Avis 5/2020 sur le projet de décision de l'autorité de contrôle compétente luxembourgeoise 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 29 janvier 2020

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'article 51, paragraphe 1, point 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 en matière de protection des données dans le domaine répressif»),

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 du cadre exposé à l'annexe de ses lignes directrices relatives à l'agrément des organismes de certification, et secondement en les analysant à l'aide de son modèle de comparaison (conformément à la norme ISO IEC 17065/2012 et auxdites lignes directrices).

(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

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

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 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. L'autorité de contrôle luxembourgeoise a présenté au comité son projet d'exigences en matière d'agrément au titre de l'article 43, paragraphe 1, point a), du RGPD. Ce projet a été publié le 25 octobre 2019, à la suite d'une décision indiquant que le dossier était jugé complet. L'autorité de contrôle luxembourgeoise procédera à l'agrément des organismes de certification à certifier sur la base des critères de certification du RGPD.

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] Point 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 d'exigences en matière d'agrément présenté

Le présent avis vise à évaluer les exigences en matière d'agrément qu'une autorité de contrôle a définies, soit pour compléter la norme ISO IEC 17065/2012, soit à titre d'ensemble complet d'exigences, afin de permettre à un organisme national d'accréditation ou à une autorité de contrôle, conformément à l'article 43, paragraphe 1, du RGPD, d'agréer un organisme de certification chargé de délivrer et de renouveler les certifications en vertu de 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 constate que, en vertu du droit national, l'autorité de contrôle luxembourgeoise est investie de l'agrément des organismes de certification. À cette fin, ladite autorité a formulé un ensemble d'exigences destinées spécialement à l'agrément des organismes de certification, parallèlement à une liste de critères de certification qui doivent encore être officiellement approuvés.

L'évaluation des exigences en matière d'agrément vise à examiner les différences (ajouts et suppressions) par rapport aux lignes directrices, et notamment à leur annexe. Par ailleurs, le comité se focalise, dans son avis, sur tous les aspects susceptibles d'avoir une incidence sur une approche cohérente concernant l'agrément des organismes de certification.

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.

Le comité a réalisé son évaluation conformément au cadre prévu à l'annexe 1 des lignes directrices. Lorsque le présent avis reste muet au sujet d'une certaine section figurant dans le projet d'exigences en matière d'agrément présenté par l'autorité de contrôle luxembourgeoise, 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. Le comité fait observer que l'autorité de contrôle luxembourgeoise a fourni des informations pour faciliter l'évaluation du projet d'exigences en matière d'agrément. Cependant, l'avis du comité a pour seul objet ledit projet d'exigences.

Le présent avis ne porte en outre pas sur les points présentés par l'autorité de contrôle luxembourgeoise 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

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

b. Indépendance de l'organisme de certification.

c. Conflits d'intérêts de l'organisme de certification.

d. Expertise de l'organisme de certification.

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

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

g. Traitement transparent des réclamations relatives aux violations de la certification.

3. 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 qui est 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 d'elle-même procéder à l'agrément des organismes de certification;

d. l'article 64, paragraphe 1, point c), du RGPD prévoit que le comité émet un avis chaque fois qu'une autorité de contrôle envisage d'approuver les exigences relatives à l'agrément d'un organisme de certification au titre de l'article 43, paragraphe 3, du RGPD,

le comité est de l'avis exposé ci-après.

2.2.1 REMARQUES GÉNÉRALES

4. Le comité constate que le projet d'exigences en matière d'agrément n'est pas parfaitement conforme au cadre exposé à l'annexe 1 des lignes directrices. Par exemple, les sections concernant le «champ d'application» et les «termes et définitions» sont absentes. À cet égard, le comité constate que certains termes, tels que «client» et «demandeur», ne sont pas utilisés de manière cohérente tout au long du document. Pour éviter toute confusion, les termes employés devraient, si possible, correspondre à ceux qui sont définis dans les lignes directrices et leur annexe et utilisés avec cohérence. Par conséquent, en vue de faciliter l'évaluation, le comité encourage l'autorité de contrôle luxembourgeoise à suivre le cadre de l'annexe 1 (des lignes directrices) dans le projet d'exigences en matière d'agrément et à ajouter les sections manquantes.

5. Le comité observe que, tout au long du document, il est à plusieurs reprises fait mention des exigences du «présent mécanisme de certification» (par exemple, à l'exigence 4.6.4) ou des organismes de certification agréés «au titre [...] du mécanisme de certification» (par exemple, à l'exigence 2.2.2). Les références au mécanisme de certification semblent être un problème rédactionnel. Le comité encourage donc l'autorité de contrôle luxembourgeoise à reformuler les références afin de laisser transparaître le fait que les organismes de certification sont agréés conformément aux exigences que l'autorité de contrôle a approuvées.

