Ordonnance sur les certifications en matière de protection des données (OCPD)

Projet du 2 février 2007

du

Le Conseil fédéral suisse,

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

arrête:

Section 1 Organismes de certification

Art. 1 Exigences

[1] Les organismes qui effectuent des certifications au sens de l'art. 11 LPD (organismes de certification) doivent être accrédités. Leur accréditation est régie par l'ordonnance du 17 juin 1996 sur l'accréditation et la désignation[2], sauf disposition contraire de la présente ordonnance.

[2] Une accréditation est requise pour les certifications portant sur :

a. l'organisation et la procédure en matière de protection des données, et

b. les produits (programmes et systèmes).

[3] Les organismes de certification doivent disposer d'une organisation et d'une procédure de certification déterminées (programme de contrôle). Les points suivants doivent notamment être réglés :

a. les critères d'évaluation ou d'essai ainsi que les exigences en découlant que doivent respecter les organismes ou les produits à certifier (schéma d'évaluation ou d'essai), et

b. les modalités du déroulement de la procédure et notamment un concept adéquat sur les mesures à prendre si des manquements sont constatés.

[4] Les exigences minimales concernant le programme de contrôle sont régies par les normes et les principes applicables selon l'annexe 2 de l'ordonnance du 17 juin 1996 sur l'accréditation et la désignation et par les art. 4 à 6.

[5] Les exigences minimales concernant la qualification du personnel qui exécute des certifications sont réglées en annexe.

RO **1993** 1962

1 RS **235.1**

2 RS **946.512**

Art. 2 Procédure d'accréditation

Le Service d'accréditation suisse associe le Préposé fédéral à la protection des données et à la transparence (le préposé) à la procédure d'accréditation et au contrôle.

Art. 3 Organismes de certification étrangers

1 Après avoir consulté le Service d'accréditation suisse, le préposé reconnaît les organismes de certification étrangers qui veulent exercer des activités sur le territoire suisse, si ces organismes prouvent qu'ils ont une qualification équivalente à celle exigée en Suisse.

2 Les organismes de certification doivent notamment prouver qu'ils remplissent les exigences fixées à l'art. 1, al. 3 et 4, et qu'ils connaissent suffisamment la législation suisse sur la protection des données.

3 Le préposé peut accorder la reconnaissance pour une durée limitée et la subordonner à des conditions ou à des charges. Il annule la reconnaissance si des conditions ou des charges essentielles ne sont pas remplies.

Section 2 Objet et procédure de certification

Art. 4 Certification de l'organisation et de la procédure

1 Peuvent faire l'objet d'une certification :

a. l'ensemble des procédures de traitement des données pour lesquelles un organisme est responsable ;

b. des procédures de traitement déterminées.

2 L'évaluation porte sur le système de gestion de la protection des données. Ce dernier comprend notamment:

a. une charte de protection des données;

b. une documentation concernant les objectifs et les mesures visant à garantir la protection et la sécurité des données;

c. les dispositions techniques et organisationnelles nécessaires à la réalisation des objectifs et des mesures fixés et en particulier des mesures visant à éliminer les manquements constatés.

3 Les exigences minimales qu'un système de gestion de la protection des données doit remplir sont régies par les normes internationales relatives à l'installation, l'exploitation, la surveillance et l'amélioration de systèmes de gestion, en particulier par rapport à la sécurité des données (norme ISO 27001:2005).

4 L'exception à l'obligation de déclarer prévue à l'art. 11*a*, al. 5, let. f, LPD ne s'applique que si l'organisme certifié a obtenu une certification pour l'ensemble des procédures de traitement portant sur les données du fichier à déclarer.

Art. 5 Certification de produits

1 Peuvent faire l'objet d'une certification des produits logiciels ou des combinaisons de produits logiciels avec certains produits matériels servant principalement au traitement de données personnelles ou générant, lors de leur utilisation, des données personnelles concernant notamment l'utilisateur.

2 L'organisme de certification examine notamment si les mesures techniques inhérentes au système ou au produit garantissent:

a. la confidentialité, l'intégrité, la disponibilité et l'authenticité des données personnelles traitées au vu des finalités du produit ou du système;

b. la prévention de la génération, de l'enregistrement ou de tout autre traitement de données personnelles inutile au vu des finalités du produit;

c. la transparence et la reproductibilité des traitements automatisés de données personnelles effectués dans le cadre de la fonctionnalité du produit définie par le fabricant.

3 Le préposé édicte des directives fixant les critères spécifiques en matière de protection des données qu'un produit doit remplir dans le cadre d'une certification.

Art. 6 Octroi et durée de validité de la certification

1 La certification est octroyée lorsque la procédure de certification permet de conclure, sur la base des critères d'évaluation ou d'essai appliqués par l'organisme de certification, que les exigences prévues par le droit de la protection des données et celles qui résultent des annexes 1 et 2 sont respectées. L'octroi de la certification peut être assorti de conditions ou de charges.

2 La durée de validité de la certification d'un système de gestion de la protection des données est de trois ans. Chaque année, l'organisme de certification vérifie sommairement que les conditions de la certification sont remplies.

3 La durée de validité de la certification d'un produit est de deux ans. Le produit est soumis à une nouvelle certification si des modifications y sont apportées.

