ils le sont sont fonction de la sensibilité des renseignements et des risques qui s'y rapportent.</p> <p>Voici des exemples de contrôles :</p> <p>Les politiques prévoient que tous les employés suivent une formation initiale sur la protection des renseignements personnels dans les 30 jours qui suivent leur embauche. Le suivi continu peut comprendre l'examen des dossiers des ressources humaines d'un échantillon d'employés pour voir si le cours a bien été effectué.</p> <p>Les politiques prévoient que, lorsque les responsabilités d'un employé changent ou que son emploi prend fin, son accès aux renseignements personnels est revu et modifié en conséquence ou supprimé dans les 24 heures</p>	<p>Committee of Sponsoring Organizations of the Treadway Commission (COSO), fournit des lignes directrices utiles pour le suivi de l'efficacité des contrôles.</p>

Section	Critères relatifs au suivi et à l'application	Exemples de contrôles et de procédures	Autres considérations
		<p>(ou immédiatement en cas de cessation d'emploi). Cela est contrôlé par un processus automatique du système des ressources humaines qui produit un rapport de changement de situation de l'employé et entraîne, à moins d'une intervention du supérieur hiérarchique, la suppression automatique de l'accès. Le suivi est assuré par le groupe responsable de la sécurité, qui reçoit un exemplaire de ces rapports et un avis des interventions des supérieurs. Les politiques stipulent qu'en cas de plainte liée à la protection des renseignements personnels, un avis de réception doit être envoyé au plaignant dans les 72 heures et que, si la plainte n'est pas réglée dans les 10 jours ouvrables qui suivent, on doit la faire remonter au responsable de la PRP. Le contrôle consiste en un registre servant à noter les plaintes concernant la PRP, accompagnées de leur date, ainsi que les actions subséquentes jusqu'au règlement. L'activité de suivi consiste en l'examen mensuel du registre, pour en vérifier la conformité à la politique prescrite.</p>	

Annexe A – Glossaire

atteinte à la protection des renseignements personnels. Il y a atteinte à la protection des renseignements personnels lorsque des renseignements personnels sont recueillis, conservés, consultés, utilisés ou communiqués d'une façon non conforme aux dispositions des politiques de l'entreprise ou des lois et règlements applicables en la matière

caviarder. Effacer ou masquer les renseignements personnels dans un document ou un fichier.

chiffrement. Transformation des renseignements de façon à les rendre inintelligibles à quiconque, à l'exception du détenteur d'une clé spéciale (pour déchiffrer).

confidentialité. Protection des données et des renseignements non personnels contre la communication non autorisée.

consentement. Fait, pour l'individu, d'accepter que l'entité recueille, utilise et communique des renseignements personnels en conformité avec l'avis relatif à la protection des renseignements personnels. Le consentement est explicite ou implicite. Le *consentement explicite* est donné oralement, par voie électronique ou par écrit, est sans équivoque et n'exige aucune inférence de la part de l'entité désireuse de l'obtenir. Le *consentement implicite* peut être raisonnablement déduit d'une action ou de l'inaction de l'individu, comme le fait de ne pas cocher la case «Je refuse» ou de fournir son numéro de carte de crédit pour effectuer une opération.

cycle informationnel (dans le contexte des renseignements personnels). Collecte, utilisation, conservation, communication, suppression ou désidentification des renseignements personnels.

désidentifier. Éliminer tout renseignement relatif à une personnel qui pourrait permettre de l'identifier.

entité. Organisation qui recueille, utilise, conserve et communique des renseignements personnels.

entité affiliée. Entité qui en contrôle une autre, qui est contrôlée par une autre ou qui fait l'objet d'un contrôle commun avec une autre entité.

externalisation. Utilisation et traitement des renseignements personnels par un tiers qui assume une fonction d'affaires pour l'entité.

fins. Raisons pour lesquelles les renseignements personnels sont recueillis par l'entité.

individu. Personne au sujet de laquelle les renseignements personnels sont recueillis (on emploie parfois le terme «personne concernée»).

personnel interne. Employés, collaborateurs externes, mandataires et autres personnes agissant au nom de l'entité et de ses entités affiliées.

pixel invisible ou mouchard. Image invisible, de la taille d'un pixel, insérée dans une page Web ou dans un courriel à des fins de collecte de données. Les entreprises font de nombreuses utilisations des pixels invisibles : information sur l'achalandage d'un site, compte de visiteurs, vérification des volets publicité et courriel et rapports connexes, et personnalisation. Un pixel

invisible peut permettre par exemple de récupérer l'adresse IP d'un utilisateur, l'adresse du dernier site qu'il a visité et les habitudes de navigation.

politique. Déclaration écrite exprimant l'intention, les objectifs, les exigences, les responsabilités et les normes de la direction.

