

L'AICPA ET L'ICCA ACTUALISENT LES PRINCIPES GÉNÉRALEMENT RECONNUS EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS

Par Nancy A. Cohen, CPA.CITP, CIPP, et Nicholas F. Cheung, CA, CIPP/C

Des améliorations importantes ont été apportées aux *Principes généralement reconnus en matière de protection des renseignements personnels* (PPRP), dont l'établissement d'un processus d'évaluation annuelle des risques pour identifier l'évolution des risques ou les risques nouveaux auxquels sont exposés les renseignements personnels. Les PPRP sont un cadre de référence reconnu mondialement en matière de protection des renseignements personnels, qui a été élaboré par l'American Institute of Certified Public Accountants (AICPA) et l'Institut Canadien des Comptables Agréés (ICCA).

«Une évaluation annuelle des risques liés à la protection des renseignements personnels est essentielle à la compréhension de ces risques au sein d'une organisation», explique Everett C. Johnson, CPA, président du Groupe de travail mixte AICPA-ICCA sur la protection des renseignements personnels et ancien président d'ISACA. «Une fois ces risques identifiés et évalués, l'organisation peut prendre les mesures appropriées pour les atténuer. Nous avons révisé les critères des PPRP afin d'aider les organisations à atténuer les risques liés à la protection des renseignements personnels.»

Les PPRP, dont la dernière mise à jour remontait à 2006, visent à aider les dirigeants des organisations à mettre en place un programme tenant compte des risques et obligations en matière de protection des renseignements personnels ou à évaluer leur programme actuel. Ils peuvent aussi être utilisés par les CA et les CPA aux fins de la prestation de services d'audit liés à la protection des renseignements personnels. Les PPRP intègrent divers concepts tirés de textes législatifs, lignes directrices et autres ensembles de connaissances à l'échelle locale, nationale et internationale dans un objectif unique de protection des renseignements personnels. Cet objectif est soutenu par dix principes :

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 la personne concernée 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 les personnes concernées ont donné leur consentement implicite ou explicite. L'entité ne conserve les renseignements personnels que

FINAL

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 personnes concernées l'accès aux renseignements personnels les concernant, pour qu'elles 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 la personne concernée.
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.

Chacun de ces principes est étayé par des critères objectifs et mesurables relatifs au traitement des renseignements personnels au sein de l'organisation. Ces principes et les critères y afférents sont utiles aux personnes qui :

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

Les changements apportés aux PPRP, dont l'ajout de huit nouveaux critères (portant à plus de 70 leur nombre total) et la modification de deux critères existants, résultent de délibérations et de l'examen des commentaires reçus du public à la suite de l'exposé-sondage publié en mars 2009. «La protection des renseignements personnels est une responsabilité particulièrement exigeante qui incombe aux organisations, qu'il s'agisse de renseignements concernant les employés ou les clients, indique Everett C. Johnson. Nous avons révisé les critères des PPRP afin de réduire au minimum les risques d'atteinte à la protection des renseignements personnels. Nous avons amélioré les indications relatives à la sécurité, à la gestion des infractions, aux questions touchant les employés, ainsi que les indications concernant la suppression et la destruction des renseignements personnels.»

FINAL

Voici un survol des nouveaux critères :

Identification et classement des renseignements personnels (1.2.3) : 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.

Cela peut comprendre la mise en place d'un processus de classement des renseignements qui permet de les identifier et de les classer par catégories, telles que les renseignements confidentiels d'affaires, les renseignements personnels, les renseignements généraux d'affaires et les renseignements publics.

Évaluation des risques (1.2.4) : Un processus d'évaluation des risques permet à l'entité 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.

Ces 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). 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. L'ICCA et l'AICPA ont élaboré un guide pour l'évaluation des risques en matière de protection des renseignements personnels (*Privacy Risk Assessment Tool*) que les organisations pourraient trouver utile.

Gestion des atteintes à la protection des renseignements personnels et des incidents qui s'y rapportent (1.2.7) : 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. Ce programme comprend, sans toutefois s'y limiter, les éléments suivants :

- 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;

FINAL

- un processus de revue périodique des incidents survenus afin d'identifier les mises à jour à apporter au programme;
- des tests périodiques ou de cheminement assortis des mesures correctives nécessaires.

