Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de justice et police DFJP

Office fédéral de la justice OFJ
Domaine de direction Droit public

31 août 2022

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

Rapport explicatif

BJ-D-83643401/176

Table des matières

1 Situation initiale

1.1 Contexte

À la suite d'une évaluation de la loi fédérale du 19 juin 1992 sur la protection des données[1] (LPD), et compte tenu des évolutions technologiques et des développements du droit européen, le Conseil fédéral a décidé de réviser une partie de la législation fédérale en matière de protection des données. Le 15 septembre 2017, il a ainsi adopté le message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales[2]. Le projet de loi comprend d'une part une révision totale de la LPD et d'autre part une révision partielle d'autres lois fédérales, afin de mettre en œuvre la directive (UE) 2016/680[3] notamment. Le Parlement a décidé que la mise en œuvre du projet du Conseil fédéral se ferait en deux étapes. Dans la première étape, seule la directive Schengen (UE) 2016/680 sur la protection des données dans le droit pénal a été mise en œuvre : la loi fédérale sur la protection des données personnelles dans le cadre de l'application de l'acquis de Schengen dans le domaine pénal (LPDS)[4] est entrée en vigueur le 1er mars 2019. Lors de la deuxième étape, le Parlement a délibéré sur la nouvelle loi sur la protection des données (nLPD)[5] et l'a adoptée le 25 septembre 2020.

En raison de la révision totale de la LPD, les ordonnances correspondantes, à savoir l'ordonnance relative à la loi fédérale sur la protection des données (OLPD)[6] et l'ordonnance sur les certifications en matière de protection des données (OCPD)[7], doivent également être adaptées.

1.2 Modifications de la nLPD en matière de certification

L'art. 13 nLPD porte sur la certification et reprend l'art. 11 LPD en y ajoutant la possibilité de faire certifier des produits et des services. En réalité, seule l'introduction des « services » est nouvelle sur un plan matériel, puisque les « produits » sont déjà appréhendés, dans le droit actuel, par l'ordonnance du 28 septembre 2007. Comme dans le droit en vigueur, l'al. 2 donne mandat au Conseil fédéral d'édicter des dispositions sur la reconnaissance des procédures de certification et sur l'introduction d'un label de qualité de protection des données, en tenant compte du droit international et des normes techniques reconnues au niveau international. Par ailleurs, selon l'art. 22, al. 5, nLPD, le responsable du traitement privé peut renoncer à établir une analyse d'impact lorsqu'il recourt à un système, un produit ou un service certifié conformément à l'art. 13 pour l'utilisation prévue. En outre, l'ordonnance « générale » relative à la protection des données, dans sa nouvelle version, permet également de communiquer des données à l'étranger sur la base d'une certification (voir dans ce sens l'art. 12 de la nouvelle ordonnance, fondé sur l'art. 16, al. 3, nLPD).

1.3 Constitutionnalité et compatibilité avec les obligations internationales

L'ordonnance sur les certifications en matière de protection des données est une ordonnance d'exécution de la loi fédérale sur la protection des données telle qu'elle a été révisée par

---

1 RS **235.1**

2 FF **2017** 6565

3 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, JO L 119 du 4.5.2016, p. 89.

4 RS **235.3**

5 FF **2020** 7397

6 RS **235.11**

7 RS **235.13**

le Parlement le 25 septembre 2020 et elle remplit le mandat donné au Conseil fédéral par l'art. 13, al. 2, nLPD. En ce sens, l'ordonnance respecte la loi et il peut être renvoyé aux explications contenues dans le message pour ce qui concerne les aspects juridiques (cf. FF 2017 6565, spécialement 6796 ss).

2 Grandes lignes du projet

Les principales nouveautés apportées dans la nouvelle OCPD portent sur des points d'ordre différents. En premier lieu, des simplifications et unifications sur un plan terminologique étaient nécessaires. Par exemple, au niveau de la nLPD, une distinction est faite entre la fonction de préposé fédéral à la protection des données et à la transparence et l'institution dans son ensemble. On se réfère à l'institution au moyen de l'abréviation « PFPDT », et le terme de « préposé » est réservé au chef de l'institution. Les adaptations nécessaires ont donc été reportées dans la nouvelle OCPD.

