
# Avis 15/2020 sur le projet de décision des autorités de contrôle compétentes allemandes concernant l'approbation des exigences en matière d'agrément d'un organisme de certification au titre de l'article 43, paragraphe 3, du RGPD

**Adopté le 25 mai 2020**

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Adopté

## Table des matières

## Le comité européen de la protection des données (le «comité»),

vu l'article 63, l'article 64, paragraphe 1, point c), l'article 64, paragraphes 3 à 8, et l'article 43, paragraphe 3, du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (ci-après le «RGPD»),

vu l'accord EEE et, en particulier, son annexe XI et son protocole 37, tels que modifiés par la décision du comité mixte de l'EEE nº 154/2018 du 6 juillet 2018[1],

vu les articles 10 et 22 de son règlement intérieur du 25 mai 2018,

considérant ce qui suit:

(1) Le rôle principal du comité est de garantir l'application cohérente du règlement (UE) 2016/679 (ci-après le «RGPD») dans l'ensemble de l'Espace économique européen. Conformément à l'article 64, paragraphe 1, du RGPD, le comité émet un avis chaque fois qu'une autorité de contrôle compétente envisage d'approuver les exigences en matière d'agrément des organismes de certification au titre de l'article 43 dudit règlement. L'objectif du présent avis est dès lors de mettre au point une approche harmonisée concernant les exigences qu'une autorité de contrôle de la protection des données ou que l'organisme national d'accréditation appliquera aux fins de l'agrément d'un organisme de certification. Même si le RGPD n'impose pas un ensemble unique d'exigences en matière d'agrément, il favorise la cohérence. Le comité cherche à atteindre cet objectif dans ses avis, premièrement en encourageant les autorités de contrôle à définir leurs exigences en matière d'agrément sur la base de la structure présentée à l'annexe 1 de ses lignes directrices 4/2018 relatives à l'agrément des organismes de certification et, deuxièmement, en les analysant à l'aide de son modèle de comparaison (conformément à la norme ISO 17065 et aux lignes directrices du comité relatives à l'agrément des organismes de certification).

(2) En vertu de l'article 43 du RGPD, les autorités de contrôle compétentes adoptent des exigences en matière d'agrément. Elles appliquent toutefois le mécanisme de contrôle de la cohérence afin que le mécanisme de certification puisse susciter la confiance, notamment en fixant un niveau élevé d'exigences.

(3) Si les exigences en matière d'agrément sont soumises au mécanisme de contrôle de la cohérence, elles ne doivent pas ipso facto être identiques. Les autorités de contrôle compétentes jouissent d'une marge d'appréciation par rapport au contexte national ou régional et doivent tenir compte de leur législation locale. L'objectif de l'avis du comité n'est pas d'obtenir un ensemble unique d'exigences au sein de l'Union, mais plutôt d'éviter de graves incohérences susceptibles, par exemple, d'ébranler la confiance en l'indépendance ou en l'expertise des organismes de certification agréés.

(4) Les «Lignes directrices 4/2018 relatives à l'agrément des organismes de certification au titre de l'article 43 du règlement général sur la protection des données (2016/679)» (ci-après les «lignes directrices»), et les «Lignes directrices 1/2018 relatives à la certification et à la définition des critères

[1] Dans le présent avis, on entend par «Union» l'«EEE».

de certification conformément aux articles 42 et 43 du règlement (UE) 2016/679» serviront de fil conducteur dans le cadre du mécanisme de contrôle de la cohérence.

(5) Si un État membre exige que les organismes de certification soient agréés par l'autorité de contrôle, cette même autorité devrait établir des exigences en matière d'agrément, y compris, mais sans s'y limiter, les exigences exposées à l'article 43, paragraphe 2. Comparé aux obligations relatives à l'agrément d'organismes de certification par des organismes nationaux d'accréditation, l'article 43 contient moins d'informations quant aux exigences en matière d'agrément lorsque l'autorité de contrôle procède elle-même à l'agrément. Dans le but de contribuer à une approche harmonisée de l'agrément, les exigences en la matière appliquées par l'autorité de contrôle devraient être orientées par la norme ISO IEC 17065/2012 et être complétées par les exigences supplémentaires établies par une autorité de contrôle conformément à l'article 43, paragraphe 1, point b). Le comité fait remarquer que l'article 43, paragraphe 2, points a) à e), reflète et précise les exigences de la norme ISO IEC 17065/2012, ce qui contribuera à la cohérence[2].

