



Commentaire concernant l'ordonnance sur les certifications en matière de protection des données

La présente ordonnance se fonde sur le nouvel art. 11, al. 2, de la loi fédérale du 24 mars 2006 sur la protection des données (LPD)¹, qui prévoit que le Conseil fédéral édicte des dispositions sur la reconnaissance des procédures de certification et l'introduction d'un label de qualité de protection des données. Elle correspond au cadre fixé dans le message (FF 2203 1915). Elle prévoit deux objets de certification : d'une part l'organisation et la procédure de protection des données (système de gestion de la protection des données), d'autre part les produits (produits hardware, software ou des systèmes pour des procédures de traitement automatisées). L'ordonnance prescrit comme exigence de base que les organismes de certification doivent être accrédités. Cette condition permet d'avoir un contrôle uniforme des certificateurs et de limiter de manière considérable le besoin d'adopter une réglementation. L'ordonnance fixe en outre quelques exigences minimales applicables aux organismes et à la procédure de certification.

Concernant la création d'un label de qualité en matière de protection des données, deux solutions ont été envisagées :

- renoncer à un label de qualité officiel et laisser au seul secteur privé (en particulier aux organismes de certification) le soin de créer des labels que les organismes certifiés seront autorisés à utiliser, en règle générale contre paiement d'une redevance. L'ordonnance ne réglerait alors que les exigences concernant la certification, étant entendu qu'aucun label ne pourrait être utilisé sans que ces exigences soient remplies.
- instaurer un label de qualité officiel, qui pourrait être utilisé par les organismes certifiés sans autre condition. Les certifications ne seraient pas pour autant opérées par un organisme étatique. Ce label officiel serait une sorte de prestation de base offerte par l'Etat et coexisterait avec d'éventuels labels de qualité privés.

Dans un cas comme dans l'autre, il serait possible de confier le label de qualité à une entité mixte (semi-privée, semi-publique). Ce mode d'organisation a été écarté pour des raisons financières.

Un argument fondamental parle en faveur de la première solution (renoncer à un label officiel) : des labels de qualité privés s'inscriraient dans le droit fil de la démarche à l'origine de l'ordonnance. En effet, l'instauration des certifications en matière de protection des données vise à améliorer l'application du droit en la

¹ Texte sujet au référendum, FF 2006 3421.

matière par des mesures privées, l'activité de contrôle étant en partie « privatisée ». En outre, cette solution aurait l'avantage de favoriser l'initiative privée sur ce point. Enfin, sur le plan de la densité normative, l'ordonnance s'en trouverait allégée. Côté inconvénients, il existe un risque de voir apparaître une multitude de labels, ce qui nuirait à la transparence du marché. Des difficultés pourraient également se faire jour au cas où le titulaire d'un label ne remplirait pas (ou plus) les exigences légales.

Un label de qualité officiel pourrait indirectement empêcher ce foisonnement des labels. Il serait également accessible à tous les organismes certifiés, ce qui n'est pas absolument garanti par la première solution. En outre, la certification reviendrait moins cher car ni l'organisme certificateur ni l'organisme certifié ne devraient payer de redevance pour le label. Cette solution présente toutefois deux inconvénients majeurs : d'une part, elle fait intervenir l'Etat dans un domaine qui relève aujourd'hui entièrement du secteur privé ; d'autre part, elle accroît la densité normative.

Après avoir mis en balance les avantages et les inconvénients de ces deux solutions, on a donné la préférence à la première, dont les avantages l'emportent sur des inconvénients somme toute hypothétiques.

1 Exigences concernant les organismes de certification (art. 1)

Les conditions que les organismes de certification doivent remplir découlent principalement des guides ISO/CEI 62 (ISO/CEI 17021 nouveau) et 65 (qui deviendra prochainement également une norme ISO), dont l'application est prévue à l'art. 7, al. 1, et à l'annexe 2 de l'ordonnance sur l'accréditation et la désignation (OAccD ; RS 946.512). Ces normes fixent notamment l'exigence de l'indépendance et règlent la procédure de certification et d'essai des produits. Une réglementation supplémentaire dans l'ordonnance ci-jointe n'est pas nécessaire.

