

PRIVACY HORIZONS: TERRA INCOGNITA

29th International Conference of
Data Protection and Privacy Commissioners

September 25 to 28, 2007
Montreal, Canada



LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE : TERRA INCOGNITA

29^e Conférence internationale des commissaires
à la protection des données et de la vie privée

du 25 au 28 septembre 2007
Montréal, Canada

Principes généralement reconnus en matière de protection des renseignements personnels

Un cadre de référence mondial

Nicholas F. Cheung, CA, CIPP/C

L'Institut Canadien des Comptables Agréés

En quoi la protection des renseignements personnels (PRP) concerne-t-elle la profession comptable?

- La PRP relève de la gestion des risques
 - Les comptables sont des conseillers d'affaires de confiance
 - Ne peut être dissociée de l'évaluation du contrôle interne
- Les organisations ont besoin d'une certification indépendante quant à leurs pratiques de PRP
 - Les CA sont reconnus pour leur expertise en vérification
 - Toute vérification s'appuie sur des «critères appropriés»
- Expérience en normalisation
 - L'ICCA établit des normes de comptabilité et de certification pour les entreprises, les OSBL et le secteur public

Que sont les Principes généralement reconnus en matière de PRP (PPRP)?

- **Un cadre de référence pour aider toutes les entités, tant ouvertes que fermées, à concevoir leur programme de PRP et à évaluer les risques liés à la PRP**
- Mis au point par l'ICCA et l'AICPA
 - Pour établir une norme nord-américaine commune
 - Avalisés par :
 - l'ISACA – Information System and Audit Control Association
 - l'IIA – The Institute of Internal Auditors

Principes généralement reconnus en matière de PRP

- Gestion
- Avis
- Choix et consentement
- Collecte
- Utilisation et conservation
- Accès
- Communication à des tiers
- Sécurité
- Qualité
- Suivi et application

PPRP	Australie	Canada (LPRPDE)	Directive UE Protection des données	Norme mondiale
Gestion		Reddition de comptes	Avis	Reddition de comptes
Avis	Transparence	Fins, Transparence	Information à donner à la personne concernée	Fins, Transparence
Choix / consentement	Utilisation et communication	Consentement	Critères à satisfaire pour rendre légitime le traitement des données, Droit d'opposition de la personne concernée	Consentement
Collecte	Collecte, Renseignements sensibles, Anonymat	Limitation de la collecte	Principes relatifs à la qualité des données, Exemptions et restrictions	Collecte, Limitation
Utilisation et conservation	Identificateurs, Utilisation et communication	Limitation de l'utilisation, la communication et la conservation	Rendre légitime le traitement des données, Catégories spéciales de traitement, Principes relatifs à la qualité des données, Exemptions et restrictions, Droit d'opposition de la personne concernée	Limitation de l'utilisation, la communication et la conservation
Accès	Accès et rectification	Accès pour l'individu	Droit d'accès aux données pour la personne concernée	Accès
Communication	Utilisation et communication, Flux transfrontières de données	Limitation de l'utilisation, la communication et la conservation	Transfert de données à caractère personnel vers un pays tiers	Limitation de l'utilisation, la communication et la conservation
Sécurité	Sécurité des données	Mesures de protection	Confidentialité et sécurité des traitements	Sécurité
Qualité	Qualité des données	Exactitude	Principes relatifs à la qualité des données	Exactitude
Suivi et application	(Application par l'Office of the Privacy Commissioner)	Contestation de la conformité	Recours judiciaires, responsabilité et sanctions, Codes de conduite, Autorité de contrôle et groupe de PRP en matière de traitement des données à caractère personnel	Conformité

Avantages des PPRP

- Exhaustifs
 - Plus de 60 critères mesurables et pertinents
 - Plus qu'une liste de principes
- Objectifs
 - Élaborés par la profession de vérificateur
 - pour répondre aux attentes sur le plan international
 - pour créer une base de comparaison
 - entièrement accessibles, sans frais
- Pertinents
 - Généralisés et reconnus
 - Applicables pour l'évaluation des risques liés à la PRP à l'échelle de l'entreprise
- Critères appropriés pour une vérification de la PRP
 - Peut aussi servir de base pour une évaluation interne

Exemple de critères PPRP

Se c	Critères de sécurité	Exemples et explications relatifs aux critères	Autres considérations
8.2. 3	<p>Contrôles d'accès physique</p> <p>L'accès physique aux renseignements personnels, quelle qu'en soit la forme, est restreint.</p>	<p>Systèmes et procédures mis en place pour :</p> <ul style="list-style-type: none"> • gérer l'accès logique et physique aux renseignements personnels (RP), y compris en ce qui concerne les supports papier, les copies d'archives et les copies de sauvegarde; • enregistrer et surveiller l'accès aux RP; • empêcher toute destruction non autorisée ou accidentelle ou perte de RP; • enquêter sur les intrusions et les tentatives d'obtenir un accès non autorisé; • communiquer les résultats des enquêtes au responsable de la PPRP; • exercer un contrôle physique sur la diffusion de rapports contenant des RP; 	<p>Parmi les mesures de protection physique, on peut citer l'utilisation de :</p> <ul style="list-style-type: none"> • classeurs verrouillés, • cartes d'accès, • clés physiques, • journal d'accès avec signature, • autres techniques, <p>permettant de contrôler l'accès aux bureaux, aux centres de données ainsi qu'à d'autres lieux où des RP sont traités ou stockés.</p>

Rapports externes sur la PRP

- Avantages d'un certificateur externe
 - Indépendant
 - Objectif
 - Rompu aux techniques de vérification
- Pourquoi est-ce important?
 - Renforcer la confiance des clients
 - Fournir des rapports utiles aux parties prenantes internes et externes
 - Respecter certaines clauses contractuelles

Mission d'application de procédés de vérification spécifiés

- Qu'est-ce que c'est?
 - Un type de mission où les procédés sont convenus entre le client et l'expert-comptable
 - Le comptable fournit une liste de tous les écarts qu'il a relevés
 - Il ne s'agit pas d'une opinion de vérificateur
 - La diffusion du rapport est restreinte
- Quelle en est l'utilité?
 - Il se peut qu'une organisation ne soit pas prête à une vérification, mais qu'elle souhaite présenter un rapport indépendant sur la PRP
 - Possibilité d'utiliser certains critères parmi les PPRP
 - Plus économique qu'une vérification

Vérification externe

- Qu'est-ce que c'est?
 - Semblable au rapport du vérificateur utilisé pour les états financiers (PPRP plutôt que PCGR)
 - Fournit une assurance raisonnable
 - Diffusion non restreinte du rapport
- Quelle en est l'utilité?
 - Fournir une assurance aux
 - clients et clients potentiels
 - employés / membres du conseil d'administration
 - instances réglementaires et gouvernementales
 - Obtenir une assurance à l'égard des pratiques d'un fournisseur externe en matière de PRP (exigence contractuelle liée à l'externalisation)

Autres utilisations des PPRP

- Évaluation des risques liés à la PRP
 - Diagnostic des programmes de PRP nouveaux ou existants
 - Ne peut servir à la conformité aux lois
- Étalonnage
 - Par rapport aux PPRP, ou comparaison des résultats avec ceux d'évaluations précédentes
 - Utilisables en contexte local, national ou international
- Élaboration d'avis sur la PRP

Pour en savoir plus

www.icca.ca/prp

Nicholas F. Cheung, CA, CIPP/C

Directeur de projets, Nouveaux services de certification

ICCA

416-204-3251

nicholas.cheung@cica.ca

