Avis 4/2020 relatif au projet de décision de l'autorité de contrôle compétente du Royaume-Uni concernant l'approbation des exigences relatives à l'agrément d'un organisme de certification conformément à l'article 43, paragraphe 3, du RGPD

Adopté le 29 janvier 2020

Adopté

Table des matières

Le comité européen de la protection des données,

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'article 51, paragraphe 1, b), de la directive (UE) 2016/680 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 (ci-après la «directive»),

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 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 européen de la protection des données (ci-après le «comité») émet un avis chaque fois qu'une autorité de contrôle envisage d'approuver les exigences relatives à l'agrément d'organismes de certification en application de l'article 43. Cet avis vise donc à créer une approche harmonisée en ce qui concerne les exigences qu'une autorité de contrôle de la protection des données ou l'organisme national d'accréditation appliquera pour 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 s'efforce d'atteindre cet objectif dans ses avis, tout d'abord, en encourageant les autorités de contrôle à rédiger leurs exigences en matière d'agrément en suivant la structure présentée à l'annexe des lignes directrices du comité relatives à l'agrément des organismes de certification et, ensuite, en les analysant à l'aide d'un modèle fourni par le comité et permettant de comparer les exigences (sur la base de la norme ISO 17065 et des lignes directrices du comité relatives à l'agrément des organismes de certification).

(2) En ce qui concerne 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 d'instaurer une confiance dans le système de certification, notamment en fixant un niveau d'exigence élevé.

(3) Bien que les exigences en matière d'agrément soient soumises au mécanisme de contrôle de la cohérence, cela ne signifie toutefois pas qu'elles doivent être identiques. Les autorités de contrôle compétentes disposent d'un pouvoir d'appréciation au regard du contexte national ou régional et doivent tenir compte de la législation locale. L'avis du comité ne vise pas à parvenir à un ensemble unique d'exigences européennes, mais plutôt à éviter des incohérences importantes susceptibles de

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

porter atteinte, par exemple, à la confiance dans l'indépendance ou 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 relatives à la certification et à la définition des critères de certification conformément aux articles 42 et 43 du règlement 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 d'accréditation nationaux, l'article 43 contient moins de détails sur les 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 utilisées par l'autorité de contrôle devraient être guidées par la norme ISO/IEC 17065 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 17065, 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 le président et l'autorité de contrôle compétente ont décidé que le dossier était complet. Sur décision du président, 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. L'autorité de contrôle britannique a présenté son projet d'exigences en matière d'agrément au titre de l'article 43, paragraphe 1, point b), au comité. À la suite d'une décision jugeant le dossier complet, le projet a été diffusé le 25 octobre 2019. L'organisme national d'accréditation britannique (UKAS) 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 l'autorité de contrôle dès que celle-ci les aura approuvées, après avis du comité sur le projet d'exigences, afin d'accréditer des organismes de certification.

2. Conformément à l'article 10, paragraphe 2, du règlement intérieur du comité, compte tenu de la complexité du dossier, la présidente a décidé de prolonger de six semaines le délai initial d'adoption de huit semaines.

[2] Paragraphe 39 des lignes directrices: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_en.pdf

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'accréditer, 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. Cette évaluation ne porte pas préjudice aux tâches et aux missions de l'autorité de contrôle compétente. En l'espèce, le comité fait valoir que l'autorité de contrôle britannique a décidé de faire appel à son organisme national d'accréditation pour délivrer des agréments et a mis en place des exigences supplémentaires conformes aux lignes directrices, que l'organisme national d'accréditation devrait utiliser lorsqu'il délivre un agrément.

4. La présente évaluation des exigences supplémentaires de l'autorité de contrôle britannique en matière d'agrément a pour but d'examiner des variantes (ajouts ou suppressions) par rapport aux lignes directrices et, notamment, à son annexe. 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 est à noter que l'objectif des lignes directrices relatives à l'agrément des organismes de certification est d'aider les autorités de contrôle lorsqu'elles définissent leurs exigences en matière d'agrément. L'annexe des lignes directrices ne constitue pas à proprement parler des exigences relatives à l'agrément. Par conséquent, les exigences relatives à l'agrément des organismes de certification doivent être définies par l'autorité de contrôle de manière à permettre leur application pratique et harmonisée, comme l'impose le contexte de l'autorité de contrôle.