Il y a lieu en revanche de concrétiser les exigences relatives à la qualification des auditeurs ou du personnel qui certifie les produits. A ce propos, il faut tenir compte du fait que dans le domaine de la protection des données, il n'existe pas de formation standardisée et que les experts sont rares. Il convient dès lors de prendre en considération l'expérience pratique. Les exigences en la matière sont par conséquent concrétisées dans l'annexe 3.

L'al. 3 fait appel à la notion de programme de contrôle selon le modèle de l'ordonnance sur l'agriculture biologique (RS 910.18). Le programme de contrôle comporte, d'une part, le schéma d'essai qui détermine à l'avance, en termes de contenu, les normes à respecter, les points sur lesquels ces normes doivent porter et, d'autre part, les modalités concernant le déroulement de la procédure de contrôle (surveillance et réévaluation). Les « organismes » à certifier au sens de la let. a de cette disposition peuvent être des organisations privées ou des organes fédéraux. Un cabinet médical ou un cabinet d'avocats qui traitent régulièrement des données sont par exemple des organismes au sens de cette définition et peuvent faire l'objet d'une certification.

Les exigences minimales (al. 4) sont déterminées en premier lieu par les standards internationaux dont l'application découle de l'ordonnance sur l'accréditation et la désignation. Par ailleurs, le renvoi aux art. 4 à 6 de la présente ordonnance explicite clairement que la législation en matière de protection des données fait également partie des exigences minimales.

2 Implication du préposé dans la procédure d'accréditation (art. 2)

Cette disposition concrétise l'art. 11, al. 1 et 2, OAccD.

3 Reconnaissance des organismes de certification étrangers (art. 3)

Dans le domaine de la protection des données, il n'existe pas encore de normes harmonisées au niveau international en matière d'accréditation ni, de ce fait, de procédure définie en conséquence. Il est dès lors nécessaire de régler la reconnaissance des organismes de certification étrangers dans l'ordonnance. Cette disposition correspond à l'art. 29 de l'ordonnance sur l'agriculture biologique.

4 Certification du système de gestion de la protection des données (art. 4)

4.1 Remarques générales

L'al. 1 distingue clairement les différents objets de certification.

L'al. 2 détermine de manière générale l'objet de l'évaluation dans le cadre de la procédure d'audit. Les critères définissent le contenu du système de gestion de la protection des données: il s'agit tout d'abord de la charte de protection des données. Cette dernière consiste en un document de base qui définit les principes de protection des données applicables dans l'organisation concernée et énonce l'engagement de respecter la protection des données. Elle décrit la mise en place de mesures organisationnelles qui permettent de garantir le respect de la loi sur la protection des données ainsi que, le cas échéant, d'autres dispositions applicables en la matière. La façon de mettre en œuvre les dispositions en matière de protection des données et éventuellement les normes internationales qui définissent ce qu'on appelle la « bonne pratique » découle de cette charte. La procédure d'audit porte en outre sur les dispositions prises par le responsable du traitement des données pour réaliser les objectifs et les mesures définis en matière de protection des données. La mise en place de procédures visant à résoudre les problèmes ou à corriger les irrégularités constatées revêt donc une importance particulière.

L'al. 3 prescrit que le Préposé fédéral à la protection des données et à la transparence émet des directives sur les exigences minimales qu'un système de gestion de la protection des données doit remplir (voir ci-après ch. 4.2).