Pour désigner qui peut prétendre à une certification, la nouvelle OCPD a également repris les termes issus de l'art. 13 nLPD, à savoir les « fournisseur de systèmes ou de logiciels de traitement de données personnelles », les « responsables du traitement » et les « sous-traitants ». Ainsi, il est désormais renoncé à l'expression « organisme au bénéfice d'une certification » utilisée jusqu'ici dans le cadre de l'OCPD, notamment parce que le terme « organisme » prête à confusion avec les « organismes de certification ». Il n'est pas inutile cependant de préciser que la notion de « fournisseur de systèmes ou de logiciels de traitement de données personnelles » comprend également les fournisseurs de produits (notamment les systèmes et programmes de traitement des données [software] et les produits matériels [hardware]), de services et de processus.

En ce qui concerne la notion de « systèmes », au sens de l'art. 13, al. 1, nLPD, la nouvelle OCPD utilise le terme de « systèmes de gestion ». Cela n'entraîne toutefois aucune modification matérielle par rapport au droit en vigueur. Les notions d'« organisation » et de « procédure », telles qu'elles sont contenues dans l'ordonnance de 2007, sont maintenues à titre de précision. L'ordonnance n'utilise plus que le terme de « systèmes de gestion » dans ce contexte. En outre, la possibilité de certifier des services, introduite par la nLPD, a conduit à préciser les exigences relatives à de telles certifications. Pour répondre aux besoins de la pratique, la nouvelle OCPD prévoit en outre la possibilité de certifier des « processus ». Ceux-ci ne sont certes pas mentionnés à l'art. 13, al. 1, nLPD, mais la base légale devra être adaptée à la prochaine occasion. Enfin, cette approche a aussi l'avantage de correspondre, d'une part, à la norme 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) relative à la certification des systèmes de management et, d'autre part, à la norme SN EN ISO/IEC 17065 (évaluation de la conformité, exigences pour les organismes certifiant les produits, les procédés et les services) qui touche tant les produits, les services, que les processus. D'une manière générale, les objets de la certification ont été mieux délimités. Bien que n'étant pas explicitement prévue par l'art. 13, al. 1 nLPD, la possibilité de certifier des traitements de données personnelles est également prise en compte, dans le cadre, notamment de la certification des produits ou des services. Cela permet de rapprocher le système suisse de certification du droit européen. Ainsi, les certifications suisses portant sur le traitement de données personnelles devraient pouvoir se faire reconnaitre par les autorités européennes.

Des exigences supplémentaires relatives au programme de certification (appelé « programme de contrôle » dans l'ordonnance de 2007), dont doivent disposer les organismes de certification, sont introduites, de même que les exigences relatives à la certification des services et des processus ; celles relatives à la certification de systèmes de gestion et des produits sont mises à jour. C'est également le cas des durées de certification.

La question de l'exemption d'établir une analyse d'impact, pour les responsables du traitement privé, est introduite par la nLPD et remplace la possibilité, existant dans le droit en vigueur jusqu'ici, de pouvoir être délié de l'obligation de déclarer ses fichiers (concept qui n'existe plus dans la loi adoptée en septembre 2020). Les dispositions traitant de cette question ont donc été adaptées dans le cadre de la nouvelle OCPD.

En mentionnant un label de qualité en matière de protection des données à l'art. 13, al. 2, la nLPD reprend la norme de délégation déjà prévue par le droit en vigueur. Comme l'ordonnance de 2007, la nouvelle OCPD ne contient cependant pas de dispositions relatives à un tel label. Jusqu'à présent, il n'a pas été jugé utile d'introduire un label général en matière de protection des données.

3 Commentaire de la nouvelle OCPD

3.1 Structure de l'ordonnance

La nouvelle ordonnance garde la même structure que l'ordonnance de 2007 : une première section est consacrée aux organismes de certification, une deuxième traite des objets et de la procédure de certification, les sanctions sont appréhendées par la troisième section, et la dernière porte sur les dispositions finales.

3.2 Section 1 : organismes de certification

La première section pose le principe de l'accréditation des organismes de certification. L'art. 1 précise les exigences auxquelles doivent se conformer ces organismes pour pouvoir être accrédités ; l'art. 2 précise quelles sont les institutions compétentes dans le cadre de la procédure d'accréditation ; enfin, l'art. 3 aborde la question de la reconnaissance, en Suisse, des organismes de certification étrangers.

