Avis du comité (article 64)

Avis 5/2021 sur le projet d'arrangement administratif relatif au transfert de données à caractère personnel entre le Haut conseil du commissariat aux comptes (H3C) et la commission de surveillance de la comptabilité des sociétés cotées en bourse (PCAOB)

Adopté le 2 février 2021

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,

vu l'article 63, l'article 64, paragraphes 2 à 8, et l'article 46, paragraphe 3, point b), 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 les lignes directrices 2/2020 du comité européen de la protection des données (ci-après le «CEPD») relatives à l'article 46, paragraphe 2, point a), et à l'article 46, paragraphe 3, point b), du règlement (UE) 2016/679 pour les transferts de données à caractère personnel entre les autorités publiques et les organismes publics de l'Espace économique européen (EEE) et hors EEE, adoptées le 15 décembre 2020,

vu l'accord sur l'EEE, et notamment son annexe XI et son protocole 37, tels que modifiés par la décision nº 154/2018 du Comité mixte de l'EEE du 6 juillet 2018[1],

vu les articles 10 et 22 de son règlement intérieur,

considérant ce qui suit:

(1) Conformément à l'article 46, paragraphe 1, à l'article 46, paragraphe 3, point b), et à l'article 46, paragraphe 4, du RGPD, en l'absence de décision en vertu de l'article 45, paragraphe 3, le responsable du traitement ou le sous-traitant ne peut transférer des données à caractère personnel vers un pays tiers ou à une organisation internationale que s'il a prévu des garanties appropriées et à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives. Sous réserve de l'autorisation de l'autorité de contrôle compétente (ci-après l'«AC compétente»), les garanties appropriées peuvent être fournies, notamment, par des dispositions intégrées dans des arrangements administratifs entre les autorités publiques ou les organismes publics qui prévoient des droits opposables et effectifs pour les personnes concernées.

(2) Compte tenu des caractéristiques spécifiques des arrangements administratifs prévus à l'article 46, paragraphe 3, point b)[2], qui peuvent varier considérablement, il convient d'examiner chaque cas individuellement, sans préjudice de l'évaluation de tout autre arrangement administratif.

(3) En application de l'article 70, paragraphe 1, du RGPD, le CEPD veille à l'application cohérente du RGPD dans l'ensemble de l'Espace économique européen. En vertu de l'article 64, paragraphe 2, le mécanisme de contrôle de la cohérence peut être déclenché par une autorité de contrôle, le président du comité ou la Commission pour toute question d'application générale ou produisant des effets dans plusieurs États membres. Le CEPD émet alors un avis sur la question qui lui est soumise, à condition qu'il n'ait pas déjà émis un avis sur la même question.

(4) Conformément à l'article 64, paragraphe 3, du RGPD, en liaison avec l'article 10, paragraphe 2, du règlement intérieur du CEPD, l'avis du CEPD est adopté dans un délai de huit semaines après que le président a décidé que le dossier était complet. Sur décision du président du CEPD, ce délai peut être prolongé de six semaines en fonction de la complexité de la question.

[1] Dans le présent avis, on entend par «États membres» les «États membres de l'EEE».
[2] Voir également le considérant 108 du RGPD.

(5) En vertu de l'article 65, paragraphe 1, point c), du RGPD, lorsqu'une AC compétente ne suit pas l'avis du CEPD émis en vertu de l'article 64, toute autorité de contrôle concernée ou la Commission peut saisir le CEPD, qui adopte alors une décision contraignante,

A ADOPTÉ L'AVIS SUIVANT:

1 RÉSUMÉ DES FAITS

1. Le Haut Conseil du commissariat aux comptes (H3C) a soumis par lettre officielle adressée à l'autorité de contrôle française (la commission nationale de l'informatique et des libertés) un projet d'arrangement administratif (ci-après l'«AA») visant à définir le cadre des transferts de données à caractère personnel du H3C à la PCAOB conformément à l'article 46, paragraphe 3, point b), du RGPD.

2. Ce projet d'AA a été communiqué à l'autorité de contrôle française le 19 novembre 2020.

3. À la suite de cette transmission, l'autorité de contrôle française a demandé au comité d'émettre un avis en vertu de l'article 64, paragraphe 2, du RGPD. La décision relative au caractère complet du dossier a été prise le 9 décembre 2020.