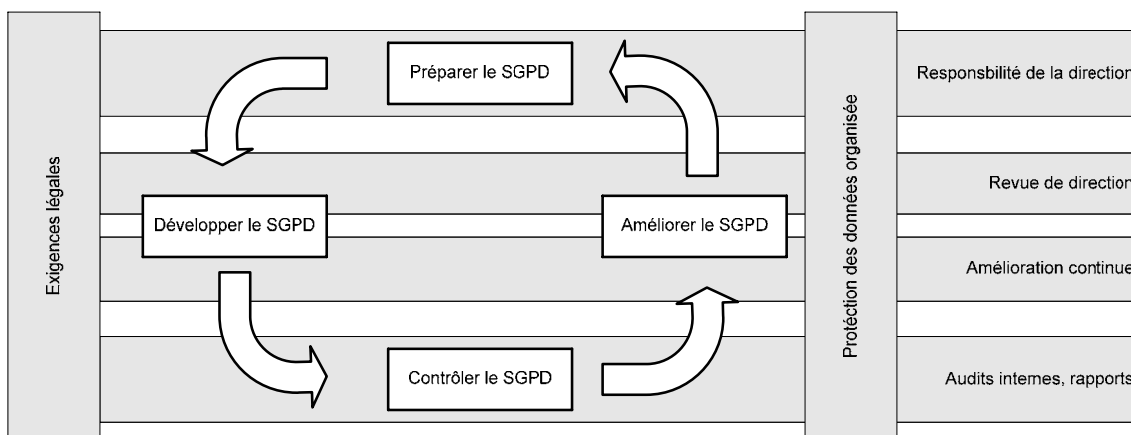
L'al. 4 précise la formulation du nouvel art. 11a, al. 5, LPD. Il prévoit expressément que le maître du fichier n'est délié de son devoir de déclarer son fichier que si tous les traitements de données effectués dans le cadre de la finalité de ce fichier et au moyen des données contenues ont été certifiés.

4.2 Exigences minimales concernant le système de gestion de la protection des données

4.2.1 Le système de gestion des données en sa qualité de « système de management »

L'al. 3, qui a pour objet les exigences minimales qu'un système de gestion de la protection des données doit remplir, fait référence notamment à la norme ISO 27001:2005 sur la sécurité de l'information². En effet, non seulement il existe un lien entre protection des données et sécurité informatique, mais de plus un système de gestion de la protection des données (SGPD) fonctionne selon les mêmes principes que les « systèmes de management » standardisés mis en œuvre dans d'autres domaines. Il peut donc être intégré simplement dans un système de management existant (par ex. un système de management de la qualité).

Le SGPD se base, comme les systèmes apparentés, sur le modèle dit « PDCA » (Plan, Do, Check, Act ; Planifier, Réaliser, Vérifier, Agir, ou Préparer, Développer, Contrôler, Améliorer). Ce modèle a pour but d'améliorer de manière constante la protection des données dans l'organisme concerné.



Le développement et la mise en œuvre d'un SGPD doivent être conformes au droit et sont déterminés notamment par la finalité et l'ampleur des traitements de données personnelles effectués, par les moyens employés et par la taille et la structure de l'organisme.

Sur le plan de l'organisation, une approche processus doit être mise en place : elle s'appliquera au développement, à la mise en œuvre, à la surveillance, à l'entretien et à l'amélioration continue du SGPD. Le modèle PDCA doit être appliqué à tous les processus du SGPD.

² Norme ISO/IEC 27001:2005 (peut être retirée auprès de l'Association suisse de normalisation).

Le SGPD est un système de management qui peut être exploité sans incompatibilité avec d'autres systèmes de management. Sa présentation est laissée au libre choix de l'organisme. Il peut s'inspirer d'exigences régissant d'autres systèmes de management, par exemple la norme ISO 27000:2005. Toutefois, les certificats correspondants ne suffisent pas à valider le SGPD, qui doit subir un contrôle spécifique ultérieur selon l'annexe 1.

4.2.2 Contenu des exigences

Pour mettre en place un SGPD, il faut définir son domaine d'application, une charte de protection des données (cf. ch. 4.1) et une méthode d'évaluation des risques concernant la sécurité des données. Il convient également d'identifier les exigences découlant des principes en matière de protection des données (cf. art. 4 ss LPD) ou d'autres bases juridiques et d'évaluer les risques pour la sécurité des données. On déterminera alors les mesures à prendre, qui devront être approuvées par la direction.

Afin de mettre en œuvre ces mesures, l'organisme devra prévoir des procédures permettant de détecter immédiatement les non-conformités et de les corriger, mais aussi d'identifier les manquements à la protection des données et de les éliminer.

Il devra contrôler régulièrement l'efficacité du SGPD, notamment grâce à des audits au minimum annuels, et mettre en œuvre les améliorations possibles (actions préventives et correctives).