(6) L'avis du comité est adopté conformément à l'article 64, paragraphe 1, point c), et à l'article 64, paragraphes 3 et 8, du RGPD, en liaison avec l'article 10, paragraphe 2, du règlement intérieur du comité, dans un délai de huit semaines à compter du premier jour ouvrable suivant la date à laquelle la présidente et l'autorité de contrôle compétente ont décidé que le dossier était complet. Sur décision de la présidente, ce délai peut être prolongé de six semaines en fonction de la complexité de la question.

**A ADOPTÉ L'AVIS SUIVANT:**

# 1 RÉSUMÉ DES FAITS

1. Les autorités de contrôle allemandes de la Fédération et des Länder (ci-après les «autorités de contrôle allemandes») ont présenté au comité leur projet d'exigences en matière d'agrément au titre de l'article 43, paragraphe 1, point b). Le dossier a été jugé complet le 13 février 2020. L'organisme national d'accréditation allemand, le DAkks, procédera à l'agrément des organismes de certification en utilisant les critères d'agrément du RGPD. En d'autres termes, l'organisme national d'accréditation utilisera la norme ISO 17065 et les exigences supplémentaires établies par les autorités de contrôle allemandes dès que celles-ci les auront approuvées, après avis du comité sur le projet d'exigences, afin d'agréer des organismes de certification.

2. Conformément à l'article 10, paragraphe 2, du règlement intérieur du comité, en raison de la complexité du dossier, la présidente a décidé de prolonger de six semaines supplémentaires la période d'adoption initiale de huit semaines.

[2] Paragraphe 39 des lignes directrices 4/2018 relatives à l'agrément des organismes de certification au titre de l'article 43 du règlement général sur la protection des données. Disponibles à l'adresse suivante: https://edpb.europa.eu/our-work-tools/our-documents/smjernice/guidelines-42018-accreditation-certification-bodies-under_fr

# 2 ÉVALUATION

## 2.1 Raisonnement général du comité concernant le projet de décision présenté

3. Le présent avis a pour objet d'évaluer les exigences en matière d'agrément établies par une autorité de contrôle, par rapport à la norme ISO 17065 ou à un ensemble complet d'exigences, afin de permettre à un organisme national d'accréditation ou à une autorité de contrôle d'agréer, conformément à l'article 43, paragraphe 1, du RGPD, un organisme de certification chargé de délivrer et de renouveler une certification conformément à l'article 42 du RGPD, et ce, sans préjudice des missions et des pouvoirs de l'autorité de contrôle compétente. En l'espèce, le comité fait valoir que les autorités de contrôle allemandes ont décidé de faire appel à leur organisme national d'accréditation, le DAkkS, et à l'autorité de contrôle compétente, pour délivrer des agréments et ont mis en place des exigences supplémentaires conformes aux lignes directrices, qui devraient être utilisées pour délivrer un agrément.

4. La présente évaluation des exigences supplémentaires des autorités de contrôle allemandes en matière d'agrément a pour but d'examiner des variantes (ajouts ou suppressions) par rapport aux lignes directrices et, notamment, à son annexe 1. En outre, l'avis du comité porte également sur tous les aspects susceptibles d'avoir une incidence sur une approche harmonisée de l'agrément des organismes de certification.

5. Il y a lieu de constater que l'objectif des lignes directrices relatives à l'agrément des organismes de certification est d'aider les autorités de contrôle à définir leurs exigences en la matière. L'annexe des lignes directrices ne constitue pas une liste d'exigences en matière d'agrément proprement dites. Les autorités de contrôle doivent par conséquent définir les exigences relatives à l'agrément des organismes de certification de sorte à garantir leur application pratique et cohérente selon leur situation.

6. Le comité reconnaît que, compte tenu de leur expertise, les organismes nationaux d'accréditation et, le cas échéant, les autorités compétentes, devraient bénéficier d'une liberté de manœuvre lorsqu'ils élaborent certaines dispositions spécifiques dans le cadre des exigences applicables en matière d'agrément. Le comité estime toutefois nécessaire de souligner que, lorsque des exigences supplémentaires sont établies, elles devraient être définies de manière à permettre leur application pratique et harmonisée et leur contrôle, le cas échéant.

7. Le comité relève que les normes ISO, notamment la norme ISO 17065, sont soumises à des droits de propriété intellectuelle et il ne fera dès lors pas référence au texte du document connexe dans le présent avis. Le comité a donc décidé de mentionner, le cas échéant, des parties spécifiques de la norme ISO, sans toutefois en reproduire le libellé.