programme de protection des renseignements personnels. Politiques, communications, procédures et contrôles mis en place pour gérer et protéger les renseignements personnels selon les risques et obligations d'affaires et de conformité.

protection des renseignements personnels. Droits et obligations des individus et des organisations en ce qui concerne la collecte, l'utilisation, la conservation, la communication et la destruction des renseignements personnels.

renseignement personnel. Renseignement qui concerne ou est susceptible de concerner un individu identifiable, ou qui est relié ou susceptible d'être relié à un individu identifiable.

renseignements personnels sensibles. Renseignements commandant un degré supérieur de protection et une obligation de diligence plus grande. Il s'agit par exemple de renseignements sur l'état de santé, la situation financière, l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance à un syndicat, les préférences sexuelles ou les renseignements ayant trait à des infractions ou à des condamnations criminelles.

témoins. Information générée par un serveur Web et stockée dans l'ordinateur de l'utilisateur, pour un accès ultérieur. Cette information peut servir à identifier l'utilisateur lorsqu'il accède de nouveau au site Web, à personnaliser le contenu du site en fonction de celui-ci et à lui proposer des articles susceptibles de l'intéresser, compte tenu de ses habitudes d'achat antérieures. Certains annonceurs emploient des méthodes de pistage, y compris des témoins, pour analyser les comportements et les parcours sur un site.

tiers. Entité non affiliée à l'entité qui recueille les renseignements personnels ou entité affiliée non visée par la politique de protection des renseignements personnels de l'entité.

Annexe B – Services de praticiens CA ou CPA fondés sur les principes généralement reconnus en matière de protection des renseignements personnels

La présente annexe donne un aperçu général des services que les CA et les CPA en cabinet (praticiens) peuvent offrir en s'appuyant sur les principes généralement reconnus en matière de protection des renseignements personnels (PPRP). Les praticiens peuvent obtenir des indications supplémentaires auprès de l'Institut Canadien des Comptables Agréés (ICCA) ou de l'AICPA (voir www.icca.ca et www.aicpa.org/privacy).

Missions de conseil relatives à la protection des renseignements personnels

Les praticiens peuvent fournir toute une gamme de services conseils à leurs clients, notamment en matière de stratégie, de diagnostic et de mise en œuvre ainsi que de services de soutien et de gestion, en s'appuyant sur les PPRP et leurs critères. Il pourrait s'agir de conseiller les clients sur les faiblesses des systèmes, d'évaluer les risques et de recommander une ligne de conduite en prenant les PPRP et leurs critères pour référence.

Aux États-Unis, les praticiens qui fournissent de tels services conseils suivent le chapitre CS 100 du *Statement on Standards for Consulting Services*, «Consulting Services: Definition and Standards» (*AICPA Professional Standards*, vol. 2). Au Canada, le *Manuel* de l'ICCA ne contient pas de norme visant la prestation de services conseils.

Missions d'attestation et de certification relatives à la protection des renseignements personnels

Les praticiens peuvent également utiliser les PPRP pour fournir des services d'attestation et de certification à leurs clients, qui aboutissent généralement à la délivrance d'un rapport destiné à des tiers. La nature de ces services ainsi que les normes professionnelles qui s'y rattachent et les types de rapport auxquels ils peuvent respectivement donner lieu sont décrits ci-dessous.

Missions de vérification relatives à la protection des renseignements personnels

Les normes américaines pertinentes à l'égard des missions d'attestation sont consignées dans les Statements on Standards for Attestation Engagements. Les normes canadiennes pertinentes à l'égard des missions de certification sont énoncées dans le chapitre 5025 du *Manuel de l'ICCA – Certification*. Les missions d'attestation et de certification relatives à la protection des renseignements personnels sont définies en fonction de ces normes. On s'attend à ce que les praticiens se conforment aux exigences des normes professionnelles pertinentes.

Les missions de vérification sont conçues pour fournir un niveau élevé, quoique non absolu, d'assurance à l'égard des éléments considérés ou d'une assertion. Le praticien élabore à cette fin des procédés de vérification qui, selon son jugement professionnel, ramènent à un niveau faible le risque d'aboutir à une conclusion inappropriée. Des modèles de rapports du vérificateur portant sur la protection des renseignements personnels sont présentés à l'Annexe C.

Les concepts clés qui suivent s'appliquent aux missions de vérification relatives à la protection des renseignements personnels :

Un rapport du vérificateur ayant trait à la protection des renseignements personnels couvre normalement les dix principes. Tous les critères pertinents énoncés à l'égard de chacun de ces principes doivent être remplis pendant la période visée par le rapport pour que le praticien puisse délivrer un rapport sans réserve^{4,5}.

Le travail doit être effectué de façon à obtenir un degré d'assurance du niveau «vérification» ou équivalent.