Une documentation doit être élaborée. Elle comprendra notamment la charte de protection des données, une description du domaine d'application du système, la méthode d'évaluation des risques pour la sécurité des données et un rapport sur cette évaluation. Doivent également être disponibles le plan de conformité aux exigences de la protection des données, le plan de gestion des risques pour la sécurité des données et la description des processus nécessaires pour garantir l'efficacité de la planification, de la mise en œuvre et du contrôle de la charte. Tous ces documents doivent être approuvés par le service compétent avant leur diffusion, puis régulièrement vérifiés et actualisés, de sorte que les modifications et l'actualité du texte apparaissent clairement. Les personnes ou services compétents doivent disposer des versions les plus actuelles.

L'organisme devra établir et conserver des « enregistrements » (fichiers journaux, etc.) pour prouver la conformité du SGPD aux exigences et l'efficacité de son fonctionnement.

La direction de l'organisme est tenue d'assumer un certain nombre de responsabilités : d'abord établir la charte de protection des données, définir les rôles et les responsabilités en matière de protection des données, décider du niveau de risque acceptable pour la sécurité des données, procéder aux améliorations ; mais aussi libérer les ressources nécessaires pour maintenir une protection des données adéquate en appliquant correctement toutes les mesures mises en place et pour améliorer si nécessaire l'efficacité du SGPD. La direction

devra également sensibiliser son personnel aux exigences de la protection des données, notamment en veillant à une formation adéquate. Au moins une fois par an – plus précisément à l'issue des audits internes, des évaluations de l'efficacité et des modifications entreprises à l'intérieur ou à l'extérieur de l'organisme et pouvant avoir un impact sur le SGPD – elle devra contrôler et évaluer le système pour s'assurer de sa conformité et de son efficacité et, éventuellement, l'améliorer. Cet exercice, appelé « revue de direction », vise surtout à mettre à jour l'évaluation des risques et le plan de gestion des risques, à modifier les processus afin d'assurer la protection des données quand des événements internes ou externes l'exigent, à identifier les besoins en ressources et à améliorer les critères de l'évaluation de l'efficacité des mesures.

5 Certification de produits et de systèmes (art. 5)

5.1 Remarques générales

L'al. 1 définit les produits qui peuvent faire l'objet d'une certification. Une certification en matière de protection des données est judicieuse non seulement pour les produits dont la finalité est le traitement des données, mais aussi pour des produits qui génèrent des données personnelles lors de leur utilisation. A ce propos, 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. 2, let. a, se réfère aux mesures techniques, telles qu'elles découlent notamment de l'art. 8 OLPD. A ce propos, il existe un standard international constitué des « Common Criteria » (CC 2.1/ISO 15408) et des profils de protection pour des catégories spécifiques de produits, qui définissent certaines exigences en matière de sécurité. L'état de la technique est décisif pour déterminer quelles sont les exigences concrètes qui découlent de cette disposition.

L'al. 2, let. b, décrit le principe de l'économicité des données (collecte et utilisation minimales), qui constitue une concrétisation du principe de la proportionnalité de la protection des données.

L'al. 2, let. c, prévoit que le produit doit garantir la transparence des processus de traitement des données. L'utilisateur doit être en mesure de reconnaître les données personnelles traitées, leur mode de traitement et les destinataires de la transmission. Les exigences seront donc définies en fonction du cercle des utilisateurs pour lesquels le produit est conçu; elles seront donc plus élevées pour un produit réalisé pour un large spectre d'utilisateurs que pour un produit utilisé uniquement par des spécialistes. L'examen porte sur les traitements qu'un produit effectue de manière automatisée dans le cadre de la fonctionnalité pour laquelle il a été conçu. Si le produit est conçu de telle manière qu'il peut être utilisé pour différentes finalités ou qu'il peut être configuré de différentes façons, il y a lieu de vérifier que l'utilisateur ne puisse pas sans autre contourner ou mettre hors fonction les mécanismes garantissant la transparence.

L'al. 2, let. d, se réfère à la mise en place de mesures techniques permettant à l'utilisateur de respecter d'autres principes et obligations en matière de protection des données que ceux mentionnés aux let. a à c. A titre d'exemple, on peut citer la sauvegarde du principe de finalité grâce au produit à certifier, le contrôle automatisé resp. la limitation de la mise en réseau d'éléments d'une banque de données, le contrôle par le système de communications de données à des tiers, la mise en place de mesures permettant à l'utilisateur de respecter le droit d'accès de la personne concernée ainsi que des fonctions permettant de donner suite à des demandes d'effacement ou de destruction des données.