Art. 1 Exigences

L'art. 1 de la nouvelle OCPD règle les exigences à respecter par les organismes qui effectuent des certifications (organismes de certification). En premier lieu, ces organismes doivent être accrédités par le Service d'accréditation suisse (SAS). Comme c'était déjà le cas dans le cadre de l'ordonnance de 2007, ces organismes doivent être accrédités séparément selon les objets qu'ils entendent certifier.

L'al. 2 a été complété par rapport à l'ordonnance de 2007, de sorte à préciser qu'une accréditation est non seulement nécessaire en vue de la certification de l'organisation et des procédures en lien avec le traitement des données (let. a) et des produits, mais également des services et des processus en lien avec le traitement des données (let. b).

Les domaines concernés par les lettres a) et b) font l'objet d'accréditations distinctes : L'accréditation selon la let. a se fonde sur les normes SN EN ISO/CEI 17021-1 (cf. *supra*) 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), ainsi que sur un programme de certification correspondant. Les exigences de la let. b sont couvertes par la norme SN EN ISO/IEC 17065 (cf. *supra*) et par un programme de certification correspondant.

L'ajout (à la let. b) des notions de services et de processus est nécessaire pour que l'ordonnance soit conforme à l'art. 13 nLPD, tel que modifié dans le cadre de la révision totale de la loi, et soit plus généralement en ligne avec la pratique et les différentes normes ISO mentionnées ci-dessus. La notion de « services » est nouvelle et on entend par-là, par exemple,

le stockage de données dans un cloud ou la collecte de données pour un concours. La notion de « processus » a également été ajoutée, dans un souci de conformité avec les différentes normes iso, notamment la norme SN EN ISO 9001 (systèmes de management de la qualité, exigences), qui distinguent généralement le processus (« entrées, sorties, activités ») et la procédure (« description » de ces éléments).

À la let. a, une parenthèse introduit la notion de « systèmes de gestion ». Cela permet d'aller dans le sens de la loi qui parle désormais de « systèmes », « produits » et « services ». La notion de « systèmes de gestion », plus précise, est celle qui est ensuite reprise tout au long du texte de l'ordonnance.

L'al. 3 est modifié de sorte à se concentrer uniquement sur le programme de certification dont les exigences sont spécifiquement réglées aux art. 5 à 7 de la nouvelle ordonnance. Le terme « programme de certification » remplace celui de « programme de contrôle » afin d'avoir une terminologie qui corresponde à celle utilisée dans les normes iso (par exemple SN EN ISO/IEC 17065, cf. *supra*). Contrairement à l'ordonnance de 2007, les exigences matérielles relatives au programme de certification sont désormais reprises dans le nouvel art. 5, afin que toutes les exigences relatives à ce programme soient réunies au sein du même article.

Le contenu de l'al. 4 de l'ordonnance de 2007 est désormais intégré à l'al. 3 de la nouvelle ordonnance. Les articles mentionnés sont adaptés afin de respecter la numérotation modifiée de la nouvelle ordonnance. Le renvoi à l'ordonnance du 17 juin 1996 sur le système suisse d'accréditation et la désignation de laboratoires d'essais et d'organismes d'évaluation de la conformité, d'enregistrement et d'homologation (OAccD)[8] figure désormais également à l'art. 5.

Enfin, l'al. 5 de l'ordonnance de 2007 devient l'al. 4. Il traite des exigences minimales concernant la qualification du personnel qui exécute des certifications et renvoie à l'annexe, en précisant de manière normative que les organismes de certification doivent prouver qu'ils disposent d'un personnel répondant à ces critères.

Art. 2 Procédure d'accréditation

Par rapport à l'ordonnance de 2007, seule l'abréviation « PFPDT » (qui désigne l'institution du Préposé fédéral à la protection des données) est introduite, en remplacement du terme « préposé » (qui, lui, se réfère désormais à la fonction dirigeante de l'institution). Sur cette modification terminologique, voir *supra*, ch. 2.

Art. 3 Organismes de certification étrangers

L'al. 1 fixe les conditions que les organismes de certification étrangers doivent remplir s'ils veulent exercer leur activité sur le territoire suisse. Par rapport à l'ordonnance de 2007, la disposition a été restructurée afin de régler toutes les conditions dans la même disposition. Outre la preuve qu'ils disposent d'une qualification équivalente, qu'ils remplissent les exigences du programme de certification et qu'ils connaissent suffisamment la législation suisse en matière de protection des données, les organismes de certification étrangers doivent désormais également prouver qu'ils remplissent les exigences en matière de qualification du personnel qui effectue les certifications.

