

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

**« Dire ce que l'on fait et faire ce que l'on dit » :
Arguments et observations en faveur d'une
norme internationale de protection des
renseignements personnels**

Colin J. Bennett

Département de science politique

Université de Victoria (C.-B.)

cjb@uvic.ca

Robin Bayley

Linden Consulting Inc., Victoria (C.-B.)

rmbayley@shaw.ca

Pourquoi les organisations certifiées ISO 9001 devraient avoir de meilleures pratiques de gestion des renseignements personnels

- Les organisations ont une meilleure compréhension de leurs systèmes d'exploitation et de leurs fonds de données personnelles.
- Leur personnel est formé.
- Les organisations doivent réfléchir et répondre aux exigences réglementaires.
- Les organisations peuvent tirer parti d'une expertise extérieure grâce au processus d'évaluation de la conformité.

Exigences liées à une norme de gestion de la protection des renseignements personnels

- Traduction des principes relatifs à l'équité dans le traitement des renseignements dans une langue et une forme propres aux normes
- Prestation de conseils pour la mise en œuvre des principes dans les organisations
- Outils d'évaluation de la conformité adaptés à la taille de l'entreprise et à la sensibilité des données
- Guide de vérification
- Système d'accréditation pour les vérificateurs spécialisés dans la protection des renseignements personnels

Chevauchement entre la gestion de la qualité et la protection des données

- Transparence de la politique et de l'objectif
- Procédures liées à l'interaction avec les sujets des données
 - Règlement des plaintes
 - Demandes d'accès et de correction
 - Disposition concernant le consentement et le retrait
- Procédures de gestion des données personnelles
 - Sécurité des données
 - Qualité des données
 - Conservation des données

Motivations pour l'adoption de normes de protection de la vie privée

- Pouvoirs d'éducation et de réglementation des autorités de protection des données
- Désir de bénéficier d'un avantage concurrentiel
- Capacité de mentionner la norme dans les contrats

Initiatives visant la normalisation de la gestion de la protection des renseignements personnels

- Organismes de normalisation nationaux
 - Association canadienne de normalisation (CSA)
 - American National Standards Institute (ANSI)
- Organisation internationale de normalisation (ISO)
 - Travail du groupe JTC-1 de l'ISO et de la Commission électrotechnique internationale (CEI)
- Comité européen de normalisation/Système de normalisation de la société de l'information
- International Security, Trust and Privacy Alliance (ISTPA)