CH_VB 2008-1896 6625 vom 28. September 2007

Bundesverwaltung, 2007-09-28, DE

Quelle: https://mcp.opencaselaw.ch/entscheid/ch_vb_2008-1896_6625_

FR: CH_VB 2008-1896 6625 du 28 septembre 2007

IT: CH_VB 2008-1896 6625 del 28 settembre 2007

Erwägungen

E. 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.

E. 2

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

E. 3

Réalisation 1 Un SGPD répond aux exigences minimales s'il se fonde sur des référentiels inter- nationaux 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 rempla- çant son annexe A, qui correspond à la table des matières de la norme ISO/CEI 27002:20055, par les objectifs et mesures énumérés au point 5.

E. 4

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

E. 5

Objectifs et mesures Lors de l'élaboration du SGPD, les objectifs et mesures7 suivants doivent être réali- sés: 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. 10a, 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. 7a, 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)

E. 6

Lettre additionnelle à la norme ISO 27001.

E. 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.

Directives sur les exigences minimales qu’un système de gestion de la protection des données doit remplir 6628 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 10a, al. 2, LPD) h. Enregistrement des fichiers (art. 11a, al. 1, LPD et art. 12b, al. 1, OLPD) 1. Obligation de déclarer (art. 11a, al. 2 et 3; exceptions art. 11a, al. 5, let. e et f, LPD) 2. Inventaire des fichiers non déclarés (art. 12b, 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

Schweizerisches Bundesarchiv, Digitale Amtsdruckschriften Archives fédérales suisses, Publications officielles numérisées Archivio federale svizzero, Pubblicazioni ufficiali digitali 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) In Bundesblatt Dans Feuille fédérale In Foglio federale Jahr 2008 Année Anno Band 1 Volume Volume Heft 34 Cahier Numero Geschäftsnummer --- Numéro d'affaire Numero dell'oggetto Datum 26.08.2008 Date Data Seite 6625-6628 Page Pagina Ref. No

E. 10

142 062 Die elektronischen Daten der Schweizerischen Bundeskanzlei wurden durch das Schweizerische Bundesarchiv übernommen. Les données électroniques de la Chancellerie fédérale suisse ont été reprises par les Archives fédérales suisses. I dati elettronici della Cancelleria federale svizzera sono stati ripresi dall'Archivio federale svizzero.