6. Le comité reconnaît que, compte tenu de leur expertise, les organismes nationaux d'accréditation devraient bénéficier d'une liberté de manœuvre lorsqu'elles 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. Lorsque le présent avis ne commente pas une section spécifique du projet d'exigences de l'autorité de contrôle britannique en matière d'agrément, cela devrait être interprété comme signifiant que le comité n'a pas de commentaire à faire et ne demande pas à l'autorité de contrôle britannique de prendre d'autre mesure.

9. Le présent avis ne porte pas sur les points présentés par l'autorité de contrôle britannique 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 Principaux points de l'évaluation (article 43, paragraphe 2, du RGPD et annexe 1 des lignes directrices du comité) que prévoient les exigences relatives à l'agrément afin que les éléments suivants soient évalués de manière harmonisée:

a. examen de tous les domaines clés mis en évidence dans l'annexe des lignes directrices et analyse de tout écart par rapport à l'annexe;

b. indépendance de l'organisme de certification;

c. conflits d'intérêt de l'organisme de certification;

d. expertise de l'organisme de certification;

e. mesures adéquates de sauvegarde afin de veiller à ce que les critères de certification du RGPD soient correctement appliqués par l'organisme de certification;

f. procédures de délivrance, d'examen périodique et de retrait d'une certification au titre du RGPD;

g. transparence du traitement 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 traiter pour être agréé;

b. l'article 43, paragraphe 3, du RGPD dispose que les exigences relatives à l'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 dispose qu'une autorité de contrôle compétente doit rédiger et publier les critères 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 critères 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 PRÉFACE (Section 0 du projet d'exigences supplémentaires en matière d'agrément)

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.

12. Le comité prend acte du fait que l'autorité de contrôle britannique met en place ces conditions de coopération avec son organisme national d'accréditation et que, dès qu'elles seront finalisées, ces conditions seront publiées sur le site internet de l'autorité de contrôle.

2.2.2 EXIGENCES GÉNÉRALES EN MATIÈRE D'AGRÉMENT (Section 4 du projet d'exigences supplémentaires en matière d'agrément)

13. En ce qui concerne l'exigence relative à la responsabilité juridique (sous-section 4.1.1), le comité prend note du fait que l'autorité de contrôle britannique impose que l'organisme de certification agréé «*devrait être en mesure d'apporter, au cours de la procédure d'agrément, la preuve de sa conformité*» avec le RGPD et la loi britannique de 2018 sur la protection des données. Afin de garantir une évaluation et une mise en œuvre adéquates de cette exigence, le comité invite l'autorité de contrôle britannique à remplacer la phrase «*devrait être en mesure d'apporter la preuve*» par «apporte la preuve». Le comité recommande dès lors à l'autorité de contrôle britannique de modifier le projet en conséquence.

14. En ce qui concerne l'accord de certification (sous-section 4.1.2) et, en particulier, l'exigence nº 8 (nº 9 dans l'annexe), le comité prend note du fait que l'autorité de contrôle britannique a reformulé une partie de l'exigence visée à l'annexe 1 des lignes directrices. L'autorité de contrôle britannique a toutefois omis une référence à la phrase [le cas échéant]: «les conséquences pour le client devraient également être examinées». Le comité recommande donc à l'autorité de contrôle britannique d'ajouter la partie manquante de l'exigence susmentionnée.

15. En ce qui concerne l'utilisation de labels et de marques de protection des données (sous-section 4.1.3), le comité relève que l'autorité de contrôle britannique demande qu'une copie «*du label/de la marque/du logo devrait être fourni(e) à l'ICO pour ses archives*». Étant donné que les labels, marques et logos sont traités non seulement par l'organisme de certification, mais également par le propriétaire du système, le comité invite l'autorité de contrôle britannique à mentionner également les labels, marques et logos prévus dans les systèmes de certification approuvés par elle.

