Avis 16/2020 sur le projet de décision de l'autorité de contrôle compétente de la République tchèque 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 certification en application 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 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 du cadre exposé à l'annexe de ses lignes directrices 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 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 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, par «Union», on entend 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, lus conjointement 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 tchèque a présenté au comité son projet d'exigences en matière d'agrément au titre de l'article 43, paragraphe 1, point b). Le dossier a été jugé complet le 17 février 2020. L'organisme national d'accréditation tchèque procédera à l'agrément des organismes de certification en utilisant les critères d'agrément du RGPD. En d'autres termes, il utilisera la norme ISO 17065 et les exigences supplémentaires établies par l'autorité de contrôle tchèque dès lors que celle-ci les aura 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 l'autorité de contrôle tchèque 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 tchèque 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 exigences en matière d'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 tchèque, 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 tchèque 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 du RGPD 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.

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 tant que telles une exigence en matière d'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 REMARQUES GÉNÉRALES

12. 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 «domaine d'application» et les «termes et définitions» sont absentes. À cet égard, par souci de clarté et pour faciliter l'évaluation des exigences, le comité estime que la numérotation et la structure générale du document pourraient être améliorées. Par conséquent, en vue de faciliter l'évaluation, le comité invite l'autorité de contrôle tchèque à respecter la structure de l'annexe dans son projet d'exigences en matière d'agrément et à ajouter les sections manquantes, et plus particulièrement la définition des termes utilisés dans le document. En outre, le comité constate que le projet d'exigences en matière d'agrément de l'autorité de contrôle tchèque fait plusieurs références à la section correspondante de la norme ISO 17065 ou aux sections correspondantes de l'annexe, sans toutefois préciser ces références. Dès lors, le comité invite l'autorité de contrôle tchèque à indiquer clairement les références aux sections de ladite norme et de l'annexe.

13. Le comité observe que le projet d'exigences en matière d'agrément de l'autorité de contrôle tchèque évoque à plusieurs reprises l'«objet de l'évaluation» (par exemple aux sections 3.2.1.2.1.2.10; 3.2.1.2.6.3.1; 3.2.1.2.8.1.6.3; 3.2.1.2.10.4.1; 3.1.2.10.7.3.1; 3.1.2.10.7.3.2 et 3.2.1.2.10.10.2). Le comité croit comprendre que ce terme est utilisé comme synonyme de la «cible d'évaluation». Cependant, afin d'éviter toute confusion, le comité invite l'autorité de contrôle tchèque à utiliser le terme «cible d'évaluation» de manière systématique.

14. Le comité constate que plusieurs exigences ne sont pas formulées comme une obligation pour l'organisme de certification (3.2.1.2.2 et 3.2.1.2.3, par exemple). Le comité recommande à l'autorité de contrôle tchèque de reformuler les exigences afin d'indiquer clairement qu'elles sont obligatoires, c'est-à-dire de commencer l'exigence par: «L'organisme de certification est tenu de [...]».

2.2.3 EXIGENCES GÉNÉRALES ERELATIVES À L'AGRÉMENT

15. Concernant l'accord de certification (section 3.2.1.2.1.2 du projet d'exigences en matière d'agrément de l'autorité de contrôle tchèque), le comité constate que la sous-section 3.2.1.2.1.2.2 ne fait pas référence aux «questions contractuellement confidentielles», auxquelles l'autorité de contrôle doit également avoir accès. Par conséquent, le comité recommande à l'autorité de contrôle tchèque de modifier le projet en introduisant l'obligation de fournir aussi à l'autorité de contrôle un accès aux questions contractuellement confidentielles.

16. Par rapport à la sous-section 3.2.1.2.1.2.8 du projet d'exigences en matière d'agrément de l'autorité de contrôle tchèque, le comité observe qu'il n'apparaît pas clairement à qui les informations seront divulguées. Dès lors, le comité invite l'autorité de contrôle tchèque à préciser les destinataires

desdites informations. Par ailleurs, les informations visées doivent être «nécessaires à la délivrance de la certification» conformément à la section 4.1.2, point 7, de l'annexe. Le comité recommande à l'autorité de contrôle tchèque de remplacer les termes «informations relatives à la délivrance de la certification» par «informations nécessaires à la délivrance de la certification».