Sensibilisation et formation en matière de protection des renseignements personnels (1.2.10) :

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. «Former les employés en matière de protection des renseignements personnels contribue à prévenir les infractions, à améliorer la qualité du service à la clientèle et à démontrer l'engagement de l'organisation à l'égard de pratiques commerciales saines», explique Donald Sheehy, CA•CISA, CIPP/C, associé délégué chez Deloitte (Canada) et membre du Groupe de travail mixte AICPA-ICCA sur la protection des renseignements personnels.

Approfondissement des renseignements personnels (4.2.4) : L'entité informe les personnes concernées lorsqu'elle approfondit les renseignements que ces personnes lui fournissent ou obtient des renseignements supplémentaires sur celles-ci pour son propre usage. Ces renseignements approfondis ou supplémentaires pourraient être obtenus auprès de sources tierces, ou par des recherches en ligne, ou au moyen de l'historique de crédit ou d'achat de la personne concernée, etc.

Suppression, destruction et caviardage des renseignements personnels (5.2.3) : 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. Cela peut comprendre la suppression ou le caviardage de certains renseignements personnels, tels que le numéro de carte de crédit une fois l'opération effectuée, et l'utilisation des services de sociétés spécialisées dans la destruction sûre des renseignements personnels.

Renseignements personnels sur supports portatifs (8.2.6) : Les renseignements personnels stockés sur des supports ou des appareils portatifs sont protégés contre les accès non autorisés.

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. Les renseignements stockés sont chiffrés, protégés par mot de passe, protégés physiquement et couverts par les politiques de l'entité en matière d'accès, de conservation et de destruction. Lorsque l'emploi d'un salarié ou le contrat d'un collaborateur extérieur prend fin, des procédures prévoient la restitution ou la destruction des supports et des appareils portatifs utilisés pour consulter ou stocker des renseignements personnels ainsi que de toute copie, imprimée ou autre, de ces renseignements.

«Les dispositifs portatifs tels que les ordinateurs portables et les cartes de mémoire flash sont commodes pour les employés, mais des mesures appropriées doivent être prises pour protéger adéquatement ces dispositifs et les données qu'ils contiennent, précise Donald Sheehy. Il faut se tenir

FINAL

au courant des progrès technologiques pour s'assurer de mettre en place des mesures appropriées pour se prémunir contre les nouvelles menaces.»

Suivi continu (10.2.5) : Des procédures de suivi continu sont mises en œuvre pour surveiller l'efficacité des contrôles sur les renseignements personnels en fonction de l'évaluation des risques et, le cas échéant, prendre en temps utile les mesures correctives nécessaires. Par exemple, si une politique prévoit que tous les employés doivent suivre une formation initiale sur la protection des renseignements personnels dans les 30 jours qui suivent leur embauche, le contrôle pourrait être l'examen du dossier des employés concernés pour voir s'il contient une pièce justificative prouvant que la formation a bien été suivie.

Les autres changements apportés aux PPRP comprennent une disposition restreignant l'utilisation des renseignements personnels pour tester et développer les processus ou les systèmes, des renvois à la norme ISO 27002 et des formulations révisées à l'intention des auditeurs qui préparent des rapports d'audit ayant trait à la protection des renseignements personnels.

Plusieurs organisations ont collaboré avec l'AICPA et l'ICCA pour élaborer les PPRP, dont l'ISACA et l'Institut des vérificateurs internes. On peut télécharger les PPRP ainsi que des ressources additionnelles sur la protection des renseignements personnels à www.aicpa.org/privacy ou à www.icca.ca/prp.

Nancy A. Cohen, CPA.CITP, CIPP (ncohen@aicpa.org) est directrice technique principale du contrôle qualité et des activités de recherche et développement à l'American Institute of Certified Public Accountants.

Nicholas F. Cheung, CA, CIPP/C (nicholas.cheung@cica.ca) est directeur de projets à l'Institut Canadien des Comptables Agréés.

Tous deux sont membres du Groupe de travail mixte AICPA-ICCA sur la protection des renseignements personnels.