8. Enfin, le comité a procédé à son évaluation en suivant la structure visée à l'annexe 1 des lignes directrices (ci-après l'«annexe»). Lorsque le présent avis reste silencieux sur une section spécifique du projet d'exigences en matière d'agrément des autorités de contrôle allemandes, il convient de comprendre que le comité n'a aucune observation à formuler et qu'il ne demande pas aux dites autorités de prendre des mesures supplémentaires.

9. Le présent avis ne porte pas sur les points présentés par les autorités de contrôle allemandes qui ne relèvent pas du champ d'application de l'article 43, paragraphe 2, du RGPD, comme les références à

la législation nationale. Le comité indique néanmoins que la législation nationale devrait être conforme au RGPD lorsque cela est nécessaire.

## 2.2 Principales questions d'intérêt (article 43, paragraphe 2, du RGPD et annexe 1 des lignes directrices du comité) prévues dans les exigences en matière d'agrément devant faire l'objet d'une évaluation cohérente

1) Traitement de l'ensemble des domaines clés décrits dans l'annexe des lignes directrices, et examen de tout écart par rapport à cette annexe.

2) Indépendance de l'organisme de certification.

3) Conflits d'intérêts de l'organisme de certification.

4) Expertise de l'organisme de certification.

5) Garanties appropriées pour veiller à l'application correcte des critères de certification par l'organisme de certification.

6) Procédures en vue de la délivrance, de l'examen périodique et du retrait d'une certification délivrée en vertu du RGPD.

7) Traitement transparent des réclamations relatives aux violations de la certification.

10. Compte tenu du fait que:

a. l'article 43, paragraphe 2, du RGPD établit une liste des domaines d'agrément qu'un organisme de certification doit aborder pour être agréé;

b. l'article 43, paragraphe 3, du RGPD prévoit que les exigences en matière d'agrément des organismes de certification sont approuvées par l'autorité de contrôle compétente;

c. l'article 57, paragraphe 1, points p) et q), du RGPD prévoit qu'une autorité de contrôle compétente doit rédiger et publier les exigences en matière d'agrément des organismes de certification et peut décider de procéder elle-même à l'agrément des organismes de certification;

d. l'article 64, paragraphe 1, point c), du RGPD dispose que le comité émet un avis chaque fois qu'une autorité de contrôle envisage d'adopter les exigences en matière d'agrément d'un organisme de certification conformément à l'article 43, paragraphe 3;

e. si l'organisme national d'accréditation procède à l'agrément conformément à la norme ISO/IEC 17065/2012, les exigences supplémentaires établies par l'autorité de contrôle compétente doivent également être appliquées;

f. l'annexe 1 des lignes directrices relatives à l'agrément des organismes de certification contient des suggestions d'exigences que l'autorité de contrôle de la protection des données rédige et qui s'appliquent durant l'agrément d'un organisme de certification par l'organisme national d'accréditation;

le comité est de l'avis suivant:

### 2.2.1 INTRODUCTION

11. Le comité reconnaît que les conditions de coopération qui régissent les rapports entre un organisme national d'accréditation et son autorité de contrôle de la protection des données ne constituent pas en soi une exigence relative à l'agrément des organismes de certification. Toutefois, par souci d'exhaustivité et de transparence, le comité estime que ces conditions de coopération, lorsqu'elles existent, doivent être rendues publiques sous une forme que l'autorité de contrôle juge appropriée.

### 2.2.2 TERMES ET DÉFINITIONS

12. Le comité note qu'au chapitre 3 («Définitions») du projet d'exigences en matière d'agrément des autorités de contrôle allemandes, sont définis les types de programmes de certification autorisés, précisant qu'ils doivent répondre aux exigences de la norme DIN EN ISO/IEC 17065. À cet égard, il convient de souligner que les sections 5.1 et 5.2 des lignes directrices du comité énoncent déjà de manière exhaustive ce qui peut être certifié en vertu du RGPD. Par conséquent, le comité reconnaît que l'intention des autorités de contrôle allemandes n'est pas de limiter ce qui est énoncé dans les lignes directrices et que les déclarations contenues au chapitre 3 du projet d'exigences en matière d'agrément des autorités de contrôle allemandes doivent être considérées comme étant applicables dans le cadre desdites exigences.

