Opinion 05/2021 on the draft Administrative Arrangement for the transfer of personal data between the Haut Conseil du Commissariat aux Comptes (H3C) and the Public Company Accounting Oversight Board (PCAOB)

Adopted on 2 February 2021

Table of contents

The European Data Protection Board

Having regard to Article 63, Article 64(2), (3) – (8) and Article 46(3)(b) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to EDPB Guidelines 2/2020 on Articles 46(2)(a) and 46(3)(b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies adopted on 15 December 2020,

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

Having regard to Article 10 and Article 22 of its Rules of Procedure,

Whereas:

(1) With reference to Article 46(1), (3)(b) and 46(4) GDPR, in the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. Subject to authorisation from the competent supervisory authority ("competent SA"), the appropriate safeguards may also be provided for, in particular, by provisions inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

(2) Taking into account the specific characteristics of the administrative arrangements provided for by Article 46(3)(b)[2], which may vary considerably, each case should be addressed individually and is without prejudice to the assessment of any other administrative arrangement.

(3) The EDPB ensures pursuant to Article 70(1) of the GDPR the consistent application of Regulation 2016/679 throughout the European Economic Area. Under Article 64(2), the consistency mechanism may be triggered by a supervisory authority, the EDPB Chair or the Commission for any matter of general application or producing effects in more than one Member State. The EDPB shall issue an opinion on the matter submitted to it provided that it has not already issued an opinion on the same matter.

(4) The opinion of the EDPB shall be adopted pursuant to Article 64(3) GDPR in conjunction with Article 10(2) of the EDPB Rules of Procedure within eight weeks after the Chair has decided that the file is complete. Upon decision of the EDPB Chair, this period may be extended by a further six weeks taking into account the complexity of the subject matter.

(5) Pursuant to Article 65(1)(c) GDPR where a competent SA does not follow the opinion of the EDPB issued under Article 64, any supervisory authority concerned or the Commission may communicate the matter to the EDPB and it shall adopt a binding decision.

[1] References to "Member States" made throughout this opinion should be understood as references to "EEA Member States".

[2] See also recital 108 GDPR

HAS ADOPTED THE FOLLOWING OPINION:

1 SUMMARY OF THE FACTS

1. The Haut Conseil du Commissariat aux Comptes (H3C) has submitted by an official letter addressed to the French Supervisory Authority (Commission Nationale de l'Informatique et des Libertés) a draft Administrative Arrangement (hereinafter draft AA) intended to frame the transfers of personal data from the H3C to the PCAOB in accordance with Article 46(3)(b) GDPR.

2. This draft AA was communicated to the French Supervisory Authority on 19 November 2020.

3. Following the submission, the French Supervisory Authority has requested the Board for an opinion pursuant to Article 64(2) GDPR. The decision on the completeness of the file was taken on 9 December 2020.

2 ASSESSMENT

4. The exchange of personal data between the H3C and the PCAOB is necessary to ensure their audit regulatory functions in accordance with the Sarbanes-Oxley Act and Article 47 of Directive 2006/43/EC of the European Parliament[3], namely for the purposes of auditor oversight, inspections and investigations of registered audit firms and their associated persons subject to the regulatory jurisdiction of the PCAOB and the H3C.

5. Other EEA Audit Authorities similarly face a need to exchange personal data with the PCAOB. Thus, the draft AA currently submitted to the EDPB for an opinion might be considered by other EEA Audit Authorities as a model to follow as they seek to frame the same kind of transfers of personal data to the PCAOB in their specific AAs, AA which in turn must be submitted to the competent SA for authorisation. As a result, the subject matter produces effects in more than one Member States within the meaning of Article 64(2) GDPR.

6. In assessing the provisions contained in this specific AA, the EDPB has taken into account a number of specific elements including the type of personal data subject to the AA and the objectives pursued.

7. The draft AA and its Annexes include the following guarantees:

Definitions of concepts and data subject rights:

8. Article I of the AA contains the relevant definitions necessary to determine the scope of the AA and its consistent application. Among them there are some definitions of key concepts and rights of the European data protection legal framework such as "personal data", "processing of personal data", "personal data breach", "right of access" and "right of erasure".

[3] Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts, amending Council Directives 78/660/EEC and 83/349/EEC and repealing Council Directive 84/253/EEC

Principle of purpose limitation and prohibition of any further use:

9. Article III.1 of the AA provides that personal data transferred by the H3C to the PCAOB may be processed by the PCAOB itself only to fulfil its audit regulatory functions in accordance with the Sarbanes - Oxley Act for the purposes of auditor oversight, inspections and investigations of registered audit firms and their associated persons subject to the regulatory jurisdiction of the PCAOB and the H3C. According to the principle of purpose limitation, the transfers can therefore only take place in the framework of such mandates and responsibilities. The PCAOB will not be allowed to process personal data it receives for any purpose other than as set forth in the AA.