Art. 7 Reconnaissance des certifications étrangères

Après avoir consulté le Service d'accréditation suisse, le préposé reconnaît les certifications étrangères, pour autant que le respect des exigences de la législation suisse soit garanti.

Art. 8 Communication du résultat de la procédure de certification

1 Si, aux fins d'être délié de son obligation de déclarer ses fichiers au sens de l'art. 11*a*, al. 5, let. f, LPD, l'organisme certifié communique au préposé qu'il a obtenu

une certification conformément à l'art. 4, il lui transmet, sur demande, les documents suivants:

a. le rapport d'évaluation;

b. les documents de certification.

2 Lorsque l'organisme de certification constate, dans le cadre de son activité de surveillance, des modifications essentielles concernant les conditions de certification, notamment en ce qui concerne le respect des charges ou des conditions, l'organisme certifié en informe le préposé.

3 Le préposé publie une liste des organismes certifiés qui sont déliés de leur obligation de déclarer leurs fichiers. La liste indique la durée de validité de la certification.

Section 3 Sanctions

Art. 9 Suspension et révocation de la certification

1 L'organisme de certification peut suspendre ou révoquer une certification, notamment lorsque, dans le cadre de la vérification (art. 6, al. 2), il constate des manquements graves. Il y a manquement grave notamment lorsque :

a. les conditions essentielles de la certification ne sont plus remplies, ou que

b. l'organisme certifié utilise un certificat de manière trompeuse ou abusive.

2 Tout litige concernant la suspension ou la révocation est soumis aux dispositions de droit civil applicables au rapport contractuel liant l'organisme de certification à l'organisme certifié.

3 L'organisme de certification informe le préposé de la suspension ou de la révocation, pour autant que la certification ait été communiquée à ce dernier conformément à l'art. 8, al. 1.

Art. 10 Procédure applicable aux mesures de surveillance du préposé

1 Le préposé informe l'organisme de certification s'il constate des manquements graves auprès d'un organisme certifié dans le cadre de son activité de surveillance au sens de l'art. 27 ou 29 LPD.

2 L'organisme de certification invite immédiatement l'organisme certifié à prendre, dans un délai de 30 jours à compter de la réception de la communication du préposé, les mesures nécessaires pour respecter les conditions de certification ou pour garantir une utilisation du certificat conforme à la loi.

3 Si l'organisme certifié ne remédie pas à la situation dans le délai fixé, l'organisme de certification suspend la certification. Il révoque la certification s'il n'existe aucune perspective d'obtenir ou de rétablir une situation conforme à la loi dans un délai convenable.

4 Si l'organisme certifié ne remédie pas à la situation dans le délai prévu à l'al. 2 et si l'organisme de certification ne suspend ni ne révoque la certification, le préposé émet une recommandation au sens de l'art. 27, al. 4, ou 29, al. 3, LPD à l'intention

de l’organisme certifié ou de l’organisme de certification concerné. Il peut notamment recommander à l’organisme de certification de suspendre ou de révoquer la certification. S’il adresse la recommandation à l’organisme de certification, il en informe le Service d’accréditation suisse.

Section 4 Entrée en vigueur

Art. 11

La présente ordonnance entre en vigueur le …. 2007.

Annexe

(art. 1, al. 5)

Exigences concernant les qualifications du personnel des organismes de certification chargé de réaliser les certifications

1 Certification des systèmes de gestion de la protection des données

L'organisme de certification doit prouver que le personnel qui certifie les systèmes de gestion de la protection des données possède les qualifications suivantes:

- connaissance du droit de la protection des données : doit être prouvée une activité pratique d'au moins deux ans dans le domaine de la protection des données ou un diplôme d'une haute école ou d'une haute école spécialisée sanctionnant des études d'une année au moins, avec comme matière principale le droit de la protection des données ;
- connaissances dans le domaine de la sécurité informatique : doit être prouvée une activité pratique d'au moins deux ans dans le domaine de la sécurité informatique ou un diplôme d'une haute école ou d'une haute école spécialisée sanctionnant des études d'une année au moins, avec comme matière principale la sécurité informatique;
- formation d'auditeur de systèmes de management (selon le guide ISO/CEI 62 [ISO/CEI 17021 ; …]).

L'organisme de certification doit pouvoir prouver qu'il dispose de personnel qualifié pour chacun des domaines qu'il couvre. Les audits peuvent être menés par une équipe interdisciplinaire.

2 Certification des produits et des systèmes

L'organisme de certification doit prouver que le personnel qui certifie les produits et les systèmes possède les qualifications suivantes:

- connaissance du droit de la protection des données : doit être prouvée une activité pratique d'au moins deux ans dans le domaine de la protection des données ou un diplôme d'une haute école ou d'une haute école spécialisée sanctionnant des études d'une année au moins, avec comme matière principale le droit de la protection des données ;
- connaissances dans le domaine de la sécurité informatique : doit être prouvée une activité pratique d'au moins deux ans dans le domaine de la sécurité informatique ou un diplôme d'une haute école ou d'une haute école spéciali-

sée sanctionnant des études d'une année au moins, avec comme matière principale la sécurité informatique;

- connaissances spécialisées concernant la certification des produits (selon le guide ISO/CEI 65).

L'organisme de certification doit pouvoir prouver qu'il dispose de personnel qualifié pour chacun des domaines qu'il couvre. La certification des produits par une équipe interdisciplinaire est autorisée.