[8] RS **946.512**

L'al. 2, raccourci par rapport à l'ordonnance de 2007 conformément aux explications données pour l'al. 1, se concentre désormais sur la reconnaissance des organismes de certification étrangers par le PFPDT, après avoir consulté le Service d'accréditation suisse.

L'al. 3 prévoit que le PFPDT peut limiter la reconnaissance dans le temps et l'assortir de charges. Le terme « conditions », utilisé dans l'ordonnance de 2007, est supprimé ici, car une reconnaissance ne peut être assortie que de charges. Contrairement aux conditions qui doivent être remplies pour obtenir une reconnaissance, les charges sont imposées après la reconnaissance afin que celle-ci conserve sa validité juridique.

En revanche, l'al. 4 prévoit que le PFPDT peut annuler la reconnaissance si les conditions et les charges ne sont plus remplies.

3.3 Section 2 : objets et procédure de certification

Avant de traiter en détail les différentes certifications et leurs exigences, deux nouveaux articles sont introduits dans cette section 2. L'art. 4 présente les éléments pouvant faire l'objet d'une certification et l'art. 5 se concentre sur les exigences relatives au programme de certification. Les art. 6 à 10 de la nouvelle OCPD reprennent les art. 4 à 8 de l'ordonnance de 2007 avec différentes modifications.

Art. 4 Objets de la certification

Ce nouvel article a pour but de présenter dans une seule disposition ce qui peut être certifié en matière de protection des données. Il s'agit des systèmes de gestion, des produits, des services et des processus en lien avec le traitement des données (al. 1).

Ces différents objets sont définis plus précisément en reprenant, pour les systèmes de gestion (al. 2), ce qui figure à l'art. 4, al. 1 de l'ordonnance de 2007 (sous réserve de modifications purement formelles).

La certification des produits est réglée à l'al. 3, let. a, et reprend ce qui figure à l'art. 5, al. 1 de l'ordonnance de 2007. On vise non seulement les navigateurs Internet, les logiciels propres au fonctionnement des serveurs Web, les applications permettant l'exploitation des sites Web, mais aussi les systèmes logistiques qui reposent sur les technologies RFID ou GPS. L'al. 3, let. b, vient préciser ce qu'il en est pour les services et les processus, à savoir ceux servant principalement au traitement de données personnelles ou générant des données personnelles.

Art. 5 Exigences relatives au programme de certification

L'art. 5 pose des exigences relatives au programme de certification. Comme déjà mentionné plus haut (cf. art. 1, al. 3), le terme « programme de contrôle » est remplacé par « programme de certification » et les conditions prévues à l'art. 1, al. 3, let. a et b de l'ordonnance de 2007 sont désormais déplacées à l'alinéa 1 de ce nouvel article. La formulation est légèrement modifiée sans changement matériel (par exemple, suppression de la notion d'essai; celle d'évaluation étant suffisante).

Le nouvel art. 5 complète les exigences actuelles en énumérant, à l'al. 2, certains aspects qui doivent impérativement être pris en compte lors de la définition du programme de certification. Ainsi, lors de l'élaboration du programme de certification, il doit être tenu compte de trois aspects : premièrement, les données personnelles traitées (autrement dit, le champ d'appli-

cation matériel) ; deuxièmement, les infrastructures électroniques utilisées pour le traitement des données personnelles (à savoir les systèmes techniques, tels que les logiciels et le matériel) ; et enfin, les mesures organisationnelles liées au traitement des données personnelles. Ces trois aspects sont pertinents pour la conception des critères de certification et des procédures. La mesure dans laquelle ils sont pris en compte peut varier en fonction de l'objet de la certification.

Autre nouveauté prévue à l'al. 3, le programme de certification doit démontrer que les critères d'évaluation respectent tous les principes de la protection des données, tels qu'ils sont définis à l'art. 6 nLPD. Cela signifie que lorsque ces mesures (critères d'évaluation, procédures, etc.) sont mises en place, il doit être tenu compte des principes du droit de la protection des données tels que la licéité, la proportionnalité et la finalité du traitement ou encore l'exactitude des données.