6. Parallèlement, l'expression «exigences énoncées dans le présent mécanisme de certification», employée partout dans le document (par exemple, à l'exigence 1.1.1.2), prête à confusion. Il pourrait être plus approprié d'indiquer «les critères énoncés dans le mécanisme de certification». Le comité

encourage donc l'autorité de contrôle luxembourgeoise à lever l'ambiguïté de toutes les références au «mécanisme de certification» dans l'ensemble du document.

7. Il observe que plusieurs exigences (par exemple, 3.2.1.1 et 4.1.2) font mention des «normes internationales applicables», de la «norme applicable» ou de la «norme indiquée». Ces normes ne sont cependant définies nulle part, et il est par conséquent difficile de savoir de quelles normes il est question. Le comité recommande dès lors à l'autorité de contrôle luxembourgeoise de préciser ce que ces normes désignent, par exemple dans la section «champ d'application» ou «termes et définitions».

2.2.2 EXIGENCES GÉNÉRALES EN MATIÈRE D'AGRÉMENT

8. Le comité constate que l'exigence 1.1.1.1 de l'autorité de contrôle luxembourgeoise fait référence à une norme (ISAE 3000) qu'il n'a pas évaluée. Il recommande par conséquent à l'autorité de contrôle luxembourgeoise de préciser qu'aucune norme externe, telle que l'ISAE 3000, ne saurait prévaloir sur les exigences.

9. Le comité constate que les exigences prévues à la section 1.6 ne comprennent pas l'obligation pour l'organisme de certification de publier toutes les versions des critères approuvés et toutes les procédures de certification et de les rendre aisément accessibles au public, conformément à l'annexe des lignes directrices (section 4.6). Il fait observer que, si l'autorité de contrôle luxembourgeoise est la propriétaire du programme de certification, il considère toutefois que l'ajout d'une indication appropriée serait utile afin de garantir que les critères sont à jour et facilement accessibles par l'intermédiaire de l'organisme de certification lui-même. À cet égard, le comité estime que, en fournissant un accès aux informations uniquement sur demande, comme établi à l'exigence 1.6.1, l'autorité de contrôle luxembourgeoise fixe une exigence plus stricte que celle visée dans l'annexe des lignes directrices, conformément à laquelle les informations doivent être rendues aisément accessibles au public. Il recommande par conséquent à l'autorité de contrôle luxembourgeoise de modifier cette exigence afin d'inclure l'obligation pour l'organisme de certification de rendre toutes les versions des critères approuvés et toutes les procédures de certification aisément accessibles au public, conformément à l'annexe des lignes directrices.

10. Le comité constate que l'exigence 1.2.4 fait référence au «traitement certifié». Il estime qu'une formulation plus claire, telle que «opérations/activités de traitement certifiées», pourrait être utilisée, conformément aux lignes directrices, ce qui permettrait de respecter le champ d'application plus large des certifications prévu par le RGPD. Le comité recommande par conséquent à l'autorité de contrôle luxembourgeoise de modifier le projet d'exigences en conséquence.

2.2.3 EXIGENCES EN MATIÈRE DE RESSOURCES

11. Le comité constate que l'exigence 3.1.1.2 semble redondante et ambiguë, d'autant plus que la terminologie varie. Par exemple, l'énoncé du troisième paragraphe porte à croire que l'associé responsable prend, à sa seule discrétion, la décision quant au caractère approprié. Le comité recommande à l'autorité de contrôle luxembourgeoise de reformuler afin de rendre cette exigence plus claire et plus compréhensible, et ce, en utilisant une terminologie uniforme.

2.2.4 EXIGENCES RELATIVES AU PROCESSUS

12. Le comité constate que l'exigence 4.2.1 comporte plusieurs exemples d'informations nécessaires. Les deux premiers exemples fournis devraient néanmoins constituer une exigence à eux seuls, conformément à la section 7.2 de l'annexe 1 des lignes directrices. Le comité recommande par conséquent à l'autorité de contrôle luxembourgeoise de modifier le libellé et d'inclure les exemples susmentionnés à titre d'exigences.

13. Concernant la section 4.4 («Évaluation») des exigences en matière d'agrément formulées par l'autorité de contrôle luxembourgeoise, le comité estime que ces exigences devraient comprendre l'obligation pour l'organisme de certification de veiller à ce que des méthodes d'évaluation soient en place et à ce que ces méthodes, décrites dans le mécanisme de certification, soient normalisées et applicables de manière générale. Ainsi, l'utilisation de méthodes d'évaluation similaires serait garantie pour des cibles d'évaluation comparables. L'organisme de certification devrait justifier tout écart par rapport à ces méthodes d'évaluation. Le comité recommande dès lors à l'autorité de contrôle luxembourgeoise de modifier le projet afin d'inclure l'obligation susvisée pour l'organisme de certification.

14. Par ailleurs, le comité constate que, conformément à l'exigence 4.4.2, l'organisme de certification peut faire appel à des experts externes dans certains domaines, en dépit de l'interdiction d'externalisation. À cet égard, il y a lieu de préciser que l'organisme de certification demeurera responsable de la prise de décisions, même s'il fait appel à des experts externes. Le comité recommande par conséquent à l'autorité de contrôle luxembourgeoise de modifier le libellé de l'exigence 4.4.2 en conséquence.

