Avis 17/2021 sur le projet de décision de l'autorité de contrôle française concernant le code de conduite européen soumis par les prestataires de services d'infrastructure en nuage (CISPE)

Adopté le 19 mai 2021

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

Table des matières

1 RÉSUMÉ DES FAITS 4

2 ÉVALUATION 4

2.1 Le code de conduite répond aux besoins du secteur 4

2.1.1 Présentation du secteur 4

2.1.2 Le propriétaire du code en tant qu'organisme représentatif 5

2.1.3 Portée du traitement 6

2.1.4 Champ d'application territorial 6

2.2 Le code de conduite facilite l'application effective du RGPD 6

2.2.1 Le code en tant qu'outil pratique 7

2.2.2 Matrice d'exigences 7

2.2.3 Caractère contraignant du code 7

2.2.4 Le code fournit des garanties suffisantes 7

2.2.5 Le code en tant qu'outil de responsabilisation 7

2.3 Le code de conduite propose des mécanismes efficaces pour le contrôle du respect du code 8

2.3.1 Application du code 8

2.3.2 Le contrôle du code 8

2.3.3 Sanctions 9

2.3.4 L'examen du code 9

3 CONCLUSIONS/RECOMMANDATIONS 9

4 REMARQUES FINALES 9

Le comité européen de la protection des données

Vu l'article 63, l'article 64, paragraphe 1, point b), et l'article 40 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 sur l'Espace économique européen (ci-après l'«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.

considérant que:

(1) Les États membres, les autorités de contrôle, le comité européen de la protection des données et la Commission européenne encouragent l'élaboration de codes de conduite (ci-après le «code») destinés à contribuer à la bonne application du RGPD[2].

(2) La principale mission du comité européen de la protection des données (ci-après le «comité») est de garantir l'application cohérente du RGPD lorsqu'une autorité de contrôle (ci-après l'«autorité de contrôle») entend approuver un code de conduite concernant des activités de traitement menées dans plusieurs États membres (ci-après le «code transnational»), conformément à l'article 40, paragraphe 7, du RGPD et aux «lignes directrices 1/2019 du comité relatives aux codes de conduite et aux organismes de suivi au titre du règlement 2016/679» (ci-après les «lignes directrices»).

(3) Le comité salue les efforts consentis par les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants pour élaborer des codes de conduite qui constituent des outils pratiques et potentiellement efficients, afin d'assurer une plus grande cohérence au sein d'un secteur donné et de favoriser le droit au respect de la vie privée et à la protection des données des personnes concernées en renforçant la transparence.

(4) Le présent avis vise à garantir l'application cohérente du RGPD, notamment par les autorités de contrôle, les responsables du traitement et les sous-traitants, ainsi qu'à mettre en évidence les éléments essentiels que doit contenir un code de conduite.

(5) Chaque code de conduite devrait faire l'objet d'un examen individuel en tenant compte des caractéristiques spécifiques du secteur concerné, sans préjudice de l'évaluation de tout autre code de conduite. Le comité rappelle que les codes sont l'occasion d'établir un ensemble de règles qui contribuent à la bonne application du RGPD, d'une manière pratique, transparente et potentiellement efficiente qui tienne compte des spécificités d'un secteur particulier et/ou de ses activités de traitement.

[1] Dans le présent avis, on entend par «États membres» les États membres de l'«Espace économique européen».
[2] Article 40, paragraphe 1, du RGPD

(6) Le comité souligne que les codes de conduite sont des outils de responsabilisation volontaires, et que l'adhésion à un code n'empêche pas les autorités de contrôle de la protection des données d'exercer leur pouvoir et leurs prérogatives en matière d'application des règles.

(7) Le présent code n'est pas un code de conduite destiné aux transferts internationaux de données à caractère personnel, au sens de l'article 46, paragraphe 2, point e), et il ne fournit donc pas de garanties appropriées dans le cadre des transferts de données à caractère personnel vers des pays tiers ou à des organisations internationales dans les conditions visées à l'article 46, paragraphe 2, point e). En effet, le transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale n'a lieu que si les dispositions du chapitre V du RGPD sont respectées.

(8) L'avis du comité est adopté conformément à l'article 64, paragraphe 3, du RGPD, en liaison avec l'article 10, paragraphe 2, du règlement intérieur du comité, dans un délai de huit semaines suivant la date à laquelle le président a décidé que le dossier était complet.