Enfin, comme dit en introduction, l'al. 4 reprend l'art. 1, al. 4 de l'ordonnance de 2007 et renvoie aux exigences de base fixées dans les normes iso listées à l'annexe 2 de l'OAccD. Cet alinéa est encore complété de sorte à préciser que l'annexe 2 de l'OAccD n'est pas exhaustive et que d'autres normes techniques sont applicables. Pour l'accréditation de produits, de services et de processus fondée sur la norme ISO/CEI 17065 (cf. *supra*), des programmes de certification sont prévus pour répondre aux exigences. Ces programmes peuvent être basés sur les normes internationales SN EN ISO/CEI 17067 (évaluation de la conformité, éléments fondamentaux de la certification de produits et lignes directrices pour les programmes de certification de produits), SN EN ISO/CEI TR 17028 (évaluation de la conformité, lignes directrices et exemples d'un schéma de certification pour les services) et SN EN ISO/CEI TR 17032 (évaluation de la conformité, lignes directrices et exemples d'un schéma de certification pour les processus). Ces programmes de certification sont émis par le PFPDT sous la forme de directives.

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

L'art. 6 reprend en grande partie l'art. 4 de l'ordonnance de 2007. Pour l'essentiel, l'al. 1 correspond matériellement à l'art. 4, al. 2. A la let. b, une documentation des risques est désormais également prescrite. En outre, des modifications formelles ont été apportées (par exemple, utilisation du terme « systèmes de gestion » ou suppression de la notion « d'essai »). Le texte français a été adapté de sorte que la let. a, qui parlait de « charte de protection des données » soit remplacée par « politique en matière de protection des données » et corresponde au texte allemand (Datenschutzpolitik).

L'art. 4, al. 3 de l'ordonnance de 2007, qui indique les normes techniques auxquelles doit se référer le PFPDT lorsqu'il émet des directives, est repris à l'art. 6, al. 2 avec quelques adaptations formelles. Celui-ci est cependant complété avec l'introduction d'une nouvelle let. c, renvoyant à la norme 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).

L'art. 4, al. 1 de l'ordonnance de 2007 a été repris à l'art. 4, al. 2 de la nouvelle OCPD. En plus d'une adaptation structurelle et terminologique, il est précisé de manière plus claire que la certification des systèmes de management peut porter sur l'ensemble du système, sur certaines parties de l'organisation ou sur des procédures isolées et délimitées. Quant à l'art. 4, al. 4 de l'ordonnance de 2007, il n'est plus pertinent en raison de la suppression de l'art. 11*a*, al. 5, let. f, LPD (sur ce point, voir le commentaire relatif à l'art. 10, *infra*).

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

L'art. 7 reprend en grande partie l'art. 5 de l'ordonnance de 2007. Il est cependant complété quant à son champ d'application matériel, puisqu'il ne concerne plus que les produits, mais également les services et les processus.

L'al. 1 se fonde sur l'art. 5, al. 2 de l'ordonnance de 2007. La let. a est modifiée afin d'introduire le concept de la traçabilité qui, couplé à la notion d'intégrité, englobe la notion d'authenticité. Il n'est dès lors plus nécessaire de la mentionner explicitement. La référence au fait que ces exigences doivent être garanties au vu des finalités prévues n'est pas reprise non plus, dans la mesure où ces principes sont de toute façon exigés en matière de protection des données, peu importe la finalité du traitement.

La let. b connaît les mêmes changements relatifs au champ d'application matériel : celle-ci s'applique désormais pour les produits, service et processus. En outre, cette lettre visant le principe de l'économicité et de la minimisation des données, elle a été simplifié en termes de formulation, sans pour autant apporter de différence quant au fond ; la « génération » et l'« enregistrement » de données faisant partie de la notion plus large de « traitement » de données.

La let. c est également simplifiée. La notion de « reproductibilité » et la précision selon laquelle il s'agirait des traitements « automatisés » sont superflues. Le principe de la transparence du traitement est important même si le traitement ne devait pas être automatisé (ce qui par ailleurs est peu probable). Ce qui compte, c'est que l'utilisateur soit en mesure de reconnaître les données personnelles traitées, leur mode de traitement et les destinataires de la communication. Les exigences seront donc définies en fonction du cercle des utilisateurs pour lesquels le produit, le service ou le processus est prévu ; elles seront donc plus élevées pour un produit, un service ou un processus touchant un large spectre d'utilisateurs que si cela ne concerne que des spécialistes. Bien que cette précision ait été supprimée de la let. c, il convient de souligner que l'examen porte sur les traitements effectués par un produit, un service ou un processus dans le cadre de la fonctionnalité pour laquelle il a été conçu. Si le produit, le service ou le processus est prévu de telle manière qu'il peut être utilisé pour différentes finalités, il y a lieu de vérifier que l'utilisateur ne puisse pas sans autre contourner ou mettre hors fonction les mécanismes garantissant la transparence.

