Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

FF 2023
www.fedlex.admin.ch
La version électronique
signée fait foi

Directives sur les exigences minimales qu'un système de gestion doit remplir

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

du 31 août 2023

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

vu l'art. 6, al. 2, de l'ordonnance du 31 août 2022 sur les certifications en matière de protection des données (OCPD)[1],

édicte les directives suivantes:

1 But

[1] Les présentes directives fixent les exigences minimales qu'un système de gestion (système de management, SM) doit remplir pour obtenir une certification de l'organisation ou de la procédure au sens de l'art. 6 OCPD.

[2] Elles visent à fournir un modèle d'établissement, d'exploitation, de surveillance, de réexamen, de mise à jour et d'amélioration d'un SM.

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

2 Définitions

En complément aux termes et définitions de la norme ISO/CEI 27000[2], 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;

1 RS **235.13**

2 «Information security management systems – Overview and vocabulary» disponible sous licence en format papier ou PDF auprès de www.iso.org.
Les normes peuvent être consultées gratuitement ou obtenues contre paiement auprès de l'Association suisse de normalisation (SNV), Sulzerallee 70, 8404 Winterthour, www.snv.ch.

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 (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. Realisation

1 Un SM répond aux exigences minimales lorsqu'il se fonde sur des référentiels internationaux en usage, en particulier la norme ISO/CEI 27001[3], interprétée au sens de l'al. 2 et complétée ou amendée conformément au ch. 4.

2 Les exigences de la norme ISO/CEI 27001 portant sur le système de management de la sécurité de l'information (SMSI) doivent être reprises en complétant la notion de sécurité de l'information (SI) par celle de protection des données (PD) et l'annexe A de la norme ISO/CEI 27001, qui correspond à la table des matières de la norme 27002[4] par les objectifs et mesures énumérés au ch. 5.

4. Mise en œuvre (exigences minimales)

Le SM mis en place par l'organisation doit contenir à tout le moins les exigences minimales de la norme ISO/CEI 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/CEI 2700.

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

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

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

4 «Information security controls», disponible sous licence en format papier, ePub ou PDF auprès de www.iso.org.

5.2.	la politique de protection des données[5] correspond à la charte de protection des données visée à l'art. 4, al. 2, let. a, OCPD;
6.1.2. c.2.	les actifs du genre des activités de traitement (art. 5 let. d et art. 12 LPD) et leur responsables (propriétaire du risque) (art. 5 let. j 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.[6]	la documentation du SM inclut au minimum le registre des activités de traitement et une évaluation si le traitement envisagé est susceptible d'entraîner un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée.

5. Objectifs et mesures

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

a. licéité (art. 6 al. 1 LPD):
   1. motifs justificatifs (art. 31 LPD),
   2. base légale (art. 34 et 36 LPD),
   3. sous-traitance (art. 9 LPD en lien avec art. 7 OPDo);

b. transparence:
   1. bonne foi (art. 6 al. 2 LPD),
   2. reconnaissabilité (art. 6 al. 3 LPD),
   3. obligation d'informer (art. 19 – 21 LPD en lien avec art. 13 OPDo),
   4. registre des activités de traitement (art. 12 LPD en lien avec art. 24 OPDo),
   5 analyse d'impact relative à la protection des données personnelles (art. 22 LPD en lien avec art. 14 OPDo),
   6. annonce des violations de la sécurité des données (art. 24 LPD en lien avec art. 15 OPDo);

c. proportionnalité:
   1. traitement proportionnel (art. 6 al. 2 LPD),
   2. protection des données dès la conception et par défaut (art. 7 LPD);

d. finalité (art. 6 al. 3 LPD);

5 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.

6 Lettre additionnelle à la norme ISO/CEI 27001.

7 Les objectifs et mesures mentionnés ne sont pas exhaustifs et une organisation est libre de prendre en compte des objectifs ou mesures supplémentaires. Les objectifs et les mesures de ce tableau doivent être choisis comme partie intégrante du processus lors de la mise en œuvre du SM.

e. exactitude des données (art. 6 al. 5 LPD);

f. communication de données personnelles à l'étranger (art. 16 LPD en lien avec art. 8 – 12 OPDo);

g. sécurité des données (art. 8 LPD en lien avec art. 1 – 6 OPDo);

h. droits et procédure:

1. droit d'accès des données concernant une personne (art. 25 LPD en lien avec art. 16 – 19 OPDo),
2. droit à la remise ou à la transmission des données personnelles (art. 28 LPD en lien avec art. 20 – 22 OPDo),
3. prétentions et procédures (art. 32 et 41s. LPD).

6. Abrogation d'un autre acte

Les Directives du 19 mars 2014 sur la certification de l'organisation et de la procédure[8] 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 mars 2024.[9]

8. Entrée en vigueur

Les présentes directives entrent en vigueur le 1er septembre 2023.

31 août 2023

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

Adrian Lobsiger

8 FF **2014** 3015

9 Les autres dispositions transitoires seront publiées par le Service d'accréditation suisse (SAS).