A ADOPTÉ LE PRÉSENT AVIS:

1 RÉSUMÉ DES FAITS

1. Conformément à la procédure de coopération définie dans les lignes directrices relatives aux codes de conduite[3], le code de conduite du CISPE (ci-après le «code CISPE» ou le «code») a été examiné par l'autorité de contrôle française en tant qu'autorité de contrôle compétente (ci-après l'«autorité compétente»).

2. Le code CISPE a été examiné dans le respect des procédures prévues par le comité.

3. L'autorité de contrôle française a présenté son projet de décision concernant le projet de code CISPE, et a demandé l'avis du comité conformément à l'article 64, paragraphe 1, point b), du RGPD, le 29 février 2021. La décision relative au caractère complet du dossier a été rendue le 31 mars 2021.

2 ÉVALUATION

2.1 Le code de conduite répond aux besoins du secteur

2.1.1 Présentation du secteur

4. L'informatique en nuage consiste en un ensemble de technologies et de modèles de services axés sur l'utilisation et la livraison par internet d'applications informatiques, de capacités de traitement et d'espace de stockage et de mémoire.

5. Le code CISPE vise à contribuer à la bonne application du RGPD, en tenant compte des spécificités du secteur de l'informatique en nuage.

6. Le terme «informatique en nuage» recouvre toute une série de modèles de prestations de services très distincts, tels que l'infrastructure en nuage en tant que service («IaaS»), le logiciel en nuage en tant que service («SaaS») et la plateforme en nuage en tant que service («PaaS»). Le terme «IaaS» désigne une situation dans laquelle un prestataire loue une infrastructure technologique, c'est-à-dire

[3] Lignes directrices 1/2019 relatives aux codes de conduite et aux organismes de suivi au titre du règlement 2016/679, adoptées par le comité européen de la protection des données le 4 juin 2019.

des serveurs virtuels à distance que l'utilisateur final peut utiliser conformément à des mécanismes et des dispositions permettant de remplacer les systèmes informatiques de l'entreprise situés dans les locaux de celle-ci et/ou d'utiliser l'infrastructure louée parallèlement aux systèmes de l'entreprise d'une manière simple, efficace et avantageuse. Lorsqu'il fournit un «SaaS», un prestataire fournit, sur le web, divers services d'application qu'il met à la disposition des utilisateurs finaux. Ces services sont souvent destinés à remplacer les applications conventionnelles que les utilisateurs doivent installer sur leurs systèmes locaux; de ce fait, les utilisateurs sont censés, à terme, externaliser leurs données vers le prestataire concerné. Lorsqu'il fournit un «PaaS», le prestataire propose des solutions avancées de développement et d'hébergement d'applications. Ces services s'adressent généralement à des acteurs du marché qui s'en servent pour développer et héberger des solutions basées sur des applications développées en interne, afin de répondre à leurs propres besoins et/ou de fournir des prestations à des tiers.

2.1.2 Le propriétaire du code en tant qu'organisme représentatif

7. Les codes de conduite doivent être soumis pour approbation à l'autorité de contrôle compétente, conformément à l'article 55 du RGPD. Dans le cas des codes transnationaux, lors de l'identification de l'autorité de contrôle compétente, certains facteurs pourraient être pris en compte, par exemple la localisation de la partie la plus dense de l'activité de traitement ou l'emplacement du siège du propriétaire du code[4].

8. Les prestataires de services d'infrastructure d'informatique en nuage (CISPE) sont une association à but non lucratif établie en Belgique.

9. Le propriétaire du code a identifié l'autorité de contrôle française comme l'autorité de contrôle compétente aux fins de l'approbation du code CISPE. Le propriétaire du code a justifié son choix dans le code de conduite en fonction de plusieurs critères, tels que l'établissement de plusieurs membres du CISPE en France, ou la présence en France de dirigeants du CISPE, y compris les sociétés du trésorier et du président.

10. Conformément à l'article 40, paragraphe 2, du RGPD, les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants (propriétaires du code) doivent élaborer un code de conduite. Le propriétaire du code ayant un rôle majeur à jouer pour assurer la cohérence et l'harmonisation des pratiques dans le secteur concerné par le code, il doit démontrer à l'autorité de contrôle compétente qu'il dispose effectivement de la qualité d'organisme représentatif. Ainsi, comme indiqué dans les lignes directrices, le propriétaire du code devrait être capable de comprendre les besoins de ses membres et de définir clairement l'activité de traitement ou le secteur auquel le code doit s'appliquer[5].