La mission peut porter 1) soit sur l'ensemble des renseignements personnels ou sur certains types seulement comme les renseignements sur les clients ou les renseignements sur les employés et 2) sur toutes les unités d'exploitation de l'entité dans son ensemble et tous les endroits où elle mène des activités ou encore sur certaines de ses unités d'exploitation seulement (les activités de vente au

4 Voir l'Annexe C, «Modèles de rapports du vérificateur portant sur la protection des renseignements personnels».

5 Dans certains cas (comme dans un rapport sur un tiers fournisseur de services), un rapport spécial sur la protection des renseignements personnels portant sur certains des dix principes pourrait être délivré. Il est recommandé que ces rapports indiquent que les principes dont il n'est pas fait mention sont essentiels à l'obtention d'une assurance globale à l'égard de la protection des renseignements personnels et qu'il s'agit de rapports à usage restreint.

détail et non les activités de fabrication, ou encore seulement les activités menées par le truchement du site Web de l'entité ou de domaines Internet spécifiés) ou sur des activités menées dans un endroit précis (au Canada, par exemple). En outre :

l'avis sur la protection des renseignements personnels devrait soit 1) être aisément accessible aux utilisateurs du rapport du vérificateur et clairement mentionné dans l'assertion de la direction et le rapport, soit 2) accompagner l'assertion de la direction et le rapport du vérificateur. L'étendue de la mission doit généralement cadrer avec la description des entités et des activités dont il est question dans l'avis qu'elle diffuse au sujet de la protection des renseignements personnels ([voir le critère 2.2.2](#)). L'étendue de la mission peut être plus étroite que la portée de l'avis mais elle ne peut l'excéder; la mission doit couvrir toutes les activités d'un [cycle informationnel](#) relatives aux renseignements personnels en cause. Ces activités doivent notamment comprendre la collecte, l'utilisation, la conservation, la communication et la suppression ou la désidentification des renseignements. Le fait de déterminer une unité d'exploitation ne comportant pas un cycle complet pourrait induire en erreur l'utilisateur du rapport du praticien; si des renseignements personnels identifiés couverts par le travail de vérification sont amalgamés à des renseignements personnels non couverts, la mission de certification relative aux renseignements personnels doit tenir compte des contrôles appliqués pour tous les renseignements à partir du moment où ils sont amalgamés; le rapport du praticien doit ordinairement porter sur une période définie (d'au moins deux mois); toutefois, le premier rapport délivré par le praticien peut être un rapport ponctuel.

Assertion de la direction

Selon les normes d'attestation de l'AICPA, pour une mission de vérification, le praticien devrait normalement obtenir une assertion écrite de la direction. Si celle-ci refuse d'en fournir une, le praticien

peut tout de même délivrer un rapport sur les éléments considérés; cela dit, la forme de son rapport sera fonction des circonstances⁶.

Selon les normes de l'AICPA, le praticien peut faire rapport, soit sur l'assertion de la direction, soit sur les éléments considérés. Lorsque le praticien fait rapport sur l'assertion, celle-ci devrait accompagner le rapport du praticien ou bien être citée dans le premier paragraphe du rapport⁷. Lorsque le praticien fait rapport sur les éléments considérés, il peut juger utile de demander à la direction de mettre une assertion à la disposition des utilisateurs de son rapport.

Selon les normes de certification de l'ICCA, le praticien peut faire rapport, soit sur une assertion de la direction portant sur les éléments considérés, soit directement sur les éléments en question. Lorsque le praticien fait rapport sur l'assertion de la direction, celle-ci devrait accompagner son rapport. Lorsqu'il fait rapport directement sur les éléments considérés, il n'est pas tenu d'obtenir une assertion écrite de la direction. En ce cas, cela dit, il est tenu d'établir par d'autres voies la responsabilité de la direction en ce qui concerne les éléments considérés : c'est une condition fondamentale de la réalisation de la mission.

Dans le cas d'une vérification ayant trait à la protection des renseignements personnels, on estime qu'une mission fondée sur une assertion est plus appropriée qu'une mission consistant à faire rapport directement sur les éléments considérés. En fournissant une assertion mise à la disposition du public, la direction reconnaît explicitement qu'elle est responsable des éléments considérés.

Missions d'examen de la protection des renseignements personnels

Une *mission d'examen* constitue un type de mission d'attestation ou de certification. Cependant, l'expression «examen de la protection des renseignements personnels» est souvent utilisée à tort pour désigner une vérification ou certains types de missions de conseil concernant la protection des renseignements personnels, par exemple une mission de diagnostic ou une mission visant à tirer des conclusions et à formuler des recommandations ayant trait à la protection des renseignements personnels. Afin de réduire le risque de voir le praticien ou le client mal interpréter les besoins ou les attentes de

⁶ Voir le chapitre 1 du Statement of Standards on Attestation Engagements (SSAE) No. 10 (AT sec. 101.58) pour une description des choix qui s'offrent au praticien, lorsqu'il n'obtient pas d'attestation de la direction.

