

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

Introduction

Pour la plupart des organisations, la gestion de la protection des renseignements personnels¹ au niveau local, national ou international comporte des défis. Bon nombre 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 ont été élaborés selon le point de vue des entreprises, en fonction des textes réglementaires importants à l'échelle nationale et internationale. Les principes 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 devant être remplis. 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.

Le présent document décrit les principes généralement reconnus en matière de protection des renseignements personnels que toutes les organisations peuvent adopter dans le cadre de leur programme de protection des renseignements personnels. Ces principes visent à permettre à la direction de mettre au point un programme efficace qui prend en compte les risques et les obligations rattachés à la protection des renseignements personnels ainsi que les occasions d'affaires. 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.

L'introduction ainsi que les principes généralement reconnus et les critères en matière de protection des renseignements personnels seront utiles aux personnes qui :

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.

- 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;
- 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

La qualité des pratiques en matière de protection des renseignements personnels relève d'une saine gestion de l'entreprise. 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 essentiel 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 mais, en même temps, ils doivent gérer 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 quelques 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.

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

Pour les organisations actives dans plusieurs ressorts territoriaux, 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 partout dans le monde. De nombreux pays ont réglementé la circulation transfrontalière des données. Citons notamment les directives de 1995 et 1997 de l'Union européenne 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'Union. 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 doivent tenter 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 nouveaux règlements.

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 parfois plus stricte. Cela accroît le risque qu'une organisation commette par inadvertance une infraction qui défraiera ensuite la chronique dans le pays hôte concerné.

Impartition et protection des renseignements personnels

L'impartition accroît la complexité de la protection des renseignements personnels. Une organisation peut externaliser une partie de ses processus d'affaires et, de ce fait, une partie de sa responsabilité en matière de protection des renseignements personnels. Cependant, elle ne peut donner en impartition sa responsabilité à l'égard de la protection des renseignements personnels inhérents à ses processus d'affaires. La complexité augmente lorsque les services impartis sont confiés à une entité d'un autre pays qui peut être assujettie à une réglementation différente en matière de protection des renseignements personnels, 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 principes généralement reconnus en matière de protection des renseignements personnels et les critères connexes décrits dans le présent document 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 à qui les services ont été confiés et à qui une partie de la responsabilité en matière de protection des renseignements personnels a été transférée.

L'application de ces principes à l'échelle mondiale peut rassurer les impartiteurs 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 en matière d'information équitables et reconnues à l'échelle internationale, recensées dans de nombreux textes légaux et réglementaires de divers pays concernant la protection des renseignements personnels, et sur des pratiques considérées comme bonnes.

En quoi consiste la protection des renseignements personnels?

Définition de la protection des renseignements personnels

Selon les principes généralement reconnus en la matière, la protection des renseignements personnels s'entend *des droits et des obligations des individus et des organisations en ce qui concerne la collecte, l'utilisation, la conservation et la communication des renseignements personnels.*

Renseignements personnels

Les *renseignements personnels* sont des renseignements qui concernent ou sont susceptibles de concerner un individu identifiable, ou qui sont reliés ou susceptibles d'être reliés à un individu identifiable. Le terme 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, l'utilisation de renseignements sensibles peut nécessiter un [consentement](#) explicite plutôt qu'implicite.

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.

Protection des renseignements personnels ou confidentialité?

Contrairement aux renseignements permettant d'identifier une personne, qui sont souvent définis dans les textes réglementaires de bon nombre de pays, 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. 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 (y compris WebTrust® et SysTrust®) établissent un ensemble de critères en matière de confidentialité (voir www.webtrust.org).

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

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

Les principes s'appuient sur des notions clés empruntées aux textes législatifs et aux lignes directrices d'importance à l'échelle nationale et internationale (voir l'Annexe B – Comparaison des notions internationales de protection des renseignements personnels¹) et sur les bonnes pratiques d'affaires. L'application des principes généralement reconnus en matière de protection des renseignements personnels 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. L'application des principes simplifie également 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 généralement reconnus en matière de protection des renseignements personnels sont fondés sur l'objectif suivant.