La let. d a été complétée par une précision mettant en avant le fait que ce sont notamment les droits des personnes concernées qui doivent être particulièrement pris en compte.

Enfin, l'al. 2 prévoit, comme l'ordonnance de 2007 (art. 5, al. 3), que le PFPDT émette des directives fixant d'autres critères en matière de protection des données qu'un produit, un service ou un processus doit remplir dans le cadre d'une certification. La désignation du préposé est remplacée par celle du PFPDT (sur cette modification terminologique, voir *supra*, ch. 2). En revanche, la liste des objets de certification figurant dans l'ordonnance de 2007 est désormais supprimée, car elle est inutile au regard de l'intitulé.

Art. 8 Octroi et durée de validité de la certification

L'art. 8, al. 1 reprend l'art. 6, al. 1 de l'ordonnance de 2007 dans une version abrégée, mais sans modification matérielle, à l'exception du terme « processus ». L'énumération des objets de certification, au sens de l'art. 1, al. 2, permet de préciser que la réglementation s'applique à tous ces objets. Dans la dernière phrase, la notion de « conditions » est supprimée (voir à ce sujet les explications relatives à l'art. 3). Le fait que la certification puisse être assortie

de charges, permet à un fournisseur de systèmes ou de logiciels de traitement de données personnelles, un responsable du traitement ou un sous-traitant qui veut faire accréditer un système de gestion, un produit, un service ou un processus de se mettre à jour dans un certain délai.

L'al. 2 est modifié afin que tous les objets pouvant être certifiés bénéficient de la même durée de certification, à savoir trois ans. La durée de certification des produits est donc désormais la même que celle applicables aux autres objets. Cette modification permet notamment de correspondre au droit européen. Comme dans l'ordonnance de 2007, une vérification permettant de savoir si les conditions de la certification sont toujours remplies doit avoir lieu chaque année. Le caractère « sommaire » de la vérification, tel qu'il était prévu à l'art. 6, al. 2 et 3 de l'ordonnance de 2007, a été supprimé. La densité de la vérification dépend en effet de l'objet certifié.

Art. 9 Reconnaissance des certifications étrangères

L'art. 9 ne connaît aucune modification matérielle. Outre quelques changements formels par rapport à l'art. 7 de l'ordonnance de 2007, le terme de préposé est remplacé par celui du PFPDT (sur cette modification terminologique, voir *supra*, ch. 2).

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

L'art. 4, al. 4 de l'ordonnance de 2007 prévoit qu'un organisme de certification peut être délié de son obligation de déclarer ses fichiers, au sens de l'art. 11*a*, al. 5, let. f, LPD, s'il a obtenu une certification pour l'ensemble des procédures de traitement portant sur les données du fichier à déclarer. En raison de la révision de la loi, cette possibilité n'existe plus. Selon le nouveau droit (art. 22, al. 5, nLPD), le responsable du traitement peut, en revanche, « renoncer à établir une analyse d'impact lorsqu'il recourt à un système, un produit ou un service certifié conformément à l'art. 13 pour l'utilisation prévue ». L'art. 4, al. 4 de l'ordonnance de 2007 n'a donc plus de raison d'être et est supprimé. En revanche, afin de s'adapter à l'art. 22, al. 5, nLPD, une précision est introduite à l'art. 10 de la nouvelle OCPD : le responsable du traitement privé ne peut renoncer à établir une analyse d'impact relative à la protection des données personnelles que si la certification inclut le traitement pour lequel il y aurait lieu de procéder à l'analyse d'impact (dans ce sens, voir le message du Conseil fédéral concernant la nouvelle loi sur la protection des données, cf. FF 2017 6565, spécialement 6678). En effet, il ne faudrait pas qu'une certification soit trop générale et ne comprenne pas le traitement pour lequel le responsable du traitement souhaite être exempté d'effectuer une analyse d'impact.