2.2.3 EXIGENCES EN MATIÈRE DE RESSOURCES (Section 6 du projet d'exigences supplémentaires en matière d'agrément)

16. En ce qui concerne le personnel de l'organisme de certification (sous-section 6.1) et, en particulier, le point 6, le comité prend note du fait que l'autorité de contrôle britannique a prévu que «*Le personnel chargé des décisions de certification doit posséder une grande expérience professionnelle en matière d'identification et de mise en œuvre de mesures de protection des données*». Le comité estime toutefois que, si le personnel qui adopte des décisions de certification peut ne pas posséder lui-même une «*grande expérience professionnelle en matière d'identification et de mise en œuvre de mesures*

de protection des données», il devrait à tout le moins avoir accès à quelqu'un qui possède cette expertise afin de prendre une décision éclairée. Une grande expérience professionnelle dans la mise en œuvre de ces mesures, au moins au début, ne sera probablement pas très répandue dans ce secteur. Le comité encourage donc l'autorité de contrôle britannique à exiger que l'organisme de certification définisse et explique les exigences en matière d'expérience professionnelle qui sont requises pour le système de certification.

2.2.4 EXIGENCES EN MATIÈRE DE TRAITEMENT, ARTICLE 43, PARAGRAPHE 2, POINTS C) ET D) (Section 7 du projet d'exigences supplémentaires en matière d'agrément)

17. En ce qui concerne la sous-section générale sur les exigences en matière de traitement (sous-section 7.1) et, en particulier, le paragraphe 4, le comité prend note de l'exigence supplémentaire imposée à l'organisme de certification de garantir qu'il procède à une enquête ou à un audit lorsque le respect de la protection des données est mis en cause. Le comité comprend que le respect de la protection des données concerne le titulaire de la certification. Néanmoins, ce point devrait être précisé dans les exigences. De plus, le comité est d'avis que l'autorité de contrôle britannique devrait préciser qu'une telle enquête devrait être liée à la portée de la certification et à l'objectif de l'évaluation. Le comité recommande dès lors que l'autorité de contrôle britannique modifie son exigence en conséquence, en indiquant clairement que le respect de la protection des données vise le titulaire de la certification et en précisant que l'enquête devrait être liée à la portée de la certification et à l'objectif de l'évaluation.

18. En ce qui concerne l'application des exigences de traitement (sous-section 7.2), le comité prend note du fait qu'il est nécessaire que l'organisme de certification précise «*s'il est fait appel à des sous-traitants et, lorsque des sous-traitants sont les demandeurs, leurs tâches et missions sont décrites et la demande contient le(s) contrat(s) du responsable du traitement/sous-traitant pertinent*». Tout en reconnaissant que l'autorité de contrôle britannique a repris le libellé de l'annexe 1, le comité l'invite à examiner la question de savoir s'il conviendrait également de faire référence aux responsables conjoints du traitement et à leurs accords spécifiques dans ce cas.

19. S'agissant des méthodes d'évaluation (sous-section 7.4), le comité prend note de l'exigence supplémentaire prévue par l'autorité de contrôle qui impose ce qui suit: «*Outre le point 7.4.5 de la norme ISO 17065, il est prévu que la certification existante, qui concerne le même objet, puisse être prise en compte dans le cadre d'une nouvelle évaluation [...]*». À cet égard, le comité juge nécessaire de préciser que, dans les cas où une certification existante est prise en compte dans le cadre d'une nouvelle évaluation, la portée de cette certification devrait également être évaluée de manière approfondie en ce qui concerne son respect des critères de certification pertinents. Le comité recommande dès lors à l'autorité de contrôle britannique de clarifier le texte en conséquence.