2 ÉVALUATION

4. L'échange de données à caractère personnel entre le H3C et la PCAOB est nécessaire pour garantir leurs fonctions réglementaires d'audit conformément à la loi Sarbanes-Oxley et à l'article 47 de la directive 2006/43/CE du Parlement européen[3], à savoir aux fins de la supervision des auditeurs, des inspections et des enquêtes de cabinets d'audit enregistrés et de leurs personnes associées relevant de la compétence réglementaire de la PCOAB et du H3C.

5. D'autres autorités d'audit de l'EEE ont également besoin d'échanger des données à caractère personnel avec la PCAOB. Partant, le projet d'AA actuellement soumis au CEPD pour avis pourrait être considéré par d'autres autorités d'audit de l'EEE comme un modèle à suivre lorsqu'elles souhaitent définir le cadre du même type de transferts de données à caractère personnel à la PCAOB dans leurs AA spécifiques, AA qui doivent ensuite être soumis à l'AC compétente pour autorisation. En conséquence, la question produit des effets dans plusieurs États membres au sens de l'article 64, paragraphe 2, du RGPD.

6. Lors de l'évaluation des dispositions figurant dans ce projet d'AA précis, le CEPD a pris en considération un certain nombre d'éléments spécifiques, dont le type de données à caractère personnel couvert par l'AA et les objectifs poursuivis.

7. Le projet d'AA et ses annexes comprennent les garanties exposées ci-après.

Définitions de notions et droits des personnes concernées

8. L'article I de l'AA contient les définitions nécessaires pour établir le champ d'application de l'AA et son application cohérente. Parmi elles figurent certaines définitions de notions et droits clés du cadre

[3] Directive 2006/43/CE du Parlement européen et du Conseil du 17 mai 2006 concernant les contrôles légaux des comptes annuels et des comptes consolidés et modifiant les directives 78/660/CEE et 83/349/CEE du Conseil, et abrogeant la directive 84/253/CEE du Conseil.

juridique européen en matière de protection des données, tels que «données à caractère personnel», «traitement des données à caractère personnel», «violation de données à caractère personnel», «droit d'accès» et «droit à l'effacement».

Principe de limitation des finalités et interdiction de toute utilisation ultérieure

9. L'article III.1 de l'AA dispose que les données à caractère personnel transférées par le H3C à la PCAOB peuvent être traitées par la PCAOB elle-même uniquement pour que celle-ci s'acquitte de ses fonctions réglementaires d'audit conformément à la loi Sarbanes-Oxley aux fins de la supervision des auditeurs, des inspections et des enquêtes des cabinets d'audit enregistrés et de leurs personnes associées relevant de la compétence réglementaire de la PCAOB et du H3C. Conformément au principe de limitation des finalités, les transferts ne peuvent donc avoir lieu que dans le cadre de ces missions et responsabilités. La PCAOB ne pourra pas traiter de données à caractère personnel reçues à toute autre fin que celles prévues dans l'AA.

10. En effet, la PCAOB s'intéresse principalement aux noms et aux informations relatives aux activités professionnelles des personnes qui étaient responsables des missions d'audit sélectionnées ou qui y ont participé au cours d'une inspection ou d'une enquête, ou qui jouent un rôle important dans la gestion et le contrôle de la qualité de l'entreprise. Ces informations seraient utilisées par la PCAOB afin d'évaluer le degré de conformité du cabinet comptable enregistré et de ses personnes associées à la loi Sarbanes-Oxley, aux lois sur les valeurs mobilières relatives à la préparation et à l'émission des rapports d'audit, aux règles de la PCAOB, aux règles de la SEC et aux normes professionnelles pertinentes en ce qui concerne la réalisation d'audits, la publication de rapports d'audit et les questions connexes concernant les émetteurs (définies dans la loi Sarbanes-Oxley).

Principe de qualité et de proportionnalité des données

11. Conformément à l'article III.2 de l'AA, les données à caractère personnel transférées par le H3C doivent être adéquates, pertinentes et non excessives au regard des finalités de leur transfert ou de leur traitement ultérieur.