### 2.2.3 REMARQUES GÉNÉRALES

13. Le comité note que la section «notes générales» du projet d'exigences en matière d'agrément des autorités de contrôle allemandes fait référence à l'«autorisation» des critères de certification par le comité «conformément à l'article 63 et à l'article 64, paragraphe 1, point c), du RGPD». Le comité note que le RGPD ne lui donne pas compétence pour «autoriser» des critères de certification. Toutefois, selon les articles susmentionnés, le comité peut approuver des critères de certification. Par conséquent, le comité recommande aux autorités de contrôle compétentes allemandes de supprimer la référence à l'«autorisation du comité» afin de mettre le projet en conformité avec le libellé du RGPD.

### 2.2.4 EXIGENCES GÉNÉRALES RELATIVES À L'AGRÉMENT (chapitre 4 du projet d'exigences en matière d'agrément)

14. En ce qui concerne l'exigence relative à la responsabilité juridique (section 4.1 du projet d'exigences en matière d'agrément des autorités de contrôle allemandes), le comité note que, dans le document justificatif, les autorités de contrôle allemandes expliquent que l'on s'attend à ce que l'organisme de certification soit doté de procédures à jour et que, par conséquent, il n'est pas nécessaire d'ajouter des exigences supplémentaires à cet égard. Toutefois, le comité considère qu'une attente n'oblige pas les organismes de certification à être doté de telles procédures. Comme indiqué à la section 4.1.1 de l'annexe des lignes directrices, les organismes de certification sont dotés de procédures à jour démontrant la conformité aux responsabilités juridiques établies dans les conditions d'agrément. En outre, l'organisme de certification doit être à même de prouver que ses procédures et mesures sont conformes au RGPD en ce qui concerne spécifiquement le contrôle et le traitement des données personnelles de l'organisation cliente dans le cadre du processus de certification. Par conséquent, le

comité recommande aux autorités de contrôle allemandes de modifier le projet d'exigences afin de le mettre en conformité avec les lignes directrices.

15. En ce qui concerne la sous-section 4.1.2.2 du projet d'exigences en matière d'agrément des autorités de contrôle allemandes («contrat de certification»), le comité note que le projet d'exigences en matière d'agrément des autorités de contrôle allemandes n'inclut pas l'obligation d'autoriser la pleine transparence vis-à-vis des autorités de contrôle compétentes s'agissant de la procédure de certification, y compris en ce qui concerne des questions contractuellement confidentielles. En outre, l'obligation pour le demandeur de fournir à l'organisme de certification l'accès à ses activités de traitement n'est pas mentionnée. Par conséquent, le comité recommande aux autorités de contrôle allemandes d'inclure les obligations susmentionnées dans leur projet.

16. Le comité fait observer que les missions et pouvoirs de l'autorité de contrôle compétente (alinéa 3 de la section 4.1.2 de l'annexe) ne sont pas explicitement mentionnés dans la sous-section 4.1.2.2 du projet d'exigences en matière d'agrément des autorités de contrôle allemandes. Le comité est d'avis qu'il convient d'ajouter cette mention dans le projet d'exigences et, par conséquent, il recommande aux autorités de contrôle allemandes de modifier le projet en conséquence.

17. En outre, le projet d'exigences des autorités de contrôle allemandes concernant le contrat de certification ne comprend pas l'obligation d'autoriser l'organisme de certification à divulguer toutes les informations nécessaires à la délivrance de la certification conformément à l'article 42, paragraphe 8, et à l'article 43, paragraphe 5, du RGPD (alinéa 7 de la section 4.1.2 de l'annexe). Bien que cette obligation figure dans la section de gestion du processus du projet d'exigences en matière d'agrément des autorités de contrôle allemandes, le comité considère qu'elle devrait faire partie du contrat de certification, afin de renforcer son caractère contraignant. Par conséquent, le comité recommande aux autorités de contrôle allemandes d'inclure l'obligation susmentionnée dans le cadre des éléments du contrat de certification.

18. Selon l'annexe, le demandeur doit tenir l'organisme de certification informé d'éventuels changements significatifs concernant sa situation réelle, sa situation juridique et ses produits, procédés et services concernés par la certification (alinéa 10 de la section 4.1.2 de l'annexe). Cependant, dans le projet d'exigences en matière d'agrément des autorités de contrôle allemandes, l'alinéa 6 de la sous-section 4.1.2.2 ne comprend que l'obligation d'informer l'organisme de certification de changements significatifs concernant la situation réelle ou la situation juridique du demandeur, mais il ne mentionne pas explicitement les produits, procédés et services. Le comité recommande aux autorités de contrôle allemandes d'inclure cette mention, conformément à l'annexe.

