Avis 14/2020 sur le projet de décision de l'autorité de contrôle compétente irlandaise concernant l'approbation des exigences relatives à l'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 relatives à l'agrément des organismes de certifications au titre de l'article 43 de ce 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 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 de prescriptions relatives à l'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 prescriptions relatives à l'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, du RGPD. Comparé aux obligations relatives à l'agrément d'organismes de certification par des organismes nationaux d'accréditation, l'article 43 du RGPD 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 et être complétées par les exigences supplémentaires établies par une autorité de contrôle conformément à l'article 43, paragraphe 1, point b), du RGPD. Le comité fait remarquer que l'article 43, paragraphe 2, points a) à e), du RGPD, reflète et précise les exigences de la norme ISO IEC 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 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 RESUME DES FAITS

1. L'autorité de contrôle irlandaise a présenté son projet d'exigences en matière d'agrément au titre de l'article 43, paragraphe 1, point b), au comité. Le dossier a été jugé complet le 13 février 2020. L'organisme national d'accréditation irlandais (INAB) procédera à l'agrément des organismes de certification en utilisant les critères d'agrément du RGPD. En d'autres termes, l'INAB utilisera la norme ISO 17065 et les exigences supplémentaires établies par l'autorité de contrôle irlandaise 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, 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'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, et ce, sans préjudice des missions et des pouvoirs de l'autorité de contrôle compétente. En l'espèce, le comité fait valoir que l'autorité de contrôle irlandaise 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 irlandaise 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. L'autorité de contrôle doit par conséquent définir les prescriptions relatives à l'agrément des organismes de certification de sorte à garantir leur application pratique et cohérente selon sa situation.

6. Le comité reconnaît que, compte tenu de leur expertise, les organismes nationaux d'accréditation 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 ne commente pas une section spécifique du projet d'exigences en matière d'agrément de l'autorité de contrôle irlandaise, il convient de comprendre que le comité n'a aucune observation à formuler et qu'il ne demande pas à ladite autorité de prendre des mesures supplémentaires.

9. Le présent avis ne porte pas sur les points présentés par l'autorité de contrôle irlandaise 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 accrédité;

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 relatives à l'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 relatives à l'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 exposé ci-après.

2.2.1 PRÉFACE (section 0 du projet d'exigences en matière d'agrément de l'autorité de contrôle irlandaise)

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 que la référence aux lignes directrices sur l'agrément sous la désignation «WP 261» n'est pas mise à jour. Le comité a adopté 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). Le comité recommande par conséquent à l'autorité de contrôle irlandaise de modifier le libellé et de faire référence aux lignes directrices 4/2018

2.2.3 REMARQUES GÉNÉRALES

13. Le comité constate que le projet d'exigences de l'autorité de contrôle irlandaise fait référence à plusieurs reprises à «l'autorité de contrôle compétente». Étant donné que l'autorité de contrôle compétente en l'espèce est l'autorité de contrôle irlandaise, le comité encourage celle-ci à remplacer la référence par «le CPD» ou «l'autorité de contrôle irlandaise» afin d'éviter toute confusion.

14. Le comité note que le projet d'exigences de l'autorité de contrôle irlandaise comprend une section sur les termes et définitions. Toutefois, certains des termes ne sont pas utilisés de manière cohérente dans tout le document (par exemple «objet d'évaluation» et «cible de l'évaluation»). Afin d'éviter toute confusion, le comité encourage l'autorité de contrôle irlandaise à utiliser une terminologie cohérente dans le projet d'exigences.

2.2.4 EXIGENCES GÉNÉRALES EN MATIÈRE D'AGRÉMENT (section 4 du projet d'exigences en matière d'agrément)

15. En ce qui concerne le point 7 de la sous-section 4.1.2 du projet d'exigences en matière d'agrément de l'autorité de contrôle irlandaise, le comité estime que la formulation est quelque peu imprécise quant à savoir à qui s'adressent les motifs d'approbation de la certification. En outre, la référence à la «simplification» du registre manque également de clarté. Par conséquent, le comité encourage l'autorité de contrôle irlandaise à reformuler ce point de manière à le clarifier.

2.2.5 EXIGENCES STRUCTURELLES (section 5 du projet d'exigences en matière d'agrément)

16. Le comité note que le projet d'exigences en matière d'agrément de l'autorité de contrôle irlandaise fait référence à la nomination d'une «personne ayant l'ancienneté requise chargée de veiller au respect de la protection des données et à la gouvernance de l'information». La référence à l'ancienneté requise devrait être précisée en ce qui concerne l'expérience et l'étendue de l'autorité. En outre, les fonctions de ce poste semblent similaires à celles d'un délégué à la protection des données. Le comité encourage l'autorité de contrôle irlandaise à définir clairement les fonctions de ce poste et à préciser l'expérience requise.