17. Concernant la sous-section 3.2.1.2.1.2.9 du projet d'exigences en matière d'agrément de l'autorité de contrôle tchèque, le type d'informations à communiquer directement au comité n'est pas indiqué clairement. L'article 42, paragraphe 8, du RGPD impose au comité une obligation de consigner dans un registre, entre autres, tous les mécanismes de certification. Dans ce contexte, il est supposé que les autorités de contrôle compétentes transmettront les informations pertinentes au comité, qui les publiera ensuite dans le registre public. Par conséquent, le comité recommande à l'autorité de contrôle tchèque de clarifier la sous-section 3.2.1.2.1.2.9 du projet d'exigences conformément à l'article 42, paragraphe 8, du RGPD.

18. En ce qui concerne la sous-section 3.2.1.2.1.2.12 du projet d'exigences en matière d'agrément de l'autorité de contrôle tchèque, le comité prend note du fait que ladite autorité de a reformulé une partie de l'exigence visée dans l'annexe. L'autorité de contrôle tchèque a toutefois omis une référence à la phrase [le cas échéant]: «il convient également de traiter des conséquences pour le client». Le comité recommande donc à l'autorité de contrôle tchèque d'ajouter la partie manquante de l'exigence susmentionnée.

19. De plus, la sous-section 3.2.1.2.1.2.13 du projet d'exigences en matière d'agrément de l'autorité de contrôle tchèque impose l'obligation de «contenir un engagement du demandeur consistant à informer l'organisme de certification de tout changement susceptible de porter préjudice à la conformité de l'objet certifié avec les critères de certification». Le comité considère que cette formulation est trop générique et recommande à l'autorité de contrôle tchèque de modifier le projet d'exigences afin d'inclure «tout changement concernant sa situation réelle, sa situation juridique ou ses produits, procédés et services concernés par la certification».

20. En ce qui concerne l'utilisation de labels et de marques en matière de de protection des données (section 3.2.1.2.1.3 du projet d'exigences en matière d'agrément de l'autorité de contrôle tchèque), le comité constate que ledit projet établit que l'accord de certification contient des «règles d'utilisation des certificats, des labels et des marques s'ils sont fournis par le propriétaire du système de certification». La même formulation figure dans la sous-section 3.2.1.2.1.2.14. Le comité considère que cette obligation est déjà couverte par le point 4.1.2.2., point I), de la norme ISO 17065 et, par conséquent, doit être intégrée dans chaque système de certification (voir aussi le point 4.1.3 de la norme ISO 17065). Dès lors, par souci de clarté, le comité recommande à l'autorité de contrôle tchèque de supprimer les sections susmentionnées.

21. En ce qui concerne les exigences relatives à la gestion de l'impartialité, selon les informations fournies par l'autorité de contrôle tchèque dans le modèle, la section 4.2.1., point b), et la section 4.2.2 de l'annexe sont suffisamment couvertes par le point 4.2 de la norme ISO 17065. Cependant, le comité estime que ces exigences devraient être reprises explicitement dans le projet d'exigences en matière d'agrément élaboré par les autorités de contrôle conformément à l'annexe. Dès lors, le comité recommande à l'autorité de contrôle tchèque d'inclure les exigences manquantes concernant la gestion de l'impartialité prévues dans l'annexe.

22. En ce qui concerne l'exigence relative à la responsabilité et au financement (section 3.2.1.2.3.1 du projet d'exigences de l'autorité de contrôle tchèque), le comité invite ladite autorité à préciser qu'il convient de s'en assurer régulièrement.