12. Par ailleurs, chaque partie informera l'autre si elle se rend compte que des informations transmises ou reçues précédemment sont inexactes et/ou doivent être mises à jour. En ce qui concerne les finalités pour lesquelles les données à caractère personnel ont été transférées, les parties apporteront toutes les corrections nécessaires à leurs dossiers respectifs, y compris l'ajout, l'effacement, la limitation du traitement, la correction ou toute autre rectification des données à caractère personnel tel qu'approprié.

Principe de transparence

13. Comme prévu par l'article III.3 de l'AA, le H3C et la PCAOB adresseront aux personnes concernées un avis général en publiant l'AA sur leurs sites web. En plus de l'AA, le H3C fournira des informations relatives au traitement effectué (y compris le transfert), au type d'entités auxquelles les données peuvent être transférées, aux droits dont les personnes concernées disposent en vertu des exigences légales applicables (y compris la manière d'exercer ces droits), ainsi qu'à tout délai ou toute restriction applicable concernant l'exercice de ces droits, et précisant les coordonnées à utiliser pour la soumission d'un litige ou l'introduction d'une réclamation. La PCAOB publiera également sur son site web les informations nécessaires relatives au traitement de données à caractère personnel, y compris les informations susmentionnées, tel que décrit dans l'arrangement. En outre, les personnes

concernées seront avisées individuellement par le H3C selon les modalités définies dans le RGPD. Le H3C notifiera la PCAOB avant de procéder à cette notification.

Principe de conservation des données

14. L'article III.2 de l'AA prévoit que les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, ou pour la durée requise par les lois, règles et règlements applicables. Les parties disposent des procédures de destruction des dossiers appropriées pour toutes les informations reçues en vertu du présent AA.

Mesures de sécurité et de confidentialité

15. L'article III.4 de l'AA prévoit que la PCAOB a fourni des informations (annexe I de l'AA) décrivant ses mesures de sécurité techniques et organisationnelles pour se protéger contre la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel ou l'accès à de telles données. La PCAOB accepte de notifier le H3C de toute modification des mesures de sécurité techniques et organisationnelles qui porterait atteinte au niveau de protection conféré par l'AA aux données à caractère personnel. La PCAOB mettra également à jour les informations contenues dans l'annexe I si des modifications sont apportées. Dans le cas où la PCAOB fournit cette notification au H3C, ce dernier notifie l'autorité française chargée de la protection des données desdites modifications.

16. La PCAOB a également fourni au H3C une description de ses lois/règles applicables en matière de confidentialité et l'a informé des conséquences de toute divulgation non autorisée d'informations privées ou confidentielles, ou de toute suspicion de violation de ces lois et/ou règles.

17. Enfin, si la PCAOB apprend qu'une violation de données à caractère personnel s'est produite, il convient qu'elle en notifie le H3C dans les meilleurs délais et, lorsque c'est possible, 24 heures au plus tard après en avoir pris connaissance. La PCAOB utilise également dès que possible des moyens raisonnables et appropriés pour remédier à la violation et réduire au minimum les effets négatifs potentiels.

Garanties relatives aux droits des personnes concernées

18. L'article III.5 de l'AA prévoit des garanties relatives aux droits des personnes concernées. En particulier, les personnes concernées dont les données à caractère personnel ont été transférées à la PCAOB peuvent exercer leurs droits des personnes concernées tels que définis à l'article I, point j), de l'AA, y compris en demandant que le H3C détermine les données à caractère personnel qui ont été transférées à la PCAOB. Par ailleurs, les personnes concernées peuvent demander directement au H3C de confirmer auprès de la PCAOB que les données à caractère personnel sont complètes, exactes et, le cas échéant, à jour, et que le traitement est conforme aux principes du présent AA. La PCAOB répondra de manière raisonnable et en temps utile à toute demande de ce genre par le H3C concernant les données à caractère personnel transférées par le H3C à la PCAOB. La personne concernée peut également contacter la PCAOB directement.

19. Toute limitation de ces droits doit être prévue par la loi et être nécessaire, et elle est maintenue uniquement aussi longtemps que le motif de la limitation continue d'exister. Ces limitations peuvent être autorisées pour empêcher une atteinte aux fonctions de surveillance ou d'exécution des parties agissant dans l'exercice de l'autorité publique dont ils sont investis, comme pour la supervision ou

l'évaluation de la conformité avec les lois applicables de la partie ou la prévention ou l'investigation d'une suspicion d'infraction; pour atteindre un objectif important d'intérêt public général, tel que reconnu aux États-Unis et en France ou au sein de l'Union européenne, y compris dans l'esprit de réciprocité pour la coopération internationale; ou pour superviser les personnes ou entités réglementées.