2.2.6 EXIGENCES EN MATIÈRE DE RESSOURCES (section 6 du projet d'exigences en matière d'agrément)

17. En ce qui concerne le personnel des organismes de certification (sous-section 6.1), le comité note que les exigences relatives au personnel ayant une expertise technique chargé de prendre des décisions incluent le fait d'avoir au moins cinq ans d'expérience professionnelle en rapport avec l'objet de la certification, tandis que le personnel chargé des évaluations devrait avoir au moins deux ans d'expérience professionnelle. De même, le personnel compétent en matière juridique chargé de prendre des décisions doit avoir au moins cinq ans d'expérience professionnelle, tandis que les personnes chargées des évaluations doivent avoir au moins deux ans d'expérience. Le comité constate que le nombre minimum d'années d'expérience professionnelle requis entre le personnel chargé de la prise de décision et le personnel chargé de l'évaluation diffère sensiblement. À cet égard, le comité estime que l'accent devrait être mis sur les différents types d'expertise plutôt que sur le nombre d'années d'expérience professionnelle. 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 encourage l'autorité de contrôle irlandaise 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.

2.2.7 EXIGENCES EN MATIÈRE DE PROCESSUS (section 7 du projet d'exigences en matière d'agrément)

18. En ce qui concerne la sous-section 7.10 du projet d'exigences en matière d'agrément de l'autorité de contrôle irlandaise («Modifications ayant une incidence sur la certification»), le comité observe qu'il n'est nullement fait mention des procédures de modification à convenir, conformément à la section 7.10 de l'annexe. Le comité encourage l'autorité de contrôle irlandaise à inclure une telle référence et à mentionner certaines des procédures qui pourraient être mises en place (par exemple, périodes de transition, processus d'approbation avec l'autorité de contrôle compétente...). En outre, le comité considère que les modifications relatives à l'état de la technique sont également pertinentes et peuvent avoir une incidence sur la certification. Le comité encourage donc l'autorité de contrôle irlandaise à inclure cette possibilité dans la liste des modifications ayant une incidence sur la certification. Enfin, le comité se félicite de l'inclusion des violations de données à caractère personnel et des infractions au RGPD dans la liste des modifications susceptibles d'avoir une incidence sur la certification. Toutefois, dans un souci de clarté, le comité encourage l'autorité de contrôle irlandaise à préciser que les violations de données ou les infractions au RGPD ne seront prises en considération que dans la mesure où elles concernent la certification.

19. En ce qui concerne les modifications ayant une incidence sur la certification (sous-section 7.10 du projet d'exigences de l'autorité de contrôle irlandaise) et, en particulier, le cinquième point, le comité note que l'autorité de contrôle irlandaise fait référence aux «décisions contraignantes applicables du comité européen de la protection des données» ainsi qu'à l'article 39 du règlement intérieur du comité, qui inclut «tous les documents finaux adoptés par le comité». 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 irlandaise à préciser la référence. Elle pourrait, par exemple, faire référence aux «documents adoptés par le comité européen de la protection des données».

20. Le comité observe que la sous-section 7.11 du projet d'exigences de l'autorité de contrôle irlandaise (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 de l'autorité de contrôle irlandaise de retirer ou de ne pas délivrer la certification à un demandeur si les exigences de certification ne sont pas ou plus remplies. Par conséquent, le comité recommande à l'autorité de contrôle irlandaise d'inclure une telle obligation.

3 CONCLUSIONS/RECOMMANDATIONS

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

22. En ce qui concerne les «exigences relatives au processus», le comité recommande à l'autorité de contrôle irlandaise:

1) d'inclure, à la sous-section 7.11, l'obligation pour l'organisme de certification d'accepter les décisions et les ordres qui émanent de l'autorité de contrôle irlandaise de retirer ou de ne pas délivrer une certification à un demandeur si les exigences en matière d'agrément cessent d'être respectées.

4 OBSERVATIONS FINALES

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

24. Conformément à l'article 64, paragraphes 7 et 8, du RGPD, l'autorité de contrôle irlandaise fait savoir à la présidente 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.

25. L'autorité de contrôle irlandaise communique 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)