15. Le comité observe que la section 4.7 des exigences en matière d'agrément formulées par l'autorité de contrôle luxembourgeoise («Documentation de la certification») n'aborde pas l'exigence visée à l'annexe relative à la documentation de la période de surveillance (section 7.9). Il encourage par conséquent l'autorité de contrôle luxembourgeoise à préciser la période de contrôle au sens de la section 7.9 relative à la surveillance.

16. S'agissant de la section 4.8 («Répertoire des activités de traitement certifiées») des exigences en matière d'agrément formulées par l'autorité de contrôle luxembourgeoise, l'exigence 4.8.1 dispose que les informations seront fournies au public «sur demande». Le comité estime que, par la fourniture proactive d'un accès aux informations, l'organisme de certification pourrait davantage respecter l'obligation de transparence énoncée à la section 7.8 de l'annexe 1 des lignes directrices. Il recommande dès lors à l'autorité de contrôle luxembourgeoise de modifier le projet afin de prévoir que l'organisme de certification rendra les informations visées à la section 7.8 de l'annexe 1 des lignes directrices accessibles au public.

17. Le comité constate que la section 4.8 comporte une rubrique consacrée à la surveillance, mais ne contient aucune exigence. Il recommande à l'autorité de contrôle luxembourgeoise de préciser la manière dont la surveillance sera assurée.

18. En ce qui concerne la résiliation, la réduction, la suspension ou le retrait d'une certification (sous-section 4.10), le comité constate qu'il n'est fait nulle mention de l'obligation pour l'organisme de certification d'accepter les décisions et les ordres de retirer ou de ne pas délivrer une certification à un client (demandeur) qui émanent de l'autorité de contrôle compétente si les exigences en matière d'agrément cessent d'être respectées. Cette obligation est énoncée à l'article 58, paragraphe 2, point h), du RGPD ainsi qu'à la section 7.11 de l'annexe 1 des lignes directrices. Le comité recommande par conséquent à l'autorité de contrôle luxembourgeoise de modifier les exigences en matière d'agrément afin d'indiquer les règles relatives au retrait, à la résiliation, à la réduction ou à la suspension de la certification.

19. Le comité constate qu'aucune exigence n'est définie pour la section 9 de l'annexe, laquelle comporte des rubriques générales. Par exemple, le contenu de la sous-section 9.3.4 concernant la suspension

ou le retrait d'un agrément n'est pas abordé. Il s'agit de rubriques importantes qui justifient l'ajout d'exigences ou de références croisées aux sections correspondantes. Le comité encourage l'autorité de contrôle à préciser où les exigences sont définies.

3 CONCLUSIONS/RECOMMANDATIONS

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

21. De manière générale, le comité recommande à l'autorité de contrôle luxembourgeoise:

    1. de préciser le sens du terme «norme», mentionné dans plusieurs exigences (dont les exigences 3.2.1.1 et 4.1.2), par exemple dans la section «champ d'application» ou «termes et définitions».

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

    1. de préciser qu'aucune norme externe, telle que l'ISAE 3000, ne saurait prévaloir sur les exigences;

    2. de modifier les exigences prévues à la section 1.6 afin d'inclure l'obligation pour l'organisme de certification de publier et de rendre toutes les versions des critères approuvés et toutes les procédures de certification aisément accessibles au public, conformément à l'annexe des lignes directrices.

23. En ce qui concerne les «exigences en matière de ressources», le comité recommande à l'autorité de contrôle luxembourgeoise:

    1. de reformuler l'exigence 3.1.1.2 afin de la rendre plus claire et plus compréhensible, et ce, en utilisant une terminologie uniforme.

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

    1. de modifier la section 4.4 du projet d'exigences afin d'inclure l'obligation pour l'organisme de certification de veiller à ce que des méthodes d'évaluation soient en place et que ces méthodes, décrites dans le mécanisme de certification, soient normalisées et applicables de manière générale. L'organisme de certification devrait justifier tout écart par rapport aux méthodes d'évaluation;

    2. de modifier le libellé de l'exigence 4.4.2 afin de rendre explicite le fait que l'organisme de certification demeurera responsable de la prise de décisions, même s'il fait appel à des experts externes;

    3. de modifier la section 4.8 de son projet d'exigences en matière d'agrément afin de prévoir que l'organisme de certification rendra les informations visées à la section 7.8 de l'annexe 1 des lignes directrices accessibles au public;

    4. de préciser, à la section 4.8, la manière dont la surveillance sera assurée;

5. de modifier la sous-section 4.10 afin d'indiquer les règles relatives au retrait, à la résiliation, à la réduction ou à la suspension de la certification.

4 OBSERVATIONS FINALES

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

26. Conformément à l'article 64, paragraphes 7 et 8, du RGPD, l'autorité de contrôle 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.

Pour le comité européen de la protection des données

La présidente

(Andrea Jelinek)