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 19 mars 2014

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 termes et définitions des ch. 2.1 à 2.89 de la norme ISO/CEI 27000:2014[3], on entend par:

a. *management de la conformité:* les activités coordonnées visant à diriger et contrôler une organisation du point de vue de la conformité, en particulier celles liées à la protection des données;

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

c. *analyse de non-conformité:* processus mis en œuvre pour comprendre la nature d'une non-conformité et pour déterminer le niveau de non-conformité

1 RS **235.1**
2 RS **235.13**
3 «Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire», disponible sous licence en format papier ou PDF auprès de www.iso.org.

(son importance exprimée en termes de combinaison des conséquences et de leur vraisemblance);

d. *évaluation de non-conformité:* le processus de comparaison des résultats de l'analyse de non-conformité avec les critères de conformité, afin de déterminer si la non-conformité ou son importance sont acceptables;

e. *traitement de non-conformité:* le processus destiné à modifier (atténuer, éliminer, prévenir, réduire ou éviter, mais pas accepter, partager ou transférer) la non-conformité.

3. Réalisation

[1] Un SGPD répond aux exigences minimales s'il se fonde sur des référentiels internationaux en usage, en particulier la norme ISO/CEI 27001:2013[4] interprétée au sens de l'al. 2 et complétée ou amendée conformément au ch. 4.

[2] Les exigences de la norme ISO 27001 portant sur le système de management de la sécurité de l'information (SMSI) doivent être reprises en remplaçant la notion de sécurité de l'information (SI) par celle de protection des données (PD) et l'annexe A de la norme ISO 27001, qui correspond à la table des matières de la norme ISO/CEI 27002:2013[5], par les objectifs et mesures énumérés au ch. 5.

4. Mise en œuvre (exigences minimales)

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

a. De manière générale, la notion de (non-)conformité 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 ch. suivants de la norme ISO 27001 doivent être interprétés comme suit:

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

   5.2. la politique de protection des données[6] correspond à la charte de protection des données visée à l'art. 4, al. 2, let. a, OCPD;

4 «Systèmes de management de la sécurité de l'information – Exigences», disponible sous licence en format papier, ePub ou PDF auprès de www.iso.org.

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

6 Cette politique de protection des données de niveau supérieur est étayée par d'autres politiques thématiques de sécurité de l'information ou de protection de la vie privée décrites dans la mesure A.5.1.1.

6.1.2.c.2. 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;

6.1.3.b. les objectifs et mesures de protection des données proprement dites définis au ch. 5 sont sélectionnés comme partie intégrante du processus, dans la mesure où ils peuvent satisfaire à ces exigences;

7.5.1.c[7]. la documentation du SGPD inclut au minimum l'inventaire des fichiers non déclarés (cf. ch. 5, let. h, ch. 2).

5. Objectifs et mesures

Lors de l'élaboration du SGPD, les objectifs et mesures[8] 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);

7 Lettre additionnelle à la norme ISO 27001.

8 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 peut 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. Pendant de la norme ISO 27002, 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. Les neuf objectifs retenus sont directement tirés de la LPD et les 20 mesures associées sont structurées conformément à la norme ISO 27002.

f. communication transfrontière de données (art. 6, al. 1, LPD):
   1. niveau de protection adéquat (art. 6, al. 2, LPD);

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, LPD; 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. Abrogation d'un autre acte

Les Directives du 16 juillet 2008 sur la certification de l'organisation et de la procédure[9] sont abrogées.

7. Disposition transitoire

Les procédures de certification en cours au moment de l'entrée en vigueur de ces directives sont régies par l'ancien droit. Ces procédures de certification doivent être achevées jusqu'au 1er octobre 2014.

8. Entrée en vigueur

Les présentes directives entrent en vigueur le 1er mai 2014.

19 mars 2014

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

Hanspeter Thür

9 FF **2008** 6625