5.2 Exigences minimales concernant la certification de produits

L'al. 3 prévoit que le Préposé à la protection des données et à la transparence (préposé) édicte les directives fixant les critères spécifiques en matière de protection des données qu'un produit doit remplir dans le cadre d'une certification. Contrairement au cas des systèmes de gestion de la protection des données, il n'existe pas de normes internationalement reconnues qui pourraient être transposées.

L'al. 3 fixe un certain délai au préposé pour édicter des directives concernant la certification. En effet, des travaux sont en cours au niveau européen pour élaborer des normes de certification de produits en matière de protection des données. Il conviendrait dès lors de suivre l'évolution de ces travaux avant d'édicter des directives dans ce domaine.

Le préposé pourrait également s'inspirer de la grille d'évaluation élaborée par le centre de protection des données du *Land* de Schleswig-Holstein (*Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*)³. Ce document énumère en effet de manière exemplaire les exigences en matière de protection et de sécurité des données, sous forme d'une liste de questions se référant aux dispositions juridiques essentielles, structurée d'une manière qui permet de faire le tour de la question. Une simple *check-list* ne saurait entrer en ligne de compte car les profils d'exigences et les types de données diffèrent d'un produit ou d'un système informatique à l'autre. En outre, les experts doivent toujours motiver leur appréciation.

Les directives du préposé fixeront les exigences relatives aux aspects techniques, notamment en ce qui concerne la collecte et l'utilisation minimales des données et la transparence.

Elles préciseront les principes pertinents en matière de protection des données (art. 4 ss LPD), afin de permettre un examen de la légalité du traitement des données.

L'organisme de certification devra également contrôler les mesures techniques et organisationnelles soutenues par le produit pour protéger les personnes faisant l'objet du traitement de données. Ces mesures se fondent en premier lieu sur les

³ Anforderungskatalog V1.2 für die Begutachtung von IT-Produkten im Rahmen des Gütesiegelverfahrens beim ULD SH (<http://www.datenschutzzentrum.de/download/anford.pdf>).

art. 8 ss OLPD. Il faudra considérer, lors de l'examen, sur quel modèle théorique des attaques possibles se fondent les mesures prises ou à prendre, quelles attaques les mesures de protection inhérentes au produit sont en mesure de parer, quelles mesures supplémentaires sont soutenues par le produit (ou s'il y a à cet égard des limitations) et, enfin, quels sont les risques résiduels.

L'organisme de certification devra également vérifier si les droits des personnes sur lesquelles de données sont collectées (rectificatifs, renseignements, transparence, etc.) sont respectés. Pour garantir les droits des personnes concernées, on fait aujourd'hui beaucoup appel à des mesures organisationnelles. Il est décisif d'examiner dans quelle mesure, sur le plan technique, le produit à certifier :

- permet directement à la personne concernée de faire respecter ses droits, voire l'y encourage, et
- assiste l'opérateur du système, par des mesures organisationnelles, dans le respect des droits des personnes concernées.

Il convient en outre de tenir compte tant du principe de la collecte et de l'utilisation minimales des données (par ex. la possibilité d'opérer de manière anonyme ou sous un pseudonyme) que des questions de droits des personnes concernées au regard de la journalisation.

Enfin, il faut prendre en considération le fait que divers types de données sont traités et échangés entre les composantes d'un produit. Citons notamment les données relatives aux personnes faisant l'objet du traitement de données, appelées *données primaires* (par ex. les données des assurances sur leurs patients), et les *données secondaires* (par ex. les données journalisées concernant l'entrée de données ou les interventions dans la banque de données, ou bien encore les modifications de configuration ou l'accès à des locaux sensibles tels que les centres de calcul).

6 Octroi et durée de validité de la certification (art. 6)

L'al. 1 prévoit expressément que les exigences que doivent remplir l'organisme ou le produit à certifier résultent d'une part des dispositions légales applicables en matière de protection des données et d'autre part des directives du préposé. Dans le futur, Il existera également des normes internationales ou européennes de certification en matière de protection des données. Dans ce cas, une certification pourra également être effectuée sur la base de ces normes, pour autant que les exigences de ces normes soient équivalentes à celles des directives du préposé.