2.2.4 EXIGENCES RELATIVES AUX RESSOURCES

23. En ce qui concerne le personnel de l'organisme de certification (section 3.2.1.2.8.1.6 du projet d'exigences de l'autorité de contrôle tchèque), le comité constate que les exigences relatives aux personnes chargées des évaluations (sous-section 3.2.1.2.8.1.6.3) incluent «*5 ans d'expérience professionnelle et au moins 10 audits réalisés dans le cadre d'une activité de certification dans le même domaine ou dans un domaine similaire [...] ou 5 ans d'expérience professionnelle dans le domaine de la certification des objets par un organisme de certification*». De même, les exigences relatives aux membres du personnel chargés de la prise de décisions (sous-section 3.2.1.2.8.1.6.4) incluent «*au moins 5 ans d'expérience professionnelle et au moins 10 audits réalisés dans le cadre d'une activité de certification dans le même domaine ou dans un domaine similaire*». Le comité estime que les exigences relatives à l'expertise des évaluateurs et des décideurs doivent être adaptées aux différentes tâches qu'ils accomplissent. À cet égard, 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. Dès lors, le comité invite l'autorité de contrôle tchèque à reformuler cette sous-section en tenant compte des différentes exigences substantielles relatives aux connaissances et/ou à l'expérience des évaluateurs et des décideurs.

24. En outre, le comité constate que le point 3.2.1.2.9.1 du projet d'exigences en matière d'agrément de l'autorité de contrôle tchèque établit que les activités de certification ne peuvent pas être sous-traitées. Or, le point suivant autorise le recours à des auditeurs et à des experts externes à des fins d'évaluation, sauf s'il s'agit d'activités de certification. Le comité estime que le projet d'exigences en matière d'agrément devrait préciser ce qui «constitue des activités de certification» ou indiquer clairement que l'organisme de certification demeurera responsable de la prise de décisions même s'il fait appel à des experts externes. Le comité recommande dès lors à l'autorité de contrôle tchèque de modifier le projet en conséquence.

2.2.5 EXIGENCES RELATIVES AUX PROCESSUS

25. Le comité constate que la section 3.2.1.2.10.1.1 du projet d'exigences supplémentaires de l'autorité de contrôle tchèque fait référence à «toutes les exigences supplémentaires relatives à un conflit d'intérêts (7.1, point 1)». Or, ledit projet ne contient pas d'exigences supplémentaires relatives au conflit d'intérêts. Le comité recommande par conséquent à l'autorité de contrôle tchèque de modifier le projet afin d'éviter toute confusion.

26. En ce qui concerne les exigences relatives à la demande, le comité constate que la sous-section 3.2.1.2.10.2.3 du projet d'exigences en matière d'agrément de l'autorité de contrôle tchèque semble sous-entendre que les informations sur les données transférées doivent uniquement être fournies dans la demande lorsqu'il s'agit d'un transfert vers un pays tiers ou une organisation internationale. Le comité souligne cependant que la demande doit toujours contenir une description des données transférées vers d'autres systèmes ou organisations, quelle que soit leur localisation. Le comité recommande par conséquent à l'autorité de contrôle tchèque de modifier le libellé afin d'éviter toute confusion.

27. Le comité constate que l'obligation de déterminer les méthodes d'évaluation contraignantes dans l'accord de certification (section 3.2.1.2.1.2.6 du projet d'exigences en matière d'agrément de l'autorité de contrôle tchèque) ne fait pas référence à la cible d'évaluation, conformément au point 1 de la section 7.3 de l'annexe des lignes directrices. Par souci de clarté, le comité invite l'autorité de contrôle tchèque à introduire une telle référence.

28. En outre, le comité observe que le projet d'exigences en matière d'agrément de l'autorité de contrôle tchèque prévoit la situation dans laquelle il est fait appel à des sous-traitants pour effectuer des opérations de traitement des données, conformément à l'annexe des lignes directrices (section 3.2.1.2.10.2 dudit projet). Le comité invite l'autorité de contrôle tchèque à examiner si une référence aux coresponsables du traitement et à leur organisation spécifique devrait aussi être mentionnée dans ce cas.