⁷ Voir le chapitre 1 du SSAE No. 10 (AT sec. 101.64).

l'autre partie, le praticien devrait s'entendre avec le client sur les détails du service à fournir et le type de rapport à délivrer.

Une mission d'examen, au sens où l'on entend ce terme dans les normes professionnelles, est un type de mission d'attestation ou de certification qui consiste, pour le praticien, à indiquer dans un rapport s'il a découvert des informations, compte tenu des travaux effectués, signalant que les éléments considérés ne sont pas conformes à certains critères ou que l'assertion de la direction ne donne pas une image fidèle des éléments considérés à tous les égards importants, au regard de certains critères. Les procédures mises en œuvre pour étayer le rapport d'examen du praticien se limitent à la prise de renseignements, aux procédures analytiques et aux entretiens. De l'avis du Groupe de travail mixte AICPA-ICCA sur la protection des renseignements personnels, ces types de procédures et l'assurance limitée que procure une mission d'examen ne seraient pas adéquats pour répondre aux besoins de la plupart des parties ayant des exigences ou des attentes en matière de protection des renseignements personnels dans le cas où on attend de l'entité qui fait rapport qu'elle démontre sa conformité avec les principes et les critères généralement reconnus en matière de protection des renseignements personnels. En conséquence, il n'est fourni aucune indication sur la réalisation d'une mission d'examen ayant trait aux renseignements personnels.

Missions d'application de procédés de vérification spécifiés

Dans le cadre d'une mission d'application de procédés de vérification spécifiés, le praticien met en œuvre des procédés spécifiés, convenus entre les parties⁸, et présente ses constatations. Il n'exécute pas la vérification ou l'examen d'une assertion ou des éléments considérés, et n'exprime ni une opinion ni une assurance de forme négative à l'égard de l'assertion ou des éléments considérés⁹. Dans ce type de mission, le rapport du praticien prend la forme d'une description des

8 Les utilisateurs déterminés du rapport conviennent avec le praticien des procédés qui seront mis en œuvre par ce dernier.

9 Aux États-Unis, les missions portant sur l'application de procédés spécifiés sont exécutées conformément au paragraphe .15 du chapitre 191 de l'AT. Au Canada, il n'existe pas de règles générales concernant les procédés spécifiés. Le praticien pourrait toutefois se reporter aux indications contenues dans le chapitre 9100 du Manuel de l'Institut Canadien des Comptables Agréés (ICCA), qui énonce les normes relatives à l'application de procédés de vérification spécifiés à des informations financières autres que des états financiers. Dans les missions d'application de procédés de vérification spécifiés, le praticien est chargé de faire rapport à des utilisateurs déterminés sur les résultats de l'application de procédés spécifiés. Lorsqu'il applique ces procédés, le praticien n'exprime pas de conclusion relativement aux éléments considérés parce qu'il ne met pas nécessairement en œuvre tous les procédés qui, selon son jugement, seraient nécessaires pour fournir un niveau d'assurance élevé. Le rapport du praticien énonce plutôt les résultats factuels de l'application des procédés, y compris les exceptions relevées.

procédés mis en œuvre et des constatations dégagées. Les principes et les critères généralement reconnus en matière de protection des renseignements personnels peuvent être appliqués dans le cadre de ces missions. Ce type de travail n'aboutirait pas à la délivrance d'un rapport du vérificateur, mais d'un rapport qui présente les procédés spécifiés et les constatations respectivement correspondantes. Les procédés spécifiés pourraient porter sur un sous-ensemble du système de l'entité ou un sous-ensemble des principes ou encore les deux. Ainsi, une entité peut demander à un praticien d'appliquer des procédés spécifiés en utilisant des critères choisis parmi les principes généralement reconnus en matière de protection des renseignements personnels et de présenter ses constatations. Au Canada, les missions portant sur des procédés spécifiés sont permises, bien qu'elles ne soient pas considérées comme des missions de certification au sens du chapitre 5025 du *Manuel de l'ICCA – Certification*.

À l'instar des besoins des utilisateurs, la nature, le calendrier d'application et l'étendue des procédés spécifiés peuvent varier considérablement. Par conséquent, les utilisateurs déterminés et le client ont la responsabilité de déterminer si les procédés spécifiés sont suffisants, car ils sont les plus à même de connaître leurs propres besoins. L'utilisation d'un tel rapport se limite aux parties spécifiées qui ont convenu des procédés à appliquer.