L'al. 2 fixe à trois ans la durée de validité de la certification d'une organisation ou d'une procédure (système de gestion de la protection des données). Il prévoit également explicitement que les certifications accordées sont réévaluées annuellement (voir la prescription correspondante du guide ISO/CEI 62, ch. 3.6.1). L'organisme de certification doit mettre en place un dispositif de surveillance approprié.

Un système analogue est prévu pour la certification des produits (al. 3). Les produits certifiés doivent être à nouveau évalués au plus tard tous les deux ans. Lorsque des modifications apportées au produit ont des répercussions sur le traitement des données personnelles, il y a lieu de procéder à une nouvelle certification dans les meilleurs délais (guide ISO/CEI 65, al. 13). S'il s'agit d'une modification mineure, un examen sommaire suffit.

À l'expiration de la durée de validité, la procédure complète doit à nouveau être effectuée, aboutissant, le cas échéant, à une nouvelle certification.

7 Reconnaissance des certifications étrangères en matière de protection des données (art. 7)

Il est opportun de prévoir un mécanisme permettant la reconnaissance des certifications étrangères. Des organismes certifiés à l'étranger pourraient ainsi être déliés de leur devoir de déclarer leurs fichiers. Tel pourrait être le cas, par exemple, lorsqu'une entreprise fait l'objet d'une certification en matière de protection des données en Allemagne et que la procédure de certification porte également sur une partie de l'entreprise située en Suisse. Il incombe au préposé d'examiner si les critères de certification appliqués à l'étranger correspondent matériellement aux exigences du droit suisse.

8 Communication du résultat de la procédure de certification au préposé (art. 8)

Cette disposition se réfère au nouvel art. 11a, al. 5, let. f, LPD. Elle détermine les documents qui doivent être transmis au préposé. Les informations qui doivent être contenues dans le rapport d'évaluation et dans les documents de certification sont définies dans le guide ISO/CEI 62, ch. 3.5. Les documents de certification contiennent des indications sur l'organisme qui a effectué la certification, les bases juridiques de cette dernière, les procédures et les services qui ont été certifiés et la durée de validité de la certification. Le rapport d'évaluation contient des indications détaillées sur la conformité du système de gestion de la protection des données aux exigences en matière de certification. Il doit indiquer clairement les non-conformités. Il peut en outre mentionner les différences avec les résultats d'audits précédents. Enfin, il doit rapporter les différends éventuels entre l'organisme de certification et l'organisme au bénéfice d'une certification.

A ce propos, il convient de relever que dans le cadre de ses tâches de surveillance le préposé peut exiger l'accès à d'autres documents en rapport avec la certification (art. 27 et 29 LPD).

Il résulte du renvoi à l'art. 4 que seule la certification d'un système de gestion de la protection des données délie l'organisme certifié de son obligation de déclaration. La simple utilisation de produits certifiés par le responsable de traitement ou par le maître du fichier ne suffit pas, au motif qu'elle n'offre pas de garanties suffisantes quant au respect des prescriptions de protection des données. La présente

disposition précise par conséquent la teneur du nouvel art. 11a, al. 5, let. f, LPD en relation avec le nouvel art. 11, al. 1, LPD.

9 Suspension et révocation de la certification (art. 9)

L'organisme de certification pourra suspendre ou révoquer la certification s'il constate des manquements graves lors de ses vérifications régulières ou à l'occasion d'un renouvellement de la certification. Il y a manquement grave notamment lorsque les conditions essentielles de la certification ne sont plus remplies. Ce serait le cas si l'on constatait à plusieurs reprises que les exigences concernant la documentation (v. ch. 4.2.2) ne sont pas remplies ou que la direction a omis plusieurs fois de procéder à une revue (v. ch. 4.2.2). De même, l'utilisation abusive d'un certificat constitue un manquement grave : par exemple, seule une partie des procédures de traitement de données a été certifiée (art. 4, al. 1, let. b), mais l'organisme utilise un label de qualité correspondant à une certification complète.