19. En ce qui concerne la sous-section 4.2.7 du projet d'exigences en matière d'agrément des autorités de contrôle allemandes («gestion de l'impartialité»), le comité recommande de renforcer les critères applicables aux organismes de certification qui appartiennent à une entité légale distincte ou qui sont contrôlés par celle-ci, afin de tenir compte du fait que tout type de relation économique entre l'organisme de certification et l'entité légale, en fonction de ses caractéristiques, est susceptible d'affecter l'impartialité de ses activités de certification.

20. En ce qui concerne la section 4.6 du projet d'exigences en matière d'agrément des autorités de contrôle allemandes («informations accessibles au public»), le comité note qu'il n'y a pas de référence à la publication de toutes les versions des critères approuvés et des procédures de certification. Par conséquent, le comité invite les autorités de contrôle allemandes à modifier le projet d'exigences en matière d'agrément afin d'indiquer explicitement que la publication comprend toutes les versions des critères approuvés et toutes les procédures de certification. En outre, le comité note que le deuxième

paragraphe de la section 4.6 indique que «les programmes de certification utilisés par l'organisme de certification les critères approuvés conformément à l'article 42, paragraphe 5, du RGPD indiquant la durée autorisée de la demande, *sont généralement publiés*». Pour éviter toute ambiguïté, le comité invite les autorités de contrôle allemandes à supprimer le mot «généralement» et à insérer «et» entre «organisme de certification» et «les critères approuvés».

### 2.2.5 EXIGENCES RELATIVES AUX RESSOURCES (chapitre 6 du projet d'exigences en matière d'agrément)

21. En ce qui concerne les exigences relatives à l'expertise et, plus précisément, la sous-section 6.1.2.1 du projet d'exigences en matière d'agrément des autorités de contrôle allemandes («compétences en matière de ressources humaines»), le comité note qu'il n'est pas précisé que les connaissances requises dans les domaines énumérés doivent être pertinentes et appropriées. Afin de garantir la cohérence avec le niveau d'expertise requis dans l'annexe, le comité recommande aux autorités de contrôle allemandes d'aligner le libellé sur celui des lignes directrices, en exigeant que les connaissances soient pertinentes et appropriées.

22. En outre, le comité note que les membres du personnel ayant une expertise technique et qui sont responsable des décisions doivent justifier d'au moins sept ans d'expérience professionnelle ou cinq ans d'expérience professionnelle dans la protection technique des données, en fonction de leur niveau d'études, tandis que les membres du personnel responsables des évaluations doit posséder quatre ans d'expérience professionnelle ou deux ans d'expérience professionnelle dans la protection technique des données ainsi que d'une expérience concernant les procédures de test, en fonction de leur niveau d'études. De même, les membres du personnel ayant une expertise juridique et qui sont responsables des décisions doivent justifier d'au moins cinq ans d'expérience professionnelle, tandis que les membres du personnel responsables des évaluations doivent avoir au moins deux ans d'expérience dans la législation relative à la protection des données et les procédures d'audit. Le comité constate que le nombre minimum d'années d'expérience professionnelle requis diffère sensiblement entre les membres du personnel responsables des décisions et les membres du personnel responsables des évaluations. Sur ce point, le comité considère que les exigences relatives aux compétences pour les évaluateurs et les décideurs doivent être adaptées en tenant compte des différentes missions dont ils s'acquittent, plutôt que du nombre d'années d'expérience. De l'avis du comité, les évaluateurs devraient avoir une expertise plus spécialisée et une expérience professionnelle en matière de procédures techniques (par exemple, les audits et les certifications), tandis que les décideurs devraient avoir une expertise plus générale et plus complète et une expérience professionnelle dans le domaine de la protection des données. Compte tenu de ce qui précède, le comité invite les autorités de contrôle allemandes à mettre davantage l'accent sur les différentes connaissances et/ou expériences de fond des évaluateurs et des décideurs et à réduire les divergences au niveau des années d'expérience requises pour ces membres du personnel.

23. En outre, le comité considère que la connaissance des systèmes de gestion concernant le domaine de la certification devrait être étendue à la norme ISO/IEC 27701:2019 - 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 et il invite les autorités de contrôle allemandes à inclure une telle référence.

24. Enfin, en ce qui concerne les exigences relatives aux études pour le personnel technique, le comité considère que la liste des matières est déjà adaptée à l'expertise technique requise par l'annexe. Par conséquent, le comité invite les autorités de contrôle allemandes à supprimer les «sciences naturelles» de la liste des matières concernant les études universitaires du personnel technique.