Liens entre les principes généralement reconnus en matière de protection des renseignements personnels et les principes et critères des services Trust

Les principes généralement reconnus en matière de protection des renseignements personnels font partie des *Principes et critères des services Trust* de l'ICCA et de l'AICPA, qui sont fondés sur un cadre de référence commun (c'est-à-dire un ensemble de principes et critères de base) pour la prestation de services professionnels d'attestation ou de certification ainsi que de conseil. Les *Principes et critères des services Trust*¹⁰ ont été élaborés par des groupes de travail formés de bénévoles, sous les auspices de l'ICCA et de l'AICPA. Les autres principes et critères des services Trust sont les suivants :

¹⁰WebTrust et SysTrust correspondent à deux offres de services spécifiques élaborées par l'ICCA et l'AICPA qui sont fondés sur les *Principes et critères des services Trust*. Les praticiens doivent détenir un permis de l'ICCA pour pouvoir utiliser les sceaux WebTrust ou SysTrust. Lorsque la mission ayant trait à la protection des renseignements personnels englobe une unité d'exploitation en ligne et que l'entité a reçu un rapport de vérification ne comprenant ni réserve ni limitation de l'étendue des travaux, l'entité peut choisir d'afficher le sceau WebTrust pour la protection des renseignements personnels en ligne. Pour de plus amples renseignements sur l'obtention de permis et les missions sur la protection des renseignements personnels en ligne, voir www.webtrust.org.

Sécurité. Le système est protégé contre les accès non autorisés (aussi bien physiques que logiques).

Accessibilité. Le système est accessible à des fins d'exploitation et d'utilisation, comme promis ou convenu.

Intégrité du traitement. Le système effectue un traitement intégral, exact, rapide et dûment autorisé.

Confidentialité. Les renseignements désignés comme étant confidentiels sont protégés comme promis ou convenu.

Les principes et critères sont décrits plus en détail sur www.aicpa.org/TrustServices.

Annexe C – Modèles de rapports du vérificateur portant sur la protection des renseignements personnels

La présente annexe comprend des modèles de rapports du vérificateur établis selon les normes professionnelles d'information applicables de l'AICPA et de l'ICCA respectivement :

Selon les normes d'attestation de l'AICPA

Modèle n° 1 – Rapport sur l'assertion de la direction et Exemple d'assertion de la direction

Modèle n° 2 – Rapport portant directement sur les éléments considérés

Selon les normes de certification de l'ICCA

Modèle n° 3 – Rapport sur l'assertion de la direction et Exemple d'assertion de la direction

Modèle n° 4 – Rapport portant directement sur les éléments considérés

Modèle n° 1 – Rapport sur l’assertion de la direction, établi selon les normes d’attestation de l’AICPA

Rapport du praticien indépendant sur la protection des renseignements personnels

À la direction de la société ABC inc. :

Nous avons vérifié l’assertion de la direction de la société ABC inc. (la société ABC) selon laquelle, au cours de la période du xx xxxx 2009 au yy yyyy 2009, la société ABC :

a exercé des contrôles efficaces relativement à la protection des renseignements personnels recueillis dans le cadre de _____ [*description des entités et activités visées, par exemple «les activités de ventes postales par catalogue»*] (l’«activité») de façon à fournir l’assurance raisonnable que ces renseignements ont été recueillis, utilisés, conservés, communiqués et supprimés conformément aux engagements énoncés dans son avis sur la protection des renseignements personnels relatif à l’activité et aux critères établis dans le cadre des principes généralement reconnus en la matière publiés par l’Institut Canadien des Comptables Agréés (ICCA) et l’American Institute of Certified Public Accountants (AICPA);

a respecté les engagements énoncés dans son avis sur la protection des renseignements personnels, daté du xx xxxx 2009 et [disponible sur www.société-ABC/protection_renseignements_personnels ou joint au présent rapport].

La responsabilité de cette assertion incombe à la direction de la société ABC. Notre responsabilité consiste à exprimer une opinion en nous fondant sur notre vérification.

Notre vérification a été effectuée conformément aux normes d’attestation établies par l’American Institute of Certified Public Accountants et a donc consisté 1) à acquérir une compréhension des contrôles exercés par la société ABC relativement à la protection des renseignements personnels, 2) à tester et à évaluer l’efficacité du fonctionnement de ces contrôles, 3) à vérifier si la société a respecté les engagements énoncés dans son avis sur la protection des renseignements personnels et 4) à mettre en œuvre les autres procédés que nous avons

jugés nécessaires dans les circonstances. Nous estimons que notre vérification constitue une base raisonnable à l'expression de notre opinion.