11. Le considérant 99 du RGPD préconise de consulter les parties intéressées au cours du processus d'élaboration d'un code de conduite. Le code CISPE a été élaboré dans le cadre d'un processus collaboratif entre les membres du CISPE, qui sont tous des prestataires de services d'infrastructure en nuage (ci-après les «prestataires de services») qui fournissent des services d'infrastructure en nuage à des clients européens. Le CISPE, qui a vocation à représenter les prestataires de services d'infrastructure en nuage, compte parmi ses membres des représentants de prestataires leaders du marché qui fournissent des services dans toute l'Europe et dans de nombreux États membres de l'UE. Toutes les parties intéressées concernées ont été consultées et invitées à approuver le code de conduite du CISPE. Le code fournit ainsi un résumé des consultations avec les parties intéressées.

[4] Voir annexe 2 des lignes directrices.
[5] Voir point 22 des lignes directrices.

12. Le propriétaire du code a démontré dans le projet de code qu'il dispose effectivement de la qualité d'organisme représentatif et qu'il est capable de comprendre les besoins de ses membres.

2.1.3 Portée du traitement

13. Le code CISPE s'applique aux caractéristiques spécifiques du traitement effectué par des prestataires d'IaaS. Il vise à clarifier ce que signifie, dans la pratique, l'application du RGPD aux prestataires d'IaaS, et quelles mesures concrètes seront prises par les prestataires de services pour garantir le respect du RGPD. Les dispositions du code énoncent les principes du RGPD qui doivent être respectés par les prestataires de services, en tant que sous-traitants. Le code ne s'applique donc ni aux services «d'entreprise à consommateur» (B2C), ni aux activités de traitement pour lesquelles le prestataire de services peut agir en tant que responsable du traitement. Toutefois, le code est également important pour les consommateurs, qui bénéficieront de garanties de conformité supplémentaires lorsqu'ils confieront leurs données à caractère personnel à une société faisant appel à un sous-traitant qui adhère au code[6].

2.1.4 Champ d'application territorial

14. Le champ d'application du code CISPE, qui est destiné à s'appliquer dans l'ensemble de l'EEE, est transnational, conformément à l'article 40, paragraphe 7, du RGPD. Le code CISPE identifie toutes les autorités de contrôle de l'Union européenne et de l'Espace économique européen comme des autorités de contrôle concernées.

2.2 Le code de conduite facilite l'application effective du RGPD

15. Les lignes directrices précisent que les codes doivent préciser les modalités d'application pratique du RGPD et refléter exactement la nature de l'activité de traitement ou du secteur. Ils doivent pouvoir présenter des améliorations claires et propres au secteur s'agissant du respect du droit en matière de protection des données. Un code ne doit pas se contenter de réaffirmer ce qui figure dans le RGPD. Il doit plutôt établir des règles concernant la voie à suivre afin d'appliquer le RGPD d'une façon spécifique, pratique et précise[7]. En outre, le code doit fournir des garanties appropriées suffisantes afin d'atténuer les risques en matière de traitement des données et de droits et libertés des personnes[8].

16. Le code CISPE contient des exigences strictes précisant les dispositions du RGPD mentionnées dans la section «Portée du traitement» du présent avis et recensant les bonnes pratiques actuellement suivies par le secteur. Le code CISPE aide les prestataires de services à comprendre clairement quelles sont leurs obligations en application du RGPD; il facilite le respect des meilleures pratiques par les fournisseurs d'IaaS et améliore l'état de la technique en matière de protection des données dans le secteur de l'informatique en nuage.

---

[6] Il convient de noter que l'adhésion d'un sous-traitant au code de conduite n'implique pas la reconnaissance automatique de la conformité du traitement effectué par ce sous-traitant, pas plus qu'il ne dispense le responsable du traitement de l'obligation de garantir la conformité de toutes les opérations de traitement effectuées pour son compte. Dans ce cas particulier, le comité rappelle que le code de conduite ne s'appliquera pas à toutes les opérations de traitement effectuées pour le compte du responsable du traitement, mais uniquement aux éléments de l'article 28 du RGPD ainsi qu'aux articles pertinents qui s'y rapportent. En outre, il convient de rappeler que, dans ce cas, le suivi du code de conduite CISPE repose sur une approche de niveau de service. Ainsi, il est possible que certains éléments des activités de traitement menées par les membres du code ne se conforment pas à celui-ci, mais les membres peuvent indiquer lesquels de leurs services doivent être considérés comme conformes au code.

[7] Points 36 et 37 des lignes directrices.

[8] Point 39 des lignes directrices.