### 2.2.6 EXIGENCES RELATIVES AUX PROCESSUS (chapitre 7 du projet d'exigences en matière d'agrément)

25. Le comité note que le chapitre 7 du projet d'exigences en matière d'agrément des autorités de contrôle allemandes contient plusieurs références au terme «ses critères» (par exemple aux sections 7.4, 7.6, 7.11 et 7.13). Afin d'éviter toute ambigüité, le comité invite les autorités de contrôle allemandes à clarifier la signification de ce terme, par exemple en ajoutant une explication à l'annexe 1 (glossaire).

26. En ce qui concerne la section 7.1 du projet d'exigences en matière d'agrément des autorités de contrôle allemandes («informations générales»), le comité note l'absence de référence explicite à l'obligation pour l'organisme de certification de se conformer aux exigences supplémentaires. Si cette obligation peut être déduite du texte du projet d'exigences, le comité considère qu'une référence explicite à l'obligation susmentionnée devrait être incluse. Le comité recommande dès lors aux autorités de contrôle allemandes de modifier le projet en conséquence.

27. Le comité note que le projet d'exigences supplémentaires des autorités de contrôle allemandes ne contient pas de référence à l'exploitation d'un label européen de protection des données approuvé, conformément à la section 7.1.2 de l'annexe. Le comité est d'avis qu'il convient d'inclure cette référence, surtout compte tenu du fait qu'il sera peut-être nécessaire de procéder à l'agrément d'un organisme de certification délivrant des labels européens de protection de données dans chacun des États membres où l'organisme de certification est établi[3]. Le comité recommande dès lors aux autorités de contrôle allemandes d'inclure la référence susmentionnée. Par exemple, le projet d'exigences pourrait indiquer ce qui suit: *«L'autorité de contrôle compétente est informée avant qu'un organisme de certification ne commence à exploiter un label européen de protection des données approuvé dans un nouvel État membre depuis un bureau satellite».*

28. Le comité note qu'à la section 7.2 («demande»), le projet d'exigences en matière d'agrément des autorités de contrôle allemandes prévoit la situation du recours à des sous-traitants pour mener les opérations de traitement, conformément à l'annexe des lignes directrices. Le comité note toutefois que, en cas de recours à des sous-traitants, la demande contient le(s) contrat(s) entre le responsable du traitement et le sous-traitant, comme indiqué dans l'annexe. Par conséquent, le comité recommande aux autorités de contrôle allemandes d'aligner le texte sur celui des lignes directrices en incluant la référence au(x) contrat(s) entre le responsable du traitement et le sous-traitant. En outre, le comité invite les autorités de contrôle allemandes à examiner si une référence aux co-responsables du traitement et à leur organisation spécifique devrait aussi être mentionnée dans ce cas.

29. Le comité note que la section 7.2 du projet d'exigences en matière d'agrément des autorités de contrôle allemandes précise que «le responsable du traitement et le sous-traitant ont le droit de demander une certification». La possibilité pour les sous-traitants de demander une certification dépendra du programme spécifique de certification. Par conséquent, afin d'éviter toute confusion, le

[3] À cet égard, voir les lignes directrices 1/2018, paragraphe 44.

comité invite les autorités de contrôle allemandes à supprimer la référence ci-dessus ou à préciser que la possibilité pour les sous-traitants d'être certifiés dépendra du champ d'application du programme de certification.

30. En ce qui concerne la section 7.3 du projet d'exigences en matière d'agrément des autorités de contrôle allemandes («demandes d'évaluation»), le comité note que le projet d'exigences en matière d'agrément des autorités de contrôle allemandes indique que «les méthodes d'évaluation prévues sont stipulées dans un contrat [...]». Afin d'indiquer clairement qu'il s'agit d'une exigence, le comité invite les autorités de contrôle allemandes à reformuler le premier paragraphe, afin d'indiquer clairement que les méthodes d'évaluation sont incluses dans le contrat de certification - c'est-à-dire reformuler l'exigence de la manière suivante: «les méthodes d'évaluation prévues sont stipulées dans un contrat [...]». En outre, le comité invite les autorités de contrôle allemandes à remplacer la référence au point 7.3.1.b de la norme ISO 17065 par le point 7.3 de la norme ISO 17065, afin d'aligner le texte sur celui de l'annexe. En outre, le comité observe que le paragraphe 4 fait référence aux compétences techniques et juridiques appropriées. Dans un souci de clarté, le comité invite les autorités de contrôle allemandes à ajouter «dans le domaine de la protection des données».