² Par exemple, l'Organisation de coopération et de développement économiques (OCDE) a publié des *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* (les «Lignes directrices») et l'Union Européenne (UE) 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 (LGLB), la *Health Insurance Portability and Accountability Act* (HIPAA) et la *Children's Online Privacy Protection Act* (COPPA). 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 à l'Annexe B les URL des sites Web de ces textes sur la protection des renseignements personnels, et d'autres textes. Le respect des critères énoncés dans le présent document n'aboutit pas nécessairement au respect des lois et règlements applicables en matière de protection des renseignements personnels; les entités pourraient donc juger utile de consulter un conseiller juridique compétent au sujet du respect de ces lois et règlements.

La collecte, l'utilisation, la conservation et la communication 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 généralement reconnus en matière 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 équitables 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 et conservation.** 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.
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 différends 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 servant à évaluer les politiques, les communications, les procédures et les 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/ou des 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 principes généralement reconnus en matière de protection des renseignements personnels

Les organisations peuvent utiliser les principes aux fins suivantes :

- conception et mise en œuvre des [politiques](#) de protection des renseignements personnels;
- mesure de la performance;
- étalonnage;
- surveillance et vérification des programmes de protection des renseignements personnels.

Les activités suivantes s'inscrivent dans le cadre 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 – création et institutionnalisation des solutions;
- Soutien/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 principes généralement reconnus en matière de protection des renseignements personnels 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>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 de des travaux de l’organisation aux fins de la protection des renseignements personnels, les principes généralement reconnus peuvent permettre de repérer des éléments importants devant être traités.</p>

ACTIVITÉ	DISCUSSION GÉNÉRALE	APPLICATION POSSIBLE DES PRINCIPES GÉNÉRALEMENT RECONNUS EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS
	<p>Affectation des ressources. Cette étape décrit les ressources humaines et financières affectées pour atteindre les buts et les objectifs énoncés dans le plan stratégique ou le plan d'affaires.</p>	<p>Affectation des ressources. En se fondant sur les principes généralement reconnus, 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 le budget alloué à ces activités.</p> <p>Stratégie globale. Un document stratégique décrit les avancées attendues ou prévues. Les principes généralement reconnus 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>

ACTIVITÉ	DISCUSSION GÉNÉRALE	APPLICATION POSSIBLE DES PRINCIPES GÉNÉRALEMENT RECONNUS EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS
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, la mission initiale la plus courante est une évaluation. Celle-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 principes généralement reconnus peuvent aider l'entité à comprendre ses risques de haut niveau, ses opportunités, ses besoins, ses politiques et les 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 principes généralement reconnus 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>À cette étape, un plan d'action est arrêté et/ou une recommandation est mise en œuvre. La mise en œuvre implique l'exécution de toutes les tâches, planifiées et autres, nécessaires pour rendre le plan d'action opérationnel : déterminer qui exécutera quelle tâche, affecter les responsabilités, établir les calendriers, définir les jalons, etc. 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.</p>	<p>Les principes généralement reconnus 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 convertis pour satisfaire aux exigences concernant la protection des renseignements personnels; • formulaires, dépliants et contrats mis à jour pour être conformes à la protection des renseignements personnels; • programmes internes et externes de sensibilisation à la protection des renseignements personnels.
Soutien/gestion	<p>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</p>	<p>L'entité peut appliquer les principes généralement reconnus, 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</p>

ACTIVITÉ	DISCUSSION GÉNÉRALE	APPLICATION POSSIBLE DES PRINCIPES GÉNÉRALEMENT RECONNUS EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS
	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.	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 de protection des renseignements personnels d'une entité en utilisant les principes généralement reconnus 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 CA et les CPA, peuvent fournir des services de certification. En général, une vérification externe portant sur les informations financières et non financières inspire confiance aux particuliers, à la direction, aux clients, aux partenaires d'affaires et aux autres utilisateurs.	Un vérificateur externe peut évaluer le programme de protection des renseignements personnels d'une entité en conformité avec les principes généralement reconnus en la matière et produire des rapports utiles pour les particuliers, la direction, les clients, les partenaires d'affaires et les autres utilisateurs.

Principes généralement reconnus en matière de protection des renseignements personnels

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 et des explications, vise à faire mieux comprendre 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 par exemple sur les bonnes pratiques et quelques exigences énoncées dans des textes légaux et réglementaires visant un secteur d'activité ou un pays donné.

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