2.2.1 Le code en tant qu'outil pratique

17. Le code vise à clarifier ce que signifie, dans la pratique, l'application du RGPD aux prestataires d'IaaS, et quelles mesures concrètes seront prises par les prestataires de services pour garantir le respect du RGPD. Le code CISPE décrit les droits et les obligations des prestataires de services adhérant au code sur la base de principes clés du RGPD, tels que les limitations de la finalité, les droits des personnes concernées, les transferts, la sécurité, les audits, la responsabilité, etc.

2.2.2 Matrice d'exigences

18. Le code se compose d'un ensemble d'exigences que les prestataires de services doivent mettre en œuvre pour s'y conformer.

19. Les exigences définies dans le code sont univoques, concrètes, réalisables et applicables. Toutes les exigences sont consolidées dans un cadre de contrôle qui garantit la transparence pour tous les membres du code comme pour les personnes concernées, et qui facilite l'application et l'interprétation du code de conduite, ce qui permet la mise en œuvre, le suivi et, si nécessaire, l'audit du code. Le comité se félicite de l'utilisation de ce type d'outil.

2.2.3 Caractère contraignant du code

20. Les dispositions du code qui font usage du présent de l'indicatif ou du verbe «devoir» sont contraignantes. Les dispositions caractérisées par l'emploi des termes «devrai(en)t» ou «peu(ven)t» donnent des exemples de bonnes pratiques et doivent donc être considérées comme des orientations.

2.2.4 Le code fournit des garanties suffisantes

21. Conformément aux lignes directrices[9], un code de conduite doit fournir des garanties suffisantes et être axé de façon appropriée sur les domaines et problèmes de la protection des données propres au secteur spécifique auquel il s'applique («valeur ajoutée»). Le code CISPE fournit des garanties suffisantes, par exemple en adoptant la même terminologie que celle utilisée dans le RGPD et en prévoyant un mécanisme de réclamation pour les personnes concernées. S'agissant de la valeur ajoutée, le code fournit des orientations adaptées au secteur en ce qui concerne, notamment, les mesures de sécurité, les exigences en matière d'audit, les droits des personnes concernées et l'obligation de transparence.

2.2.5 Le code en tant qu'outil de responsabilisation

22. L'objectif du code CISPE est d'aider les prestataires de services à démontrer le respect de l'article 28 du RGPD et de permettre aux clients de vérifier plus facilement, et de manière plus transparente, si les services d'informatique en nuage sont adaptés à leur cas d'utilisation, conformément à l'article 28, paragraphe 1, du RGPD, qui dispose que les responsables du traitement font uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD et garantisse la protection des droits de la personne concernée, et conformément à l'article 28, paragraphe 5, du RGPD, selon lequel l'application, par un sous-traitant, d'un code de conduite approuvé peut servir d'élément pour démontrer l'existence des garanties suffisantes conformément aux paragraphes 1 et 4 de l'article 28 du RGPD.

[9] Voir point 36 des lignes directrices.

2.3 Le code de conduite propose des mécanismes efficaces pour le contrôle du respect du code

23. Conformément à l'article 40, paragraphe 4, du RGPD et aux lignes directrices[10], un code doit être accompagné de la mise en œuvre de mécanismes adaptés afin de garantir que ses règles soient contrôlées de façon appropriée et que des mesures de mise en application efficientes et pertinentes soient instaurées pour en assurer la pleine conformité. Un code doit en particulier déterminer et proposer des structures et procédures prévoyant un contrôle efficace et l'application de sanctions.

2.3.1 Application du code

24. Le code doit prévoir un mécanisme d'adhésion.

25. Un mécanisme d'adhésion effectif doit définir un processus divisé en trois phases qui coïncident avec la «durée de vie» du code de conduite. Au cours de la première phase, le mécanisme doit préciser que les membres du code sont tenus de respecter toutes les exigences du code, et que l'organisme de suivi évaluera l'éligibilité du candidat souhaitant souscrire au code. Dans une deuxième phase, le mécanisme décrira les modalités de ce suivi continu, qui sera réalisé de manière ponctuelle dans une troisième phase[11]. Le code CISPE définit un mécanisme d'adhésion qui satisfait aux trois phases de suivi.

2.3.2 Le contrôle du code

26. Les lignes directrices indiquent qu'un code doit également désigner un organisme approprié qui dispose de mécanismes lui permettant d'assurer un contrôle efficace du respect du code[12]. Conformément à l'article 41, paragraphe 1, du RGPD, l'organisme de suivi désigné par le code doit être agréé par l'autorité de contrôle compétente[13]. Par conséquent, l'autorité de contrôle compétente fera office de point de contact unique avec le propriétaire du code et l'organisme de suivi.