31. Le comité observe que la section 7.4 du projet d'exigences en matière d'agrément des autorités de contrôle allemandes («méthodes d'évaluation») ne comprend pas l'obligation pour l'organisme de certification de décrire suffisamment de méthodes d'évaluation afin de déterminer si la ou les opérations de traitement sont conformes aux critères de certification. Le comité recommande aux autorités de contrôle allemandes de modifier le projet d'exigences afin d'inclure cette référence. Elles pourraient notamment ajouter le paragraphe suivant: *«L'organisme de certification veille à ce que les mécanismes utilisés pour délivrer une certification décrivent suffisamment de méthodes d'évaluation afin de déterminer si la ou les opérations de traitement sont conformes aux critères de certification».* En outre, en ce qui concerne le premier domaine qui doit être couvert dans les méthodes d'évaluation, le comité considère que la nécessité et la proportionnalité sont évaluées également en ce qui concerne les personnes concernées, le cas échéant. Enfin, le comité note l'absence de référence à la documentation des méthodes et des conclusions. Par conséquent, le comité invite les autorités de contrôle allemandes à modifier le projet et à inclure explicitement ces références.

32. En ce qui concerne les certifications existantes (section 7.4 du projet d'exigences en matière d'agrément des autorités de contrôle allemandes), le comité considère que l'alinéa 4 à la page 13 prête à confusion, étant donné qu'il est difficile de déterminer quel est le lien entre les périodes de validité de la certification actuelle et de la certification précédente, et comment elles s'imbriqueraient. En outre, il ne semble pas possible de remettre en cause la validité d'une certification précédemment délivrée par un autre organisme de certification agréé. Pour résumer, le paragraphe gagnerait à être clarifié en ce qui concerne le lien entre les différents éléments mentionnés. Le comité recommande aux autorités de contrôle allemandes de modifier le projet, en particulier en précisant que la période de validité de la certification au titre du RGPD ne doit pas dépendre de la validité d'autres types de certification.

33. En ce qui concerne la section 7.5 («évaluation») du projet d'exigences en matière d'agrément des autorités de contrôle allemandes, le comité invite les autorités de contrôle allemandes à modifier le titre de la section et à le remplacer par «examen».

34. En ce qui concerne les changements ayant des conséquences sur la certification (section 7.10 du projet d'exigences en matière d'agrément des autorités de contrôle allemandes), le comité note que le projet d'exigences en matière d'agrément des autorités de contrôle allemandes prévoit que «le client est

informé en temps voulu des changements apportés au cadre juridique le concernant». Compte tenu de la nécessité de préserver l'impartialité de l'organisme de certification, le comité invite les autorités de contrôle allemandes à reformuler la phrase pour indiquer clairement que le client reçoit, en temps voulu, des informations générales sur les changements susceptibles de le concerner. En outre, afin de bien comprendre de ce qui est entendu par «décisions du comité européen de la protection des données», le comité invite les autorités de contrôle allemandes à préciser la référence. Elles pourraient, par exemple, faire référence aux «documents adoptés par le comité européen de la protection des données».

35. Le comité observe que la section 7.11 du projet d'exigences en matière d'agrément des autorités de contrôle allemandes («résiliation, restriction, suspension ou retrait de la certification») ne contient pas l'obligation pour l'organisme de certification d'accepter les décisions et les ordres émanant des autorités de contrôle allemandes afin de retirer une certification à un demandeur ou de ne pas la lui délivrer si les exigences applicables à la certification ne sont pas ou plus satisfaites. Le comité recommande dès lors aux autorités de contrôle allemandes d'inclure une telle obligation. En outre, le comité invite les autorités de contrôle allemandes à remplacer le mot «restriction» par «réduction» dans le titre de la section, conformément à l'annexe des lignes directrices.

### 2.2.7 AUTRES EXIGENCES SUPPLÉMENTAIRES

36. En ce qui concerne la sous-section 8.11.3 du projet d'exigences en matière d'agrément des autorités de contrôle allemandes («gestion des réclamations»), le comité invite les autorités de contrôle allemandes à remplacer la référence aux «réclamations justifiées» par une référence aux «réclamations étayées», pour plus de clarté.

