La protection de la vie privée, dès la conception des systèmes d'information *(Privacy by Design)*

Québec, le 1er juin 2017

David Henrard, CISA, CISM, CRISC

levio
AFFAIRES ET TECHNOLOGIES

ISACA®
Fiabilisez, optimisez et rentabilisez les systèmes d'information
Section de Québec

Privacy by Design (Pbd)
Sa provenance et sa signification

- Approche développée dans les années 1990 par Dr. Ann Cavoukian, commissaire à l'information et à la protection de la vie privée de l'Ontario
- Consiste à intégrer la protection de la vie privée dès la conception, l'opération et la gestion d'un système d'information ou d'un processus d'affaires
- Repose sur l'adoption de 7 principes fondamentaux

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

ISACA®
Fiabilisez, optimisez et rentabilisez les systèmes d'information
Section de Québec

Les 7 principes fondamentaux du PbD

1. Prendre des mesures **proactives** et non réactives, des mesures préventives et non correctives
2. Assurer la protection **implicite** de la vie privée
3. Intégrer la protection de la vie privée dans la conception des systèmes et des pratiques
4. Assurer une fonctionnalité intégrale selon un paradigme à **somme positive** et non à somme nulle
5. Assurer la sécurité de bout en bout, pendant toute la période de conservation des renseignements
6. Assurer la visibilité et la transparence
7. Respecter la vie privée des utilisateurs

ISACA®
Fiabilisez, optimisez et rentabilisez les systèmes d'information
Section de Québec

1. Prendre des mesures proactives et non réactives, des mesures préventives et non correctives

- En amont – doit être considérée dès les premières étapes du projet (lors de la conception)
- Nécessite l'implication de la haute direction
- Éviter la survenance d'un incident du fait de son caractère irréversible

1. Prendre des mesures proactives et non réactives, des mesures préventives et non correctives

- ✓Personne responsable de la protection de la vie privée
- ✓Rôles et responsabilités
- ✓Processus d'évaluation de la PVP
- ✓Évaluations documentées avec recommandations et feuille de route
- ✓Processus de gestion des incidents impliquant des renseignements personnels
  - ✓Politique de notification des incidents
  - ✓Processus d'évaluation post-incident
  - ✓Tests du processus
- ✓Adoption/revue des politiques de PVP
- ✓Revue de conformité
- ✓Suivi des risques et activités de remédiation
- ✓Conformité des politiques avec la législation en vigueur et les bonnes pratiques
- ✓Programme de formation et de sensibilisation
- ✓Qualification du personnel
- ✓Ententes avec les tiers
- ✓Évaluation des contrôles mis en place par les tiers
- ✓Gestion des flux transfrontaliers

2. Assurer la protection implicite de la vie privée

- Offrir un maximum de vie privée
- Protéger systématiquement les renseignements dans les systèmes d'information (TI, processus, comportement)
- Protection sans que l'individu n'ait à poser de geste
- Protection non optionnelle
- = « *Privacy by default* » – al.2 de l'article 23 du GDPR
- Seuls les renseignements personnels nécessaires seront utilisés pour le traitement
- Évaluation de la nécessité en fonction de la finalité du traitement
- Pas de collecte non nécessaire et pas de conservation au-delà de ce qui est nécessaire pour l'atteinte de la finalité (tant en quantité qu'en durée)
- Limitation par défaut du nombre de personnes ayant accès aux renseignements personnels

2. Assurer la protection implicite de la vie privée

- ✓Paramètre de confidentialité des utilisateurs
- ✓Configuration par défaut
- ✓Mécanismes et procédure de limitation de la collecte
- ✓Revue périodique de l'étendue de la collecte
- ✓Consentement explicite pour les renseignements personnels sensibles
- ✓Activités de surveillance de la collecte
- ✓Anonymisation
- ✓Dépersonnalisation
- ✓Encadrement de l'analytique

ISACA®
Fiabilisez, optimisez et rentabilisez les systèmes d'information
Section de Québec

3. Intégrer la protection de la vie privée dans la conception des systèmes et des pratiques

- Constitue un élément essentiel des fonctionnalités de base
- Intégration dans les fonctions du système sans y porter atteinte
- À intégrer dans la conception et l'architecture du système ainsi que dans les processus
- Responsabilité à différents niveaux
  - Développeurs
  - Chargés de projet
  - Responsable de programme
  - Responsable de la conformité

3. Intégrer la protection de la vie privée dans la conception des systèmes et des pratiques

- ✓Documentation technique et conception de la solution
- ✓Cycle de vie des renseignements personnels
- ✓Exigences d'évolution
- ✓Continuité des affaires et récupération après incident
- ✓Processus et procédure opérationnels
- ✓Gestion du changement

ISACA®
Fiabilisez, optimisez et rentabilisez les systèmes d'information
Section de Québec