À notre avis, l'assertion de la direction de la société ABC selon laquelle, au cours de la période du xx xxxx 2009 au yy yyyy 2009, la société ABC :

a exercé des contrôles efficaces relativement à la protection des renseignements personnels recueillis dans le cadre de l'activité de façon à fournir l'assurance raisonnable que ces renseignements ont été recueillis, utilisés, conservés, communiqués et supprimés conformément aux engagements énoncés dans son avis sur la protection des renseignements personnels relatif à l'activité et aux critères établis dans le cadre des principes généralement reconnus en la matière;
a respecté les engagements énoncés dans son avis sur la protection des renseignements personnels susmentionné,

donne, à tous les égards importants, une image fidèle de la réalité.

OU

À notre avis, l'assertion de la direction de la société ABC dont il est fait état plus haut donne, à tous les égards importants, une image fidèle de la réalité, qui est conforme à l'avis sur la protection des renseignements personnels susmentionné donné par la société ABC et aux critères établis dans le cadre des principes généralement reconnus en la matière.

La nature et les limites inhérentes des contrôles peuvent affecter la capacité de la société ABC à satisfaire aux critères susmentionnés et aux engagements énoncés dans son avis sur la protection des renseignements personnels. Par exemple, il se peut que des fraudes, des accès non autorisés aux systèmes et aux renseignements ou des cas de non-respect des politiques ou des obligations internes ou externes surviennent et ne soient pas détectés. Par ailleurs, l'extrapolation de conclusions fondées sur nos constatations à des périodes futures est risquée dans la mesure où des changements ou des événements futurs peuvent altérer la validité de ces conclusions.

[Nom du cabinet de CPA]
Certified Public Accountants
[Ville, État]
[Date]

Exemple d’assertion de la direction en rapport avec le modèle n° 1

Au cours de la période du xx xxxx 2009 au yy yyyy 2009, la société ABC a, à tous les égards importants :

exercé des contrôles efficaces relativement à la protection des renseignements personnels recueillis dans le cadre de _____ [*description des entités et activités visées, par exemple «les activités de ventes postales par catalogue»*] (l’«activité») de façon à fournir l’assurance raisonnable que ces renseignements ont été recueillis, utilisés, conservés, communiqués et supprimés conformément aux engagements énoncés dans notre avis sur la protection des renseignements personnels relatif à l’activité et aux critères établis dans le cadre des principes généralement reconnus en la matière publiés par l’Institut Canadien des Comptables Agréés (ICCA) et l’American Institute of Certified Public Accountants (AICPA);
respecté les engagements énoncés dans notre avis sur la protection des renseignements personnels, daté du xx xxxx 2009 et [disponible sur www.société-ABC/protection_renseignements_personnels ou joint au présent rapport].

Modèle n° 2 – Rapport portant directement sur les éléments considérés, établi selon les normes d’attestation de l’AICPA

Rapport du praticien indépendant sur la protection des renseignements personnels

À la direction de la société ABC inc. :

Nous avons vérifié 1) l’efficacité des contrôles exercés par la société ABC inc. (la société ABC) sur les renseignements personnels recueillis dans le cadre de _____ [*description des entités et activités visées, par exemple «les activités de ventes postales par catalogue»*] (l’«activité») de façon à fournir l’assurance raisonnable que ces renseignements ont été recueillis, utilisés, conservés, communiqués et supprimés conformément aux engagements énoncés dans son avis sur la protection des renseignements personnels et aux critères établis dans le cadre des principes généralement reconnus en la matière publiés par l’Institut Canadien des Comptables Agréés et l’American Institute of Certified Public Accountants (AICPA), et 2) le respect, par la société ABC, des engagements énoncés dans son avis sur la protection des renseignements personnels, daté du xx xxxx 2009 et [disponible sur www.société-ABC/protection_renseignements_personnels ou joint au présent rapport] relatif à l’activité au cours de la période du xx xxxx 2009 au yy yyyy 2009. La responsabilité du maintien de l’efficacité de ces contrôles et du respect des engagements énoncés dans l’avis sur la protection des renseignements personnels incombe à la direction de la société ABC. Notre responsabilité consiste à exprimer une opinion en nous fondant sur notre vérification.

Notre vérification a été effectuée conformément aux normes d’attestation établies par l’AICPA et a donc consisté 1) à acquérir une compréhension des contrôles exercés par la société ABC relativement à la protection des renseignements personnels, 2) à tester et à évaluer l’efficacité du fonctionnement de ces contrôles, 3) à vérifier si la société a respecté les engagements énoncés dans son avis sur la protection des renseignements personnels et 4) à mettre en œuvre les autres procédés que nous avons jugés nécessaires dans les circonstances. Nous estimons que notre vérification constitue une base raisonnable à l’expression de notre opinion.