Prise de décision automatisée

20. L'article III.5 prévoit que la PCAOB ne prendra pas de décision juridique concernant une personne concernée exclusivement fondée sur le traitement automatisé des données à caractère personnel, y compris un profilage, sans participation humaine.

Catégories spéciales de données à caractère personnel/données sensibles

21. L'article III.6 dispose que certaines catégories spéciales de données à caractère personnel/données sensibles ne sont pas transférées par le H3C à la PCAOB.

Restrictions concernant les transferts ultérieurs

22. Conformément à l'article III.7, la PCAOB partagera uniquement les données à caractère personnel reçues du H3C avec les entités énumérées à l'annexe II de l'AA. Le cas échéant, sauf pour la commission américaine des valeurs et des changes, la PCAOB demandera le consentement écrit préalable du H3C et ne partagera ces informations que si le tiers donne des assurances appropriées qui sont compatibles avec les garanties prévues par l'AA. Lorsqu'elle demande ce consentement écrit préalable, la PCAOB fournit au H3C les éléments nécessaires pour permettre à ce dernier de donner son consentement, en ce qui concerne le type de données à caractère personnel qu'elle entend partager et les raisons et finalités pour lesquelles le partage aurait lieu. Si le H3C ne donne pas son consentement écrit pour le partage dans les dix jours au maximum, la PCAOB consultera le H3C et tiendra compte de toute objection qu'il pourrait soulever. Si la PCAOB décide de partager les données à caractère personnel sans le consentement écrit du H3C, elle notifie à ce dernier son intention et le H3C peut ensuite décider de suspendre le transfert des données à caractère personnel. Cette décision devrait être notifiée à l'autorité française chargée de la protection des données. En outre, à titre exceptionnel, lorsque les garanties appropriées ne peuvent pas être fournies par le tiers, les données à caractère personnel peuvent être partagées avec le tiers avec l'accord du H3C si ce partage est nécessaire pour des motifs importants d'intérêt public, tels que reconnus aux États-Unis et en France ou dans l'Union européenne, ou s'il est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice.

23. En ce qui concerne le partage de données à caractère personnel avec la commission américaine des valeurs et des échanges, la PCAOB obtiendra des assurances appropriées antérieures qui sont conformes aux mesures de protection prévues dans l'AA. En outre, la PCAOB informera périodiquement le H3C de la nature des données à caractère personnel partagées et de la raison pour laquelle elles ont été partagées si la communication de ces informations ne risque pas de compromettre une enquête en cours. Cette limitation concernant les informations relatives à une enquête en cours sera maintenue uniquement aussi longtemps que le motif de la limitation continue d'exister.

24. Enfin, une personne concernée peut demander au H3C certaines informations relatives à ses données à caractère personnel qui ont été transférées par le H3C à la PCAOB. Il incombe au H3C de fournir ces informations conformément aux exigences légales applicables du RGPD et de la loi française sur la protection des données.

Voies de recours

25. L'article III 8 de l'AA prévoit un mécanisme de recours. L'AA prévoit quatre niveaux de recours pour les personnes concernées. Premièrement, tout litige ou réclamation introduit par une personne concernée à propos du traitement de ses données à caractère personnel conformément à l'AA peut être adressé au H3C, à la PCAOB, voire aux deux, le cas échéant. Chaque partie informe l'autre partie de tout litige ou réclamation et fait tout ce qui est en son pouvoir pour régler à l'amiable le litige ou la réclamation en temps utile.

26. La PCAOB informera le H3C des rapports reçus des personnes concernées et consultera le H3C pour y répondre.

27. Deuxièmement, si une ou les parties ne sont pas en mesure de répondre à une préoccupation ou une réclamation d'une personne concernée et que cette préoccupation ou réclamation n'est pas manifestement infondée ou excessive, la personne concernée, la partie ou les parties peuvent faire usage d'un premier niveau de recours à un mécanisme de règlement des différends approprié mené par une personne occupant une fonction indépendante au sein de la PCAOB, le conseiller-auditeur.