4. Assurer une fonctionnalité intégrale selon un paradigme à somme positive et non à somme nulle

- Ne pas opposer la protection de la vie privée à d'autres objectifs comme l'atteinte des objectifs d'affaires
- Tenir compte de tous les intérêts légitimes de l'organisme
- Approche commune avec la sécurité de l'information
- Protection des renseignements personnels en lien avec les déroulement des affaires
- PVP n'est pas l'ennemi des affaires – ils sont partenaires complémentaires
- Doit être considérée par toutes les entités de l'organisation, notamment la fonction commerciale
- Doit être relayé par chacun des acteurs.
- Ne doit pas être vu comme une contrainte

4. Assurer une fonctionnalité intégrale selon un paradigme à somme positive et non à somme nulle

- ✓Solutions multifonctionnelles
- ✓Limitation des compromis non nécessaires

5. Assurer la sécurité de bout en bout, pendant toute la période de conservation des renseignements

- Protection intégrée au système avant de commencer à recueillir des renseignements
- Mesures de protection tout au long du cycle de vie des renseignements
- Assurer leur destruction
- Gestion sécurisée de bout en bout pendant toute leur période de conservation
- Responsabilité du responsable de la protection des renseignements personnels (DPO)
- Ref. article 14 du GDPR

5. Assurer la sécurité de bout en bout, pendant toute la période de conservation des renseignements

- ✓ Politique de sécurité de l'information
- ✓ Documentation des mesures de sécurité
- ✓ Connaissance des responsabilités en matière de sécurité et de PVP
- ✓ Responsabilité de la sécurité
- ✓ Sensibilisation et formation à la sécurité
- ✓ Programme de sécurité
- ✓ Inventaire et classification des renseignements personnels
- ✓ Accès aux renseignements personnels
  - ✓ Moindre privilège, besoin de savoir
  - ✓ Authentification
  - ✓ Autorisation
  - ✓ Gestion des accès
  - ✓ Séparation des tâches
  - ✓ Accès distants
  - ✓ Journalisation
  - ✓ Protection des journaux
- ✓ Contrôle des accès physiques au RP
- ✓ Protection environnementale
- ✓ Transmission de RP
  - ✓ Chiffrement
  - ✓ Réseaux externes
  - ✓ Réseaux sans fil
- ✓ Rétention et stockage des RP
- ✓ Disposition, destruction des RP
- ✓ Test des mesures de protection
  - ✓ Tests périodiques
  - ✓ Vulnérabilité
  - ✓ Mises à jour
  - ✓ rapport

ISACA®
Fiabilisez, optimisez et rentabilisez les systèmes d'information
Section de Québec

6. Assurer la visibilité et la transparence

- Vérification – maintien d'un climat de confiance
- PbD garantit au détenteur que le système fonctionne conformément aux promesses et objectifs établis
- Responsabilité – RPRP (audit interne) et équipes de développement
- Traitements doivent être visibles et transparents

6. Assurer la visibilité et la transparence

- ✓Politique et engagement organisationnel
- ✓Ouverture
  - ✓Demandes d'information et plaintes
  - ✓Transparence des politiques et des pratiques
  - ✓Information sur le responsable désigné

7. Respecter la vie privée des utilisateurs

- Privilégier les intérêts des particuliers
- Mesures strictes et implicites de PVP
- Fonctions conviviales et axées sur l'utilisateur
- Être conforme aux attentes des utilisateurs et aux exigences légales
- Nécessite l'engagement de tous les effectifs de l'organisation

7. Respecter la vie privée des utilisateurs

- ✓Information sur l'objectif de la collecte
- ✓Information et consentement
  - ✓Terminologie claire et concise pour effectuer un choix
  - ✓Mise à jour des préférences
  - ✓Conséquences sur la non fourniture des renseignements personnels
  - ✓Retrait du consentement
  - ✓Type de consentement requis
  - ✓Consentement explicite pour les renseignements personnels sensibles
  - ✓Consentement pour les nouvelles utilisations
- ✓Droit d'accès et de rectification des individus sur leurs renseignements personnels
- ✓Droit à l'effacement et droit de refus
- ✓Précision des renseignements personnels

ISACA®
Fiabilisez, optimisez et rentabilisez les systèmes d'information
Section de Québec

Les avantages du PbD

- Renforcer la confiance des utilisateurs / des clients
- Se distinguer de la compétition
- Limiter les risques pour les individus mais aussi pour l'organisation
- Se conformer à la loi

Références

- Commissariat à l'information et à la vie privée de l'Ontario
  https://www.ipc.on.ca/privacy/protecting-personal-information/privacy-by-design/

- Ryerson University – Privacy & Big Data Institute – Deloitte
  « Privacy by Design Certification Programm: Assessment Control Framework »
  http://www.ryerson.ca/pbdi/privacy-by-design/certification/

Merci !

David Henrard, CISA, CISM, CRISC

david.henrard@levio.ca

david.henrard@isaca-quebec.ca

levio
AFFAIRES ET TECHNOLOGIES

ISACA®
Fiabilisez, optimisez et rentabilisez les systèmes d'information
Section de Québec