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

du 31 août 2022 (État le 1er septembre 2023)

Le Conseil fédéral suisse,

vu l'art. 13, al. 2, de la loi fédérale du 25 septembre 2020 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. 13 LPD (organismes de certification) doivent être accrédités. Leur accréditation est régie par l'ordonnance du 17 juin 1996 sur l'accréditation et la désignation (OAccD)[2], sauf disposition contraire de la présente ordonnance.

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

a. l'organisation et les procédures (systèmes de gestion) en lien avec le traitement des données;

b. les produits, notamment les systèmes et programmes de traitement des données et les produits matériels, ainsi que les services et les processus en lien avec le traitement des données.

[3] Les organismes de certification doivent disposer d'une organisation et d'une procédure de certification (programme de certification) déterminées.

[4] Les exigences minimales concernant la qualification du personnel qui exécute des certifications sont réglées en annexe. Les organismes de certification doivent prouver qu'ils disposent de personnel qualifié selon ces critères.

Art. 2 Procédure d'accréditation

Le Service d'accréditation suisse (SAS) associe le Préposé fédéral à la protection des données et à la transparence (PFPDT) à la procédure d'accréditation et au contrôle ainsi qu'à la suspension et à la révocation de l'accréditation.

RO **2022** 569

1 RS **235.1**

2 RS **946.512**

Art. 3 Organismes de certification étrangers

1 Les organismes de certification étrangers qui veulent exercer des activités sur le territoire suisse doivent prouver qu'ils disposent d'une qualification équivalente, 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.

2 Le PFPDT reconnaît un organisme de certification étranger après avoir consulté le SAS.

3 Il peut accorder la reconnaissance pour une durée limitée et la subordonner à des charges.

4 Il annule la reconnaissance si les conditions ou les charges ne sont plus remplies.

Section 2 Objets et procédure de certification

Art. 4 Objets de la certification

1 Peuvent faire l'objet d'une certification:

a. les systèmes de gestion;

b. les produits, les services et les processus.

2 La certification des systèmes de gestion peut porter sur l'ensemble du système, sur certaines parties de l'organisation ou sur certaines procédures déterminées.

3 La certification des produits, des services et des processus peut porter sur:

a. les produits servant principalement au traitement de données personnelles ou générant, lors de leur utilisation, des données personnelles;

b. les services ou les processus servant principalement au traitement de données personnelles ou générant des données personnelles.

Art. 5 Exigences relatives au programme de certification

1 Le programme de certification doit au moins régler:

a. les critères d'évaluation ainsi que les exigences en découlant que doivent respecter les objets à certifier;

b. les modalités du déroulement de la procédure, notamment les mesures à prendre si des irrégularités sont constatées.

2 Lors de l'élaboration du programme de certification, il doit être tenu compte des points suivants:

a. les données personnelles à traiter;

b. les infrastructures électroniques utilisées pour le traitement des données personnelles;

c. les mesures organisationnelles liées au traitement des données personnelles.

3 Les critères d'évaluation doivent respecter tous les principes de l'art. 6 LPD.

4 Le programme de certification doit respecter les normes applicables selon l'annexe 2 de l'OAccD[3], ainsi que d'autres normes techniques applicables.

Art. 6 Exigences relatives à la certification de systèmes de gestion

1 L'évaluation du système de gestion porte notamment sur:

a. la politique en matière de protection des données;

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

c. les dispositions techniques et organisationnelles nécessaires à la mise en œuvre des objectifs et des mesures fixés, notamment pour remédier aux manquements.

2 Le PFPDT émet des directives sur les exigences minimales qu'un système de gestion doit remplir. Il tient compte des critères internationaux relatifs à l'installation, à l'exploitation, à la surveillance et à l'amélioration de tels systèmes et en particulier des normes techniques suivantes[4]:

a. SN EN ISO 9001, systèmes de management de la qualité, exigences;

b. SN EN ISO/IEC 27001, technologies de l'information, techniques de sécurité, système de management de la sécurité de l'information, exigences;

c. SN EN ISO/IEC 27701, techniques de sécurité, extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée, exigences et lignes directrices.

Art. 7 Exigences relatives à la certification des produits, des services et des processus

1 L'évaluation des produits, des services et des processus permet notamment de garantir:

a. la confidentialité, l'intégrité, la disponibilité et la traçabilité des données personnelles traitées;

b. la prévention de tout traitement de données personnelles inutile au vu des finalités du produit, du service ou du processus;

c. la transparence du traitement des données personnelles;

d. les mesures techniques permettant à l'utilisateur de respecter d'autres principes et obligations en matière de protection de données, notamment les droits des personnes concernées.

2 Le PFPDT émet des directives fixant d'autres critères en matière de protection des données dont il doit être tenu compte lors de l'évaluation.

3 RS **946.512**

4 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.

Art. 8 Octroi et durée de validité de la certification

1 L'organisme de certification certifie le système de gestion, le produit, le service ou le processus si les exigences prévues par le droit de la protection des données et les conditions prévues par la présente ordonnance, par les directives émises par le PFPDT ou par toute autre norme équivalente sont respectées. L'octroi de la certification peut être assorti de charges.

