Directives sur les exigences minimales qu'un système de gestion de la protection des données doit remplir

(Directives sur la certification de l'organisation et de la procédure)

du 16 juillet 2008

Le Préposé fédéral à la protection des données et à la transparence,

vu l'art. 11, al. 2, de la loi fédérale du 19 juin 1992 sur la protection des données (LPD)[1],

vu l'art. 4, al. 3, de l'ordonnance du 28 septembre 2007 sur les certifications en matière de protection des données (OCPD)[2],

édicte les directives suivantes:

1. But

1 Les présentes directives fixent les exigences minimales qu'un système de gestion de la protection des données (SGPD) doit remplir pour obtenir une certification de l'organisation ou de la procédure au sens de l'art. 4 OCPD.

2 Elles visent à fournir un modèle d'établissement, de mise en œuvre, de fonctionnement, de surveillance, de réexamen, de mise à jour et d'amélioration d'un SGPD.

3 Elles s'appliquent à tous les types d'organisation.

2. Définitions

En complément aux définitions des chapitres 3.1 à 3.16 de la norme ISO/CEI 27001:2005[3], on entend par:

a. *gestion de la conformité* les activités coordonnées d'une organisation pour respecter les exigences légales et réglementaires auxquelles elle est soumise, en particulier toutes celles liées à la protection des données;

b. *appréciation de non-conformité* l'ensemble du processus d'analyse de non-conformité et d'évaluation de non-conformité;

c. *analyse de non-conformité* l'utilisation systématique d'informations pour identifier les sources de non-conformité et estimer la non-conformité;

1 RS **235.1**
2 RS **235.13**
3 «Systèmes de gestion de la sécurité de l'information – Exigences», disponible sous licence en format papier ou PDF auprès de www.iso.org.

d. *évaluation de non-conformité* le processus de comparaison de la non-conformité estimée avec des critères de conformité donnés pour en déterminer l'importance (nature mineure ou majeure);

e. *traitement de non-conformité* le processus de sélection et implémentation de mesures visant à remédier à une non-conformité[4].

3. Réalisation

[1] Un SGPD répond aux exigences minimales s'il se fonde sur des référentiels internationaux en usage, en particulier la norme ISO 27001 interprétée au sens de l'al. 2 et complétée ou amendée conformément au point 4.

[2] Les exigences de la norme ISO 27001 portant sur le système de gestion de la sécurité de l'information (SGSI) doivent être reprises en transposant la notion de sécurité de l'information (SI) par celle de protection des données (PD) et en remplaçant son annexe A, qui correspond à la table des matières de la norme ISO/CEI 27002:2005[5], par les objectifs et mesures énumérés au point 5.

4. Mise en œuvre (exigences minimales)

Le SGPD mis en place par l'organisation doit contenir à tout le moins les exigences minimales décrites dans la norme ISO 27001 et tenir compte des aspects de protection des données suivants:

a. De manière générale, la notion de (non-)conformité relative aux exigences de protection des données complète systématiquement celle de risques relatifs aux objectifs de sécurité d'information. Une analyse de conformité excluant toute non-conformité résiduelle complète ainsi l'analyse de risques prévue dans la norme ISO 27001.

b. De manière spécifique dans l'établissement du SGPD, les points suivants de la norme ISO 27001 doivent être interprétés comme suit:

   4.2.1. a. le domaine d'application et les limites du SGPD sont définis conformément à l'art. 4, al. 1, OCPD;

   4.2.1. b. la politique pour le SGPD correspond à la charte de protection des données visée à l'art. 4, al. 2, let. a, OCPD;

   4.2.1. d 1. les actifs de type fichier (art. 3, let. g, LPD) et leur propriétaire, en l'occurrence le maître du fichier (art. 3, let. i, LPD), sont identifiés en particulier;

   4.2.1. g. les objectifs et mesures de protection des données proprement dites définis au point 5 sont sélectionnés comme partie intégrante

4 A défaut, il est possible d'éviter une non-conformité, par exemple en renonçant au traitement concerné. Il est par contre interdit d'accepter ou de transférer une non-conformité.

5 «Code de bonne pratique pour la gestion de la sécurité de l'information», disponible sous licence en format papier ou PDF auprès de www.iso.org.

du processus, dans la mesure où ils peuvent satisfaire à ces exigences;

4.3.1. j[6]. la documentation du SGPD inclut au minimum l'inventaire des fichiers non déclarés (cf. point 5, let. h, ch. 2).

5. Objectifs et mesures

Lors de l'élaboration du SGPD, les objectifs et mesures[7] suivants doivent être réalisés:

a. Licéité (art. 4, al. 1, LPD)
   1. Motifs justificatifs (art. 13 LPD)
   2. Base légale (art. 17, 19 et 20 LPD)
   3. Traitement de données par un tiers (art. 10*a*, al. 1, LPD)

b. Transparence
   1. Bonne foi (art. 4, al. 2, LPD)
   2. Reconnaissabilité (art. 4, al. 4, LPD)
   3. Obligation d'informer (art. 7*a*, al. 1, LPD)

c. Proportionnalité
   1. Traitement proportionnel (art. 4, al. 2, LPD)

d. Finalité (art. 4, al. 3 LPD)
   1. Spécification/Modification de la finalité (art. 3, let. i, LPD)
   2. Limitation d'utilisation

e. Exactitude des données
   1. Exactitude des données (art. 5, al. 1, LPD)
   2. Rectification des données (art. 5, al. 2, LPD)

f. Communication transfrontière de données (art. 6, al. 1, LPD)
   1. Niveau de protection adéquat (art. 6, al. 2, LPD)

6 Lettre additionnelle à la norme ISO 27001.

7 Les objectifs et mesures énumérés proviennent directement et sont alignés sur ceux du «Code de bonne pratique pour la gestion de la protection des données» (le texte peut être consulté sous www.edoeb.admin.ch). Le tableau des mesures n'est pas exhaustif et une organisation y ajouter d'autres objectifs ou mesures. Les objectifs et mesures de ce tableau doivent être sélectionnés comme partie intégrante du processus d'application du SGPD. Le « Code de bonne pratique pour la gestion de la protection des données » fournit des recommandations de mise en œuvre et des lignes directrices afférentes aux meilleures pratiques, venant à l'appui des mesures proposées. Ce guide est le pendant de la norme ISO 27002 («Code de bonne pratique pour la gestion de la sécurité de l'information»). Les neuf objectifs retenus sont directement tirés de la LPD et les 20 mesures associées sont structurées conformément à la norme ISO 27002.

g. Sécurité des données (art. 7 LPD)
   1. Confidentialité des données
   2. Intégrité des données
   3. Disponibilité des données
   4. Traitement de données par un tiers (art 10*a*, al. 2, LPD)

h. Enregistrement des fichiers (art. 11*a*, al. 1, LPD et art. 12*b*, al. 1, OLPD)
   1. Obligation de déclarer (art. 11*a*, al. 2 et 3; exceptions art. 11*a*, al. 5, let. e et f, LPD)
   2. Inventaire des fichiers non déclarés (art. 12*b*, al. 1, let. b, OLPD)

i. Droit d'accès et de procédure
   1. Droit d'accès à ses propres données (art. 8, al. 1, LPD)
   2. Prétentions et procédures (art. 15 et 25 LPD)

6. Entrée en vigueur

Les présentes directives entrent en vigueur le 1er septembre 2008.

16 juillet 2008

Le Préposé fédéral à la protection des données et à la transparence:

Hanspeter Thür