Dans ce contexte, l'art. 8 de l'ordonnance de 2007, qui précise les conditions dans lesquelles il est possible d'être délié de l'obligation de déclarer les fichiers, c'est-à-dire principalement en informant le PFPDT de la certification et en lui fournissant les documents nécessaires, est également supprimé. Il n'a pas été jugé utile de réintroduire une obligation d'informer le PFPDT pour le cas de l'art. 22, al. 5, nLPD dans la mesure où les résultats de l'analyse d'impact ne doivent pas non plus être communiqués au PFPDT. Le PFPDT aurait souhaité que le responsable privé reste néanmoins tenu de lui demander son avis au préalable dans le cas où il subsisterait des risques élevés pour la personnalité ou les droits fondamentaux de la personne concernée après une analyse des risques. Cela aurait toutefois eu pour conséquence de réintroduire une obligation d'informer le PFPDT pour les responsables privés, contrairement à la volonté du législateur. Dans la mesure où la certification ne doit pas être communiquée au PFPDT, les al. 2 et 3 de l'art. 8 de l'ordonnance de 2007 n'ont dès lors plus lieu d'être. La publication d'une liste des organismes au bénéfices d'une certification n'est pas

non plus jugée utile puisque les organismes certifiés ont un intérêt à communiquer directement sur cette question et n'ont ainsi pas besoin de figurer sur le site du PFPDT.

3.4 Section 3 : sanctions

Les art. 11 et 12 reprennent de manière générale les art. 9 et 10 de l'ordonnance de 2007, sous réserve de certaines modifications ponctuelles.

Art. 11 Suspension et révocation de la certification

L'al. 1 est modifié sur deux points par rapport à l'art. 9, al. 1 de l'ordonnance de 2007. Premièrement, le renvoi interne est supprimé. En effet, il ressort clairement du contexte qu'il s'agit d'une vérification selon l'art. 8, al. 2. Deuxièmement, la let. b est légèrement reformulée, sans conduire à une modification matérielle.

Le terme « notamment » figure déjà à l'art. 9, al. 1 de l'ordonnance de 2007, mais il n'est pas inutile de rappeler qu'il est là pour souligner qu'il ne s'agit que d'un exemple et que d'autres situations peuvent se présenter. Par exemple, il est possible de suspendre ou de retirer la certification en cas de vérification spéciale ou spontanée d'un produit défectueux, même si les défauts n'ont pas été découverts dans le cadre d'une procédure de vérification formelle annuelle.

L'al. 2 ne subit que la modification formelle consistant à remplacer « l'organisme au bénéfice d'une certification » par la terminologie de l'art. 13 nLPD, à savoir « fournisseur de systèmes ou de logiciels de traitement de données personnelles, [le] responsable du traitement ou [le] sous-traitant au bénéfice d'une certification » et permettant ainsi de désigner qui sont les personnes qui peuvent bénéficier d'une certification (sur ce point, voir également les explications, *supra*, ch. 2).

L'al. 3 est supprimé, car il a été renoncé, d'une part, à communiquer au PFPDT si une certification a été octroyée ainsi que, d'autre part, à ce que le PFPDT tienne un registre des responsables privés ayant obtenu une certification et étant exemptés de l'obligation d'établir une analyse d'impact relative à la protection des données. Le PFPDT aurait souhaité que le titulaire de la certification soit tenu d'informer le PFPDT de la suspension ou du retrait de la suspension, dans la mesure où il aurait dû lui demander un avis préalable en cas de persistance de risques élevés pour la personnalité ou les droits fondamentaux de la personne concernée (voir à ce sujet les explications relatives à l'art. 10).

Art. 12 Procédure applicable aux mesures de surveillance du PFPDT

Cet article reprend essentiellement l'art. 10 de l'ordonnance de 2007. Le titre est modifié de sorte à utiliser le terme de PFPDT à la place de préposé PFPDT (sur cette modification terminologique, voir *supra*, ch. 2).

L'al. 1 est modifié sur le plan formel. La précision, dans l'ordonnance de 2007, selon laquelle les manquements sont constatés *dans le cadre de l'activité de surveillance du PFPDT* est supprimée, car elle n'est pas nécessaire. Cela entre en tous les cas dans les compétences du PFPDT au sens des art. 4 et 49 à 51 nLPD. Par ailleurs, comme pour l'art. 11, al. 2, la terminologie est adaptée afin de correspondre à l'art. 13 nLPD.

L'al. 2 n'est modifié que formellement, notamment sur le terme du préposé et de la terminologie adaptée à l'art. 13 nLPD.