À notre avis, au cours de la période du xx xxxx 2009 au yy yyyy 2009, la société ABC a, à tous les égards importants, 1) exercé des contrôles efficaces relativement à la protection des renseignements personnels

recueillis dans le cadre de l'activité, de façon à fournir l'assurance raisonnable que ces renseignements ont été recueillis, utilisés, conservés, communiqués et supprimés conformément aux engagements énoncés dans son avis sur la protection des renseignements personnels et aux critères établis dans le cadre des principes généralement reconnus en la matière publiés par l'ICCA et l'AICPA, et 2) respecté les engagements énoncés dans son avis sur la protection des renseignements personnels susmentionné.

La nature et les limites inhérentes des contrôles peuvent affecter la capacité de la société ABC à satisfaire aux critères susmentionnés et aux engagements énoncés dans son avis sur la protection des renseignements personnels. Par exemple, il se peut que des fraudes, des accès non autorisés aux systèmes et aux renseignements ou des cas de non-respect des politiques ou des obligations internes ou externes surviennent et ne soient pas détectés. Par ailleurs, l'extrapolation de conclusions fondées sur nos constatations à des périodes futures est risquée dans la mesure où des changements ou des événements futurs peuvent altérer la validité de ces conclusions.

[Nom du cabinet de CPA]
Certified Public Accountants
[Ville, État]

[Date]

Modèle n° 3 – Rapport sur l’assertion de la direction, établi selon les normes de certification de l’ICCA

Rapport du vérificateur sur la protection des renseignements personnels

À la direction de la société ABC inc. :

Nous avons vérifié l’assertion de la direction de la société ABC inc. (la société ABC) selon laquelle, au cours de la période du xx xxxx 2009 au yy yyyy 2009, la société ABC :

a exercé des contrôles efficaces relativement à la protection des renseignements personnels recueillis dans le cadre de _____ [*description des entités et activités visées, par exemple «les activités de ventes postales par catalogue»*] (l’«activité») de façon à fournir l’assurance raisonnable que ces renseignements ont été recueillis, utilisés, conservés, communiqués et supprimés conformément aux engagements énoncés dans son avis sur la protection des renseignements personnels relatif à l’activité et aux critères établis dans le cadre des principes généralement reconnus en la matière publiés par l’Institut Canadien des Comptables Agréés (ICCA) et l’American Institute of Certified Public Accountants (AICPA);

a respecté les engagements énoncés dans son avis sur la protection des renseignements personnels, daté du xx xxxx 2009 et [disponible sur www.société-ABC/protection_renseignements_personnels ou joint au présent rapport].

La responsabilité de cette assertion incombe à la direction. Notre responsabilité consiste à exprimer une opinion en nous fondant sur notre vérification.

Notre vérification a été effectuée conformément aux normes relatives aux missions de certification établies par l’ICCA. Ces normes exigent que la vérification soit planifiée et exécutée de manière à fournir une assurance raisonnable sur laquelle sera fondée notre opinion. Notre vérification a consisté 1) à acquérir une compréhension des contrôles exercés par la société ABC relativement à la protection des renseignements personnels, 2) à tester et à évaluer l’efficacité du fonctionnement de ces contrôles, 3) à vérifier si la société a

respecté les engagements énoncés dans son avis sur la protection des renseignements personnels et 4) à mettre en œuvre les autres procédés que nous avons jugés nécessaires dans les circonstances. Nous estimons que notre vérification constitue une base raisonnable à l'expression de notre opinion.

À notre avis, l'assertion de la direction de la société ABC selon laquelle, au cours de la période du xx xxxx 2009 au yy yyyy 2009, la société ABC :

a exercé des contrôles efficaces relativement à la protection des renseignements personnels recueillis dans le cadre de l'activité de façon à fournir l'assurance raisonnable que ces renseignements ont été recueillis, utilisés, conservés, communiqués et supprimés conformément aux engagements énoncés dans son avis sur la protection des renseignements personnels et aux critères établis dans le cadre des principes généralement reconnus en la matière;
a respecté les engagements énoncés dans son avis sur la protection des renseignements personnels susmentionné,

donne, à tous les égards importants, une image fidèle de la réalité.

OU

À notre avis, l'assertion de la direction de la société ABC dont il est fait état plus haut donne, à tous les égards importants, une image fidèle de la réalité, qui est conforme à l'avis sur la protection des renseignements personnels susmentionné donné par la société ABC et aux critères établis dans le cadre des principes généralement reconnus en la matière.

La nature et les limites inhérentes des contrôles peuvent affecter la capacité de la société ABC à satisfaire aux critères susmentionnés et aux engagements énoncés dans son avis sur la protection des renseignements personnels. Par exemple, il se peut que des fraudes, des accès non autorisés aux systèmes et aux renseignements ou des cas de non-respect des politiques ou des obligations internes ou externes surviennent et ne soient pas détectés. Par ailleurs, l'extrapolation de conclusions fondées sur nos constatations à des périodes futures est risquée dans la mesure où des changements ou des événements futurs peuvent altérer la validité de ces conclusions.