20. En ce qui concerne la phrase «*Le rapport d'évaluation complet ou les informations complètes permettant une évaluation de l'activité de certification antérieure et de ses résultats peuvent être pris en considération*», le comité recommande à l'autorité de contrôle britannique de remplacer «peuvent» par «sont», lorsque l'organisme de certification décide de tenir compte d'une certification existante. De plus, le comité considère qu'il serait plus clair de parler simplement de «certification» plutôt que d'«activité de certification» et il recommande à l'autorité de contrôle britannique de modifier le projet en conséquence. En outre, la référence à la «certification antérieure» pourrait être équivoque, étant donné qu'elle ne fait pas clairement référence à la certification existante que

l'organisme de certification souhaite prendre en compte dans le cadre de sa propre évaluation. Le comité invite l'autorité de contrôle britannique à modifier le libellé afin de préciser que la référence vise la certification existante. Enfin, le comité relève que l'organisme de certification devrait pouvoir accéder au rapport d'évaluation et à toute autre information pertinente permettant d'évaluer l'activité de certification afin de pouvoir prendre une décision éclairée. Le comité recommande dès lors à l'autorité de contrôle britannique de clarifier le texte en conséquence.

21. Par ailleurs, au paragraphe commençant par «*Outre le point 7.4.5 de la norme ISO 17065*», le comité estime que, lorsque l'autorité de contrôle britannique fait référence à «son mécanisme de certification», elle veut en fait dire «le système de certification». Le comité recommande dès lors à l'autorité de contrôle britannique de modifier le texte en conséquence.

22. S'agissant des changements qui touchent la certification (sous-section 7.10) et, en particulier, le quatrième point («décisions du comité européen de la protection des données»), le comité reconnaît que l'autorité de contrôle britannique a utilisé le libellé visé à l'annexe 1. Toutefois, afin de bien comprendre de ce qui est entendu par «décisions du comité européen de la protection des données», le comité invite l'autorité de contrôle britannique à préciser la référence. Elle pourrait, par exemple, faire référence aux «documents adoptés par le comité européen de la protection des données».

3 CONCLUSIONS/RECOMMANDATIONS

23. Le projet d'exigences relatives à l'agrément de l'autorité de contrôle britannique peut donner lieu à une application incohérente de l'agrément des organismes de certification et les modifications ci-après doivent être apportées.

24. En ce qui concerne les «exigences générales en matière d'agrément», le comité recommande à l'autorité de contrôle britannique de:

    1. remplacer, à la sous-section 4.1.1, la phrase «devrait être en mesure d'apporter la preuve» par «est en mesure d'apporter la preuve»;

    2. inclure à la sous-section 4.1.2 la partie manquante de l'exigence afin de l'aligner sur le texte de l'annexe 1 des lignes directrices.

25. En ce qui concerne les «exigences en matière de traitement», le comité recommande à l'autorité de contrôle britannique de:

    1. modifier la sous-section 7.1 afin de préciser que le respect de la protection des données vise le titulaire de la certification et que l'enquête devrait être liée à la portée de la certification et à l'objectif de l'évaluation;

    2. modifier la sous-section 7.4 en remplaçant «peuvent» par «sont» et «activité de certification» par «certification»;

    3. remplacer la référence au «mécanisme de certification» par «système de certification».

4 OBSERVATIONS FINALES

26. Le présent avis est adressé à l'autorité de contrôle britannique et il sera publié conformément à l'article 64, paragraphe 5, point b), du RGPD.

27. Conformément à l'article 64, paragraphes 7 et 8, du RGPD, l'autorité de contrôle fait savoir au président du comité par voie électronique, dans un délai de deux semaines suivant la réception de l'avis, si elle maintiendra ou si elle modifiera son projet de liste. Dans le même délai, elle fournit le projet de liste modifié ou, si elle n'a pas l'intention de suivre l'avis du comité, en tout ou en partie, elle fournit les motifs pertinents pour lesquels elle n'a pas l'intention de suivre cet avis.

Pour le comité européen de la protection des données

La présidente

(Andrea Jelinek)

Adopté