2 La durée de validité de la certification est de trois ans. Chaque année, l'organisme de certification vérifie que les conditions de la certification sont remplies.

Art. 9 Reconnaissance des certifications étrangères

Après avoir consulté le SAS, le PFPDT reconnaît les certifications étrangères, pour autant que le respect des exigences de la législation suisse soit garanti.

Art. 10 Exemption de l'obligation d'établir une analyse d'impact relative à la protection des données personnelles

Le responsable du traitement privé ne peut renoncer à établir une analyse d'impact relative à la protection des données personnelles, conformément à l'art. 22, al. 5 LPD, que si la certification inclut le traitement pour lequel il y aurait lieu de procéder à l'analyse d'impact.

Section 3 Sanctions

Art. 11 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, il constate des manquements graves. Il y a manquement grave notamment:

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

b. si une certification est utilisée 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 au fournisseur de systèmes ou de logiciels de traitement de données personnelles, au responsable du traitement ou au sous-traitant au bénéfice d'une certification.

Art. 12 Procédure applicable aux mesures de surveillance du PFPDT

1 Le PFPDT informe l'organisme de certification s'il constate des manquements graves de la part d'un fournisseur de systèmes ou de logiciels de traitement de données personnelles, d'un responsable du traitement ou d'un sous-traitant au bénéfice d'une certification.

2 L'organisme de certification invite immédiatement le fournisseur de systèmes ou de logiciels de traitement de données personnelles, le responsable du traitement ou le

sous-traitant au bénéfice d'une certification à remédier, dans un délai de 30 jours après avoir été informé par le PFPDT, aux manquements constatés.

3 S'il n'est pas remédié aux manquements dans les 30 jours, 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 S'il n'est pas remédié aux manquements dans le délai prévu à l'al. 2 et si l'organisme de certification ne suspend ni ne révoque la certification, le PFPDT prend une mesure au sens de l'art. 51, al. 1 LPD. Il peut notamment ordonner la suspension ou la révocation de la certification. S'il donne cet ordre à l'organisme de certification, il en informe le SAS.

Section 4 Dispositions finales

Art. 13 Abrogation d'un autre acte

L'ordonnance du 28 septembre 2007 sur les certifications en matière de protection des données[5] est abrogée.

Art. 14 Entrée en vigueur

La présente ordonnance entre en vigueur le 1er septembre 2023.

5 [RO **2007** 5003; **2010** 949; **2016** 3447]

Annexe
(art. 1, al. 4)

Exigences minimales concernant les qualifications du personnel

1 Certification des systèmes de gestion

Le personnel qui certifie les systèmes de gestion, pris dans son ensemble, possède les qualifications suivantes:

- connaissances dans le domaine du droit de la protection des données: activité pratique d'au moins deux ans dans le domaine de la protection des données ou 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 de l'information: activité pratique d'au moins deux ans dans le domaine de la sécurité de l'information ou 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 de l'information;
- connaissances des développements en matière de droit de la protection des données et dans le domaine de la sécurité de l'information;
- formation d'auditeur de système de gestion satisfaisant aux critères internationaux pertinents, tels qu'ils figurent notamment dans les normes suivantes[6]:
  - SN EN ISO/IEC 17021-1, évaluation de la conformité, exigences pour les organismes procédant à l'audit des systèmes de management, partie 1: exigences,
  - SN EN ISO/IEC 17021-3, évaluation de la conformité, exigences pour les organismes procédant à l'audit et à la certification des systèmes de management, partie 3: exigences de compétence pour l'audit et la certification des systèmes de management de la qualité, et
  - SN EN ISO/IEC 27006, technologies de l'information, techniques de sécurité, exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information.

L'organisme de certification doit disposer d'un personnel qualifié pour chacun des domaines qu'il couvre. L'évaluation des systèmes de gestion par une équipe interdisciplinaire est autorisée.

6 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.

2 Certification des produits, des services et des processus

Le personnel qui certifie les produits, les services ou les processus, pris dans son ensemble, possède les qualifications suivantes:

- connaissances dans le domaine du droit de la protection des données: activité pratique d'au moins deux ans dans le domaine de la protection des données ou 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 de l'information: activité pratique d'au moins deux ans dans le domaine de la sécurité de l'information ou 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 de l'information;
- connaissances des développements en matière de droit de la protection des données et dans le domaine de la sécurité de l'information;
- connaissances spécialisées concernant la certification des produits, des services ou des processus satisfaisant aux exigences du programme de certification et des directives émises par le PFPDT, ainsi qu'aux critères internationaux pertinents, tels qu'ils figurent notamment dans les normes techniques applicables, et dans la norme «SN EN ISO/IEC 17065[7], évaluation de la conformité, exigences pour les organismes certifiant les produits, les procédés et les services».

L'organisme de certification doit disposer d'un personnel qualifié pour chacun des domaines qu'il couvre. L'évaluation des produits, des services et des processus par une équipe interdisciplinaire est autorisée.

[7] La norme peut être consultée gratuitement ou obtenue contre paiement auprès de l'Association suisse de normalisation (SNV), Sulzerallee 70, 8404 Winterthour, www.snv.ch.