[*Nom du cabinet de CA*]
Comptables agréés

[*Ville (Province)*]
[Date]

Exemple d’assertion de la direction en rapport avec le modèle n° 3

Au cours de la période du xx xxxx 2009 au yy yyyy 2009, la société ABC a, à tous les égards importants :

exercé des contrôles efficaces relativement à la protection des renseignements personnels recueillis dans le cadre de _____ [*description des entités et activités visées, par exemple «les activités de ventes postales par catalogue»*] (l’«activité») de façon à fournir l’assurance raisonnable que ces renseignements ont été recueillis, utilisés, conservés, communiqués et supprimés conformément aux engagements énoncés dans notre avis sur la protection des renseignements personnels relatif à l’activité et aux critères établis dans le cadre des principes généralement reconnus en la matière publiés par l’Institut Canadien des Comptables Agréés (ICCA) et l’American Institute of Certified Public Accountants (AICPA);

respecté les engagements énoncés dans notre avis sur la protection des renseignements personnels, daté du xx xxxx 2009 et [disponible sur www.société-ABC/protection_reenseignements_personnels ou joint au présent rapport].

Modèle n° 4 – Rapport portant directement sur les éléments considérés, établi selon les normes de certification de l'ICCA

Rapport du vérificateur sur la protection des renseignements personnels

À la direction de la société ABC inc. :

Nous avons vérifié 1) l'efficacité des contrôles exercés par la société ABC inc. (la société ABC) sur les renseignements personnels recueillis dans le cadre de _____ [*description des entités et activités visées, par exemple «les activités de ventes postales par catalogue»*] (l'«activité») de façon à fournir l'assurance raisonnable que ces renseignements ont été recueillis, utilisés, conservés, communiqués et supprimés conformément aux engagements énoncés dans son avis sur la protection des renseignements personnels et aux critères établis dans le cadre des principes généralement reconnus en la matière publiés par l'Institut Canadien des Comptables Agréés (ICCA) et l'American Institute of Certified Public Accountants (AICPA), et 2) le respect, par la société ABC, des engagements énoncés dans son avis sur la protection des renseignements personnels, daté du xx xxxx 2009 et [disponible sur www.société-ABC/protection_renseignements_personnels ou joint au présent rapport], relatif à l'activité au cours de la période du xx xxxx 2009 au yy yyyy 2009. La responsabilité du maintien de l'efficacité de ces contrôles et du respect des engagements énoncés dans l'avis sur la protection des renseignements personnels incombe à la direction de la société ABC. Notre responsabilité consiste à exprimer une opinion en nous fondant sur notre vérification.

Notre vérification a été effectuée conformément aux normes relatives aux missions de certification établies par l'ICCA. Ces normes exigent que la vérification soit planifiée et exécutée de manière à fournir une assurance raisonnable sur laquelle sera fondée notre opinion. Notre vérification a consisté 1) à acquérir une compréhension des contrôles exercés par la société ABC relativement à la protection des renseignements personnels, 2) à tester et à évaluer l'efficacité du fonctionnement de ces contrôles, 3) à vérifier si la société a respecté les engagements énoncés dans son avis sur la protection des renseignements personnels et 4) à mettre en œuvre les autres procédés que nous avons jugés nécessaires dans les circonstances. Nous estimons que notre vérification constitue une base raisonnable à l'expression de notre opinion.

À notre avis, au cours de la période du xx xxxx 2009 au yy yyyy 2009, la société ABC a, à tous les égards importants, 1) exercé des contrôles efficaces relativement à la protection des renseignements personnels recueillis dans le cadre de l'activité, de façon à fournir l'assurance raisonnable que ces renseignements ont été recueillis, utilisés, conservés, communiqués et supprimés conformément aux engagements énoncés dans son avis sur la protection des renseignements personnels et aux critères établis dans le cadre des principes généralement reconnus en la matière, et 2) respecté les engagements énoncés dans son avis sur la protection des renseignements personnels susmentionné.

La nature et les limites inhérentes des contrôles peuvent affecter la capacité de la société ABC à satisfaire aux critères susmentionnés et aux engagements énoncés dans son avis sur la protection des renseignements personnels. Par exemple, il se peut que des fraudes, des accès non autorisés aux systèmes et aux renseignements ou des cas de non-respect des politiques ou des obligations internes ou externes surviennent et ne soient pas détectés. Par ailleurs, l'extrapolation de conclusions fondées sur nos constatations à des périodes futures est risquée dans la mesure où des changements ou des événements futurs peuvent altérer la validité de ces conclusions.

[*Nom du cabinet de CA*]
Comptables agréés

[*Ville (Province)*]
[Date]