28. Troisièmement, la décision rendue au moyen de ce mécanisme de règlement des différends peut être soumise à un deuxième examen indépendant, qui est réalisé par une personne occupant une fonction indépendante distincte, l'examinateur de recours. Les décisions tant du conseiller-auditeur que de l'examinateur de recours sont contraignantes pour la PCAOB. Les mécanismes de règlement des différends sont décrits en détail à l'annexe III de l'AA.

29. Dans des situations où le H3C estime que la PCAOB n'a pas agi conformément aux garanties prévues dans l'AA, il peut suspendre les transferts jusqu'à ce que la question soit réglée de manière satisfaisante et peut en informer la personne concernée.

30. Enfin, en tout état de cause, la personne concernée peut exercer son droit à un recours judiciaire ou administratif (y compris en ce qui concerne les dommages) en vertu de la loi française en matière de protection des données.

Mécanisme de surveillance

31. L'article III.9 de l'AA prévoit un mécanisme de surveillance assurant la mise en œuvre des garanties prévues par l'AA. Ce mécanisme de surveillance consiste en une combinaison de la surveillance interne et de la surveillance externe.

32. En ce qui concerne la surveillance interne, chaque partie réalisera des examens périodiques de ses propres politiques et procédures mettant en œuvre les garanties de l'AA. Sur demande raisonnable de l'autre partie, une partie révisera ses politiques et procédures pour assurer et confirmer que les garanties prévues dans le présent arrangement sont mises en œuvre efficacement et enverra une synthèse de l'examen à l'autre partie.

33. En ce qui concerne l'examen externe, sur demande du H3C de réaliser un examen indépendant de la conformité avec les garanties de l'AA, la PCAOB notifiera le Bureau de supervision interne et d'assurance de la performance («IOPA»), un bureau indépendant de la PCAOB, pour qu'il procède à un examen afin de vérifier et de confirmer que les garanties prévues dans l'examen sont effectivement appliquées. Les détails relatifs au fonctionnement de l'IOPA sont fournis à l'annexe IV de l'AA. L'IOPA fournira une synthèse des résultats de son examen au H3C une fois que le conseil d'administration de la PCAOB approuve la divulgation de la synthèse au H3C.

34. Lorsque le H3C n'a pas reçu les résultats de l'examen et estime que la PCAOB n'a pas agi conformément aux garanties spécifiques en vertu de ses obligations au titre de l'AA, il peut suspendre les transferts à la PCAOB jusqu'à ce que la question soit réglée de manière satisfaisante par cette dernière. Cette suspension devrait être notifiée à l'autorité française chargée de la protection des données.

3 CONCLUSIONS/RECOMMANDATIONS

35. Le CEPD salue les efforts ayant conduit à l'élaboration de cet AA, qui comprend un certain nombre de garanties importantes en matière de protection des données conformes au RGPD ainsi qu'aux garanties prévues dans les lignes directrices 2/2020 du CEPD. Pour que ces garanties permettent de faire en sorte qu'un niveau approprié de protection des données soit maintenu lorsque des données sont transférées vers la PCAOB et compte tenu du caractère particulier de tels accords non contraignants, le CEPD souligne ce qui suit:

- l'AC française contrôlera l'AA et son application pratique – en particulier en ce qui concerne les articles III.7, III.8 et III.9 relatifs aux transferts ultérieurs, aux voies de recours et au mécanisme de surveillance – afin de veiller à ce que les personnes concernées bénéficient de droits effectifs et opposables et de voies de recours appropriées et à ce que le respect de l'AA fasse l'objet d'une surveillance efficace.
- L'AC française n'autorisera cet AA qu'à titre de garde-fou adéquat en matière de protection des données aux fins du transfert transfrontière de données, sous réserve du respect intégral de toutes les dispositions de l'AA par les signataires.
- L'AC française suspendra les flux de données effectués par le H3C conformément à l'autorisation si l'AA n'offre plus de garanties appropriées au sens du RGPD.

4 OBSERVATIONS FINALES

36. Le présent avis sera rendu public conformément à l'article 64, paragraphe 5, point b), du RGPD.

Pour le comité européen de la protection des données

La présidente

(Andrea Jelinek)