## 3 CONCLUSIONS/RECOMMANDATIONS

37. Le projet d'exigences en matière d'agrément des autorités de contrôle allemandes de la Fédération et des Länder peut donner lieu à une application incohérente de l'agrément des organismes de certification et les modifications ci-après doivent être apportées.

38. En ce qui concerne les «remarques générales», le comité recommande aux autorités de contrôle allemandes:

    1) de supprimer la référence à l'«autorisation du comité», afin de mettre le projet en conformité avec le libellé du RGPD.

39. En ce qui concerne les «exigences générales relatives à l'agrément», le comité recommande aux autorités de contrôle allemandes:

    1) de modifier les exigences concernant la responsabilité juridique (sous-section 4.1) afin de les mettre en conformité avec les lignes directrices.

    2) de modifier la sous-section 4.1.2.2 pour inclure, dans le contrat de certification, l'obligation d'autoriser la pleine transparence vis-à-vis des autorités de contrôle allemandes s'agissant de la procédure de certification et de fournir à l'organisme de certification l'accès aux activités de traitement du demandeur.

3) d'inclure, à la sous-section 4.1.2.2, une référence explicite aux missions et pouvoirs de l'autorité de contrôle compétente, conformément à l'annexe.

4) d'inclure, parmi les éléments du contrat de certification, l'obligation d'autoriser l'organisme de certification à divulguer toutes les informations nécessaires à la délivrance de la certification conformément à l'article 42, paragraphe 8, et à l'article 43, paragraphe 5, du RGPD.

5) d'inclure une référence explicite aux «produits, procédés et services concernés par la certification» au paragraphe 6 de la sous-section 4.1.2.2.

6) de renforcer, à la sous-section 4.2.7, les critères applicables aux organismes de certification qui appartiennent à une entité légale distincte ou qui sont contrôlés par celle-ci, afin de tenir compte du fait que tout type de relation économique entre l'organisme de certification et l'entité légale, en fonction de ses caractéristiques, est susceptible d'affecter l'impartialité de ses activités de certification.

40. En ce qui concerne les «exigences relatives aux ressources», le comité recommande aux autorités de contrôle allemandes:

1) d'aligner le libellé de la sous-section 6.1.2.1 sur celui des lignes directrices, en exigeant que les connaissances soient pertinentes et appropriées.

41. En ce qui concerne les «exigences relatives au processus», le comité recommande aux autorités de contrôle allemandes:

1) de modifier la section 7.1 afin qu'elle contienne une référence explicite à l'obligation pour l'organisme de certification de respecter les exigences supplémentaires.

2) d'inclure une référence à l'exploitation d'un label européen de protection des données approuvé.

3) d'aligner le libellé de la section 7.2 sur celui des lignes directrices en incluant la référence au(x) contrat(s) entre le responsable du traitement et le sous-traitant.

4) d'inclure à la section 7.4 l'obligation pour l'organisme de certification de décrire suffisamment de méthodes d'évaluation aux fins de déterminer si la ou les opérations de traitement sont conformes aux critères de certification.

5) de préciser à la section 7.4 que la période de validité de la certification prévue par le RGPD ne doit pas dépendre de la validité d'autres types de certifications.

6) d'inclure, à la sous-section 7.11, l'obligation pour l'organisme de certification d'accepter les décisions et les ordres émanant des autorités de contrôle allemandes afin de retirer une certification à un demandeur ou de ne pas la lui délivrer si les exigences applicables à la certification ne sont plus satisfaites.

# 4 REMARQUES FINALES

42. Le présent avis est adressé aux autorités de contrôle allemandes de la Fédération et des Länder et sera publié conformément à l'article 64, paragraphe 5, point b), du RGPD.

43. Conformément à l'article 64, paragraphes 7 et 8, du RGPD, les autorités de contrôle allemandes font savoir au président du comité par voie électronique, dans un délai de deux semaines suivant la réception de l'avis, si elles maintiendront ou si elles modifieront leur projet de décision. Dans le même délai, elles fournissent le projet de décision modifié ou, si elles n'ont pas l'intention de suivre l'avis du comité, en tout ou en partie, elles fournissent les motifs pertinents pour lesquels elles n'ont pas l'intention de suivre cet avis.

44. Les autorités de contrôle allemandes communiquent la décision finale au comité en vue de son inclusion dans le registre des décisions ayant fait l'objet d'un examen dans le cadre du mécanisme de contrôle de la cohérence, conformément à l'article 70, paragraphe 1, point y), du RGPD.

Pour le comité européen de la protection des données

La présidente

(Andrea Jelinek)