29. En ce qui concerne les exigences relatives à l'évaluation (section 3.2.1.2.10.4 du projet d'exigences de l'autorité de contrôle tchèque), le comité constate que les exigences en matière d'agrément de l'autorité de contrôle tchèque ne contiennent pas l'obligation, pour l'organisme de certification, d'exposer en détail dans son mécanisme de certification la façon dont les informations requises au point 7.4.6 de la norme ISO 17065 seront fournies au demandeur à propos des non-conformités d'un mécanisme de certification. Conformément à l'annexe (sous-section 7.4), il convient de définir au moins la nature et le calendrier de telles informations. Le comité recommande par conséquent à l'autorité de contrôle tchèque d'ajouter l'obligation susmentionnée.

30. De plus, la sous-section 3.2.1.2.10.4.2 du projet d'exigences de l'autorité de contrôle tchèque semble limiter les méthodes d'évaluation aux tests, aux audits ou aux inspections. Le comité considère que d'autres méthodes d'évaluation peuvent également être utilisées et, par conséquent, invite l'autorité de contrôle tchèque à modifier le projet de sorte à indiquer clairement que l'énumération n'est pas exhaustive.

31. En ce qui concerne la sous-section 3.2.1.2.10.4.4.1.4 du projet d'exigences en matière d'agrément de l'autorité de contrôle tchèque, le comité considère que les exigences devraient clairement établir que l'organisme de certification est tenu de vérifier la conformité avec les critères et recommande à l'autorité de contrôle tchèque de modifier ledit projet en conséquence.

32. En ce qui concerne les exigences relatives à l'examen (sous-section 3.2.1.2.10.5 du projet d'exigences en matière d'agrément de l'autorité de contrôle tchèque), le comité observe que lesdites exigences ne font pas référence à l'obligation d'élaborer des procédures de délivrance et de retrait des certifications. Le comité recommande à l'autorité de contrôle tchèque de modifier le projet en conséquence.

33. En ce qui concerne les exigences relatives aux documents de certification, le comité constate que la section 3.1.2.10.7.2 du projet d'exigences en matière d'agrément de l'autorité de contrôle tchèque établit que l'organisme de certification doit préciser que la surveillance est une condition de validité de la certification «si la surveillance est requise par un système de certification [...]». Le comité considère que, dans le cas d'une certification au titre du RGPD, les activités de surveillance sont toujours obligatoires et, par conséquent, recommande à l'autorité de contrôle tchèque d'inclure une telle obligation.

34. En ce qui concerne les exigences liées au répertoire de produits certifiés (section 3.2.1.2.10.8 du projet d'exigences en matière d'agrément de l'autorité de contrôle tchèque et point 7.8 de l'annexe), et en particulier l'obligation d'informer l'autorité de contrôle compétente des raisons de la délivrance ou

du retrait de la certification demandée, le comité constate que ledit projet renvoie à la section 3.2.1.2.10.4.5. Or, ladite section porte sur l'obligation selon laquelle la documentation d'évaluation doit être mise à la disposition de l'autorité de contrôle tchèque à sa demande, tandis que l'exigence de la section 7.8 de l'annexe des lignes directrices contient une obligation de communiquer à l'autorité de contrôle de manière proactive les raisons de la délivrance ou du retrait de la certification. Le comité recommande dès lors à l'autorité de contrôle tchèque de modifier le projet en conséquence.

35. En ce qui concerne les changements qui ont une incidence sur la certification, le comité constate que le projet d'exigences en matière d'agrément de l'autorité de contrôle tchèque ne mentionne pas, parmi les procédures à convenir, le processus d'approbation avec l'autorité de contrôle compétente cité dans l'annexe des lignes directrices (page 19). Le comité reconnaît que la liste fournie à la section 7.10 de l'annexe n'est pas obligatoire. Cependant, par souci de cohérence, le comité invite l'autorité de contrôle tchèque à ajouter une référence au processus d'approbation avec l'autorité de contrôle.

36. Le comité observe que le projet d'exigences en matière d'agrément de l'autorité de contrôle tchèque n'inclut pas clairement l'obligation pour l'organisme de certification d'accepter les décisions et les ordres émanant de l'autorité de contrôle compétente 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. Le comité recommande à l'autorité de contrôle tchèque d'inclure clairement une telle obligation dans le projet d'exigences en matière d'agrément. En ce qui concerne la résiliation, la réduction, la suspension ou le retrait de la certification, le comité constate que les sections 3.2.1.2.10.10.2 et 3.2.1.2.10.10.3 du projet d'exigences font référence à une «instigation». Si l'objectif est de renvoyer aux «décisions et ordres» émanant de l'autorité de contrôle, conformément à l'article 58, paragraphe 2, point h), du RGPD, le comité invite l'autorité de contrôle tchèque à utiliser la même terminologie que celle du RGPD en faisant référence aux «décisions et ordres».