L'al. 3 ne subit aussi que quelques modifications rédactionnelles. En particulier, la durée du délai de 30 jours pour remédier aux défauts est à nouveau explicitement mentionnée pour des raisons de clarté juridique.

L'al. 4 est modifié afin de renvoyer à l'article pertinent de la nLPD (art. 51, al. 1) ce qui a pour conséquence de devoir modifier les termes qualifiant l'action du PFPDT. En effet, il ne peut plus « émettre de recommandation » mais peut « prendre une mesure » à l'intention du fournisseur de systèmes ou de logiciels de traitement de données personnelles, du responsable du traitement ou du sous-traitant au bénéfice d'une certification ou de l'organisme de certification concerné. De même à la dernière phrase, il ne peut plus « adresser une recommandation », mais il peut « donner un ordre » à l'organisme de certification de suspendre ou de retirer la certification si celui-ci n'a pas lui-même suspendu ou retiré une certification malgré la persistance du manquement. Dans ce cas, il en informe le Service d'accréditation suisse, comme dans l'ordonnance de 2007.

3.5 Section 4 : dispositions finales

L'art. 13 règle l'abrogation de l'ordonnance de 2007 et l'art. 14 fixe la date d'entrée en vigueur de la nouvelle OCPD.

3.6 Annexe

Le titre, ainsi que les ch. 1 et 2 de l'annexe ne subissent que quelques changements formels par rapport à l'ordonnance de 2007 et sont précisés sur certains points.

1 Certification des systèmes de gestion

Le titre, la phrase introductive et la phrase finale sont modifiés afin de correspondre à la terminologie de la nouvelle ordonnance (sur ce point, voir aussi les explications relatives à l'art. 1, al. 2, let. a, *supra*). En outre, la phrase introductive, les tirets et la phrase finale sont modifiées dans la mesure où l'exigence de la preuve fait désormais partie du texte de l'ordonnance (cf. commentaire relatif à l'art. 1, al. 5, *supra*). Dans la phrase introductive, l'expression « pris dans son ensemble », déjà utilisée dans l'ordonnance de 2007, doit être comprise comme signifiant que l'ensemble de l'équipe qui effectue les examens doit remplir toutes les qualifications et non chaque individu, car il n'y a guère de spécialistes qui remplissent toutes les exigences.

En outre, le premier tiret n'est modifié que formellement (ajout de « dans le domaine ») afin d'être uniforme avec le deuxième tiret.

Dans le deuxième tiret, la notion, désormais désuète, de « sécurité informatique » est remplacée par celle de « sécurité de l'information » (voir dans ce sens également la nouvelle loi fédérale sur la sécurité de l'information, LSI, cf. FF 2020 9665).

Un troisième tiret, nouveau, est introduit. Il précise que le personnel qui certifie les systèmes de gestion doit non seulement disposer de connaissances dans les domaines de la protection des données et de la sécurité de l'information, prouvées par une activité pratique ou un diplôme, mais qu'il doit également être à jour avec les développements dans ces domaines, notamment en continuant de se perfectionner et en suivant des formations continues.

Enfin, le dernier tiret est réorganisé et est complété par la mention de deux normes ISO supplémentaires : la norme 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 la norme SN EN ISO/IEC 27006 (cf. *supra*).

Précisons encore que le terme « domaine » qui figure dans la dernière phrase (et qui n'est pas modifié en français, mais partiellement en allemand) se réfère aux deux « domaines » cités dans les deux premiers tirets, à savoir le domaine de la protection des données et celui de la sécurité de l'information. Comme dans l'ordonnance de 2007, il est précisé que l'évaluation des systèmes de gestion par une équipe interdisciplinaire est autorisée.

2 Certification des produits, des services et des processus

Toutes les adaptations faites au ch. 1 relatif à la certification des systèmes de gestion sont valables pour cette seconde partie de l'annexe relative à la certification des produits, des services et des processus, à l'exception de l'ajout – dans le dernier tiret – des références au programme de certification, aux lignes directrices du PFPDT et aux nouvelles normes ISO. Ces ajouts sont nécessaires parce que la norme ISO SN EN ISO/IEC 17065 (cf. *supra*), déjà mentionnée dans l'ordonnance de 2007, ne contient pas toutes les exigences nécessaires pour la certification de produits, de services et de processus en ce qui concerne les connaissances techniques du personnel qui effectue les certifications. Pour le reste, il est renvoyé par analogie aux explications fournies au ch. 1.