Le guide ISO/CEI 62 (la future norme ISO/IEC 17021⁴) prévoit déjà cette sanction (ch. 3.7.3 de la remarque 6), qui représente un principe essentiel de l'accréditation. Il s'agit en fait d'une disposition déclaratoire qui doit être énoncée dans l'ordonnance pour des raisons de clarté. Par conséquent, les modalités relatives à la suspension et à la révocation ne sont pas réglées dans l'ordonnance. Il convient en outre de relever que cette disposition *ne* confère *pas* au certificateur la compétence de rendre une décision. L'al. 2 prescrit enfin qu'en cas de litige, la procédure et le droit au fond sont régis par les dispositions légales applicables aux contrats.

10 Procédure applicable aux mesures de surveillance du préposé (art. 10)

La certification en matière de protection des données concerne en premier lieu les rapports juridiques entre particuliers, qui relèvent principalement du droit privé. Cela correspond au concept d'autorégulation : la certification vise à utiliser les mécanismes du marché pour améliorer la mise en œuvre du droit de la protection des données.

Le préposé ne doit donc pas empiéter directement sur ces rapports de droit privé. S'il constate, dans le cadre de son activité de surveillance, des manquements graves, il doit avoir la possibilité d'intervenir afin de faire respecter les prescriptions légales applicables. L'art. 10 définit la procédure. En vertu de cette disposition, le préposé ne peut toutefois pas suspendre ou révoquer lui-même la certification.

Si le préposé constate que des conditions essentielles de la certification ne sont pas respectées ou que le certificat est utilisé de manière abusive ou trompeuse, il doit tout d'abord s'adresser à l'organisme de certification compétent et l'informer

⁴ La date d'entrée en vigueur n'est pas encore connue.

des manquements constatés (al. 1). Il incombe à l'organisme de certification d'intervenir auprès de l'organisme certifié en l'invitant à prendre les mesures nécessaires afin de remédier à la situation dans un délai de 30 jours. Si ce dernier n'est pas en mesure d'y donner suite dans le délai fixé, l'organisme de certification suspend la certification (al. 3). Une fois le délai de 30 jours écoulé, il révoque la certification si l'organisme certifié n'est pas en mesure de remédier à la situation dans un délai convenable. Par délai convenable, on entend une durée maximale de trois mois.

Si l'organisme au bénéfice d'une certification ne remédie pas à la situation dans le délai fixé et si l'organisme de certification ne suspend ni ne révoque la certification, le préposé établit une recommandation au sens des art. 27, al. 4, et 29, al. 3, LPD. La recommandation est adressée à l'organisme de certification ou à l'organisme certifié, selon que la responsabilité des défauts incombe à l'un ou à l'autre. Si la recommandation est adressée à l'organisme de certification, le Service d'accréditation suisse doit en être informé en tant qu'autorité de surveillance. Si la recommandation n'est pas suivie ou si elle est rejetée, le préposé peut saisir les tribunaux en exigeant une décision du Tribunal administratif fédéral et recourir, le cas échéant, auprès du Tribunal fédéral⁵.

En cas d'irrégularités graves (par exemple lorsque l'organisme de certification a été trompé pour octroyer un certificat ou lorsque de faux certificats sont détenus), il y a lieu d'examiner si les éléments constitutifs d'une infraction sont réalisés dans le cas d'espèce (escroquerie, tromperie, etc.).

Enfin, il convient de relever que les concurrents concernés, les clients, ainsi que certaines organisations, en particulier les organisations de défense des consommateurs, pourraient également, en vertu des art. 9 et 10 de la loi fédérale du 19 décembre 1986 contre la concurrence déloyale, intenter action, lorsque des certificats ou des labels de qualité sont utilisés sans que les exigences correspondantes ne soient satisfaites.

11 Exigences minimales concernant les qualifications du personnel des organismes de certification (annexe)

Les qualifications minimales dont doit disposer le personnel d'un organisme de certification qui entend procéder à des certifications en matière de protection des données sont fixées en annexe. Comme il existe peu de spécialistes remplissant l'ensemble des conditions, il sera possible de mener des audits et des examens des produits en équipe interdisciplinaire, pourvu que les membres de cette équipe totalisent l'ensemble des exigences requises.

⁵ Selon le droit en vigueur, le préposé a la faculté de saisir les tribunaux uniquement en ce qui concerne le secteur privé. Dès l'entrée en vigueur de la révision, il pourra exercer cette faculté également dans le cadre de ses tâches de surveillance sur les organes fédéraux (art. 27, al. 6, nouveau, LPD).