2.2.6 SYSTÈME DE GESTION

37. Le comité considère que la section 3.2.1.2.11 du projet d'exigences supplémentaires de l'autorité de contrôle tchèque ne contient pas l'obligation, pour l'organisme de certification, de «rendre public, de façon permanente et continue, quelles sont les certifications qui ont été effectuées et sur quelle base et quelle est leur durée de validité dans quel cadre et dans quelles conditions», conformément à la section 8 de l'annexe. Le comité recommande par conséquent à l'autorité de contrôle tchèque de modifier le projet d'exigences en introduisant la référence susmentionnée.

3 CONCLUSIONS/RECOMMANDATIONS

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

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

    1) d'introduire l'obligation de fournir à l'autorité de contrôle un accès aux «questions contractuellement confidentielles» dans la section 3.2.1.2.1.2;

2) de remplacer les termes «informations relatives à la délivrance de la certification» par «informations nécessaires à la délivrance de la certification» dans la sous-section 3.2.1.2.1.2.8;

3) de clarifier la sous-section 3.2.1.2.1.2.9 conformément à l'article 42, paragraphe 8, du RGPD;

4) d'ajouter, dans la sous-section 3.2.1.2.1.2.12, une référence à la phrase [le cas échéant]: «il convient également de traiter des conséquences pour le client»;

5) de modifier la sous-section 3.2.1.2.1.2.13 pour inclure «tout changement concernant sa situation réelle, sa situation juridique ou ses produits, procédés et services concernés par la certification»;

6) de supprimer la section 3.2.1.2.1.3 et la sous-section 3.2.1.2.1.2.14;

7) d'inclure les exigences manquantes concernant la gestion de l'impartialité prévues dans l'annexe.

40. En ce qui concerne les «exigences relatives aux ressources», le comité recommande à l'autorité de contrôle tchèque:

1) de modifier la section 3.2.1.2.9.1 pour préciser ce qui «constitue des activités de certification» ou indiquer clairement que l'organisme de certification demeurera responsable de la prise de décisions même s'il fait appel à des experts externes.

41. En ce qui concerne les «exigences relatives aux processus», le comité recommande à l'autorité de contrôle tchèque:

1) d'inclure, dans la section 3.2.1.2.10.4, l'obligation, pour l'organisme de certification, d'exposer en détail dans son mécanisme de certification la façon dont les informations requises au point 7.4.6 de la norme ISO 17065 seront fournies au demandeur à propos des non-conformités d'un mécanisme de certification;

2) de modifier la section 3.2.1.2.10.5 pour faire référence à l'obligation d'élaborer des procédures de délivrance et de retrait des certifications;

3) de modifier la section 3.1.2.10.7.2 pour indiquer que dans le cas d'une certification au titre du RGPD, les activités de surveillance sont toujours obligatoires;

4) de modifier la section 3.1.2.10.8 pour refléter l'obligation pour l'organisme de certification de communiquer à l'autorité de contrôle de manière proactive les raisons de la délivrance ou du retrait de la certification;

5) d'inclure l'obligation pour l'organisme de certification d'accepter les décisions et les ordres émanant de l'autorité de contrôle compétente 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.

42. En ce qui concerne le «système de gestion», le comité recommande à l'autorité de contrôle tchèque:

1) d'inclure l'obligation pour l'organisme de certification de «rendre public, de façon permanente et continue, quelles sont les certifications qui ont été effectuées et sur quelle

base et quelle est leur durée de validité dans quel cadre et dans quelles conditions», conformément à la section 8 de l'annexe.

4 OBSERVATIONS FINALES

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

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

45. L'autorité de contrôle tchèque 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)