27. Le code CISPE désigne plusieurs organismes de suivi externes conformément à l'article 41 du RGPD. Ces organismes de suivi seront chargés de s'assurer que les membres du code respectent les dispositions du code CISPE et de prendre des mesures, y compris des sanctions, en cas d'infraction aux dispositions du code CISPE. Les décisions prises par ces organismes de suivi dans le cadre de leurs fonctions de contrôle (par exemple concernant l'interprétation des règles du code) ne sont pas soumises à l'approbation d'une autre entité. En effet, ces organismes de suivi doivent exercer leur mission de manière indépendante.

28. Le comité reconnaît que le code CISPE comprend un mécanisme permettant aux organismes de suivi d'exercer leurs fonctions de contrôle comme prévu à l'article 40, paragraphe 4, du RGPD.

29. Enfin, le comité rappelle que le code de conduite ne sera pas opérationnel tant que l'organisme de suivi désigné n'aura pas été agréé[14].

---

[10] Voir point 40 des lignes directrices.
[11] Point 70 des lignes directrices.
[12] Point 40 des lignes directrices.
[13] Conformément au mécanisme de contrôle de la cohérence visé à l'article 63 du RGPD, le comité a adopté, le 28 janvier 2020, l'avis 3/2020 sur le projet de conditions d'agrément de l'autorité française de contrôle de la protection des données pour l'agrément d'un organisme de suivi des codes de conduite conformément à l'article 41 du RGPD. Les organismes de suivi désignés par le propriétaire du code de conduite CISPE devront être agréés par l'autorité de contrôle française et devront donc démontrer qu'ils satisfont aux exigences imposées par l'article 41 du RGPD.
[14] Lorsque plusieurs organismes de suivi sont désignés par le code, l'agrément de l'un d'entre eux suffit à conférer un caractère contraignant au code de conduite.

2.3.3 Sanctions

30. Conformément à l'article 40, paragraphe 4, du RGPD et aux lignes directrices, sans préjudice des missions et des pouvoirs de l'autorité de contrôle compétente, l'organisme de suivi désigné par le propriétaire du code doit prendre, sous réserve de garanties appropriées, des mesures adaptées en cas de violation du code par un responsable du traitement ou un sous-traitant. Ces sanctions vont du blâme non public mais officiel, jusqu'à l'exclusion temporaire ou définitive de l'application du code. L'organisme de suivi s'engage à informer l'autorité de contrôle compétente de toute mesure prise en ce sens.

31. Afin de garantir la transparence à l'égard des membres du code, le code comporte une liste de mesures correctrices qui doivent être appliquées par l'organisme de suivi. À cet effet, le code CISPE définit un cadre d'application qui détermine la sanction appropriée à appliquer par les organismes de suivi.

2.3.4 L'examen du code

32. Conformément à l'article 40, paragraphe 2, du RGPD et aux lignes directrices, le code établit un mécanisme d'examen approprié afin de garantir que le code demeure pertinent au regard des normes juridiques et techniques. En particulier, la section 7.3 du code CISPE dispose que le code fait l'objet d'un examen régulier, afin de tenir compte des changements dans la législation, des évolutions technologiques ou opérationnelles ainsi que des meilleures pratiques, le cas échéant.

3 CONCLUSIONS/RECOMMANDATIONS

33. En conclusion, le comité estime que le projet de code est conforme au RGPD dans la mesure où le code de conduite du CISPE satisfait aux exigences imposées par l'article 40 et l'article 41 du RGPD.

34. Enfin, le comité rappelle également les dispositions visées à l'article 40, paragraphe 5, du RGPD, selon lequel, en cas de modification ou de prorogation du code de conduite du CISPE, l'autorité de contrôle compétente doit soumettre la version modifiée au comité conformément aux procédures définies dans les lignes directrices approuvées par le comité.

4 REMARQUES FINALES

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

36. Conformément à l'article 64, paragraphes 7 et 8, du RGPD, l'autorité compétente française communique au président sa réponse au présent avis dans un délai de deux semaines suivant la réception de l'avis.

37. Conformément à l'article 70, paragraphe 1, point y), du RGPD, l'autorité compétente française communique la décision finale au comité en vue de son inclusion dans le registre des décisions auxquelles le mécanisme de contrôle de la cohérence a été appliqué.

38. Conformément à l'article 40, paragraphe 8, du RGPD, le comité soumet le présent avis à la Commission européenne.

Pour le comité européen de la protection des données

La présidente

(Andrea Jelinek)

Adopté