10. Indeed, the PCAOB primarily seeks the names, and information relating to the professional activities, of the individual persons who were responsible for or participated in the audit engagements selected for review during an inspection or an investigation, or who play a significant role in the firm's management and quality control. Such information would be used by the PCAOB in order to assess the degree of compliance of the registered accounting firm and its associated persons with the Sarbanes-Oxley Act, the securities laws relating to the preparation and issuances of audit reports, the rules of the PCAOB, the rules of the SEC and relevant professional standards in connection with its performance of audits, issuances of audit reports and related matters involving issuers (as defined in the Sarbanes-Oxley Act).

Principle of data quality and proportionality:

11. According to Article III.2 of the AA the personal data transferred by the H3C must be accurate, adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

12. In addition, each Party will inform the other if it becomes aware that previously transmitted or received information is inaccurate and/or must be updated. Having regard to the purposes for which the personal data have been transferred, the Parties will make any appropriate corrections to their respective files, which may include supplementing, erasing, restricting the processing of, correcting or otherwise rectifying the personal data as appropriate.

Principle of transparency:

13. As provided by Article III.3 of the AA, a general notice to data subjects will be provided by both the H3C and the PCAOB by publishing the AA itself on their websites. In addition to the AA, H3C will provide Information in relation to the processing carried out, including the transfer, the type of entities to which data may be transferred, the rights available to them under the applicable legal requirements, including how to exercise those rights and information about any applicable delay or restrictions on the exercise of such rights and the contact details for submitting a dispute or claim. The PCAOB also will publish on its website appropriate information relating to its processing of Personal Data, including information noted above, as described in the Agreement. Furthermore, individual notice will be provided to data subjects by the H3C in accordance with the GDPR. The H3C will notify the PCAOB in advance of making such individual notification.

Principle of data retention:

14. Article III.2 of the AA provides that personal data must be retained in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed, or for the time as required by applicable laws, rules

and regulations. The Parties shall have in place appropriate record disposal procedures for all information received pursuant to this AA.

Security and confidentiality measures:

15. Article III.4 of the AA envisages that the PCAOB has provided information (Annex I of the AA) describing its technical and organisational security measures to guard against accidental or unlawful destruction, loss, alteration, disclosure of, or access to the personal data. The PCAOB agrees to notify the H3C of any change to the technical and organisational security measures that would adversely affect the protection level afforded for personal data by the AA. The PCAOB will also update the information in Annex I if such changes are made. In the case that the PCAOB provides such notification to the H3C, the H3C would notify the French Data Protection Authority of such changes.

16. The PCAOB has also provided to the H3C a description of its applicable laws and/or rules relating to confidentiality and the consequences for any unlawful disclosure of non-public or confidential information or suspected violations of these laws and/or rules.

17. Finally, in the case where the PCAOB becomes aware of a personal data breach, it will without undue delay and, where feasible, not later than 24 hours after having become aware that it affects such personal data, notify the breach to the H3C. The PCAOB shall also as soon as possible use reasonable and appropriate means to remedy the breach and minimize the potential adverse effects.

Safeguards relating to data subject rights:

18. Article III.5 of the AA provides for safeguards relating to data subject rights. In particular, data subjects whose personal data has been transferred to the PCAOB can exercise his/her data subject rights as defined in Article I(j) of the AA including by requesting that the H3C identifies any personal data that has been transferred to the PCAOB. In addition, data subjects may request directly to the H3C to confirm with the PCAOB that their personal data is complete, accurate and, if applicable, up-to-date and that the processing is in accordance with the principles in this AA. The PCAOB will address in a reasonable and timely manner any such request from the H3C concerning any Personal Data transferred by the H3C to the PCAOB. The data subject can also contact the PCAOB directly.

19. Any restriction to these rights has to be provided by law and should be necessary and will continue only for as long as the reason for the restriction continues to exist. Such restrictions may be allowed to avoid prejudice or harm to supervisory or enforcement functions of the Parties acting in the exercise of the official authority vested in them, such as for the monitoring or assessment of compliance with the Party's applicable laws or prevention or investigation of suspected offenses; for important objectives of general public interest, as recognized in the United States and in France or in the European Union, including in the spirit of reciprocity of international cooperation; or for the supervision of regulated individuals and entities.

Automated decision making:

20. Article III.5 provides that the PCAOB will not take a legal decision concerning a data subject based solely on automated processing of Personal Data, including Profiling, without human involvement.

Special categories of Personal Data/Sensitive Data:

21. Article III.6 provides that special categories of personal data/sensitive data shall not be transferred by the H3C to the PCAOB.

Restrictions on onward transfers:

22. According to Article III.7 of the AA, the PCAOB will only share Personal Data received from the H3C with those entities identified in Annex II of the AA. In the event of such sharing, except for the U.S. Securities and Exchange Commission, the PCAOB will request the prior written consent of the H3C and will only share such personal data if the third party provides appropriate assurances that are consistent with the safeguards in the AA. When requesting such prior written consent, the PCAOB should provide the elements to the H3C, to allow the latter to provide consent, on the type of personal data that it intends to share and the reasons and purposes for which the sharing would take place. If the H3C does not provide its written consent to such sharing within a maximum of ten days, the PCAOB will consult with the H3C and consider any objections it may have. If the PCAOB decides to share the personal data without the H3C written consent, the PCAOB will notify the H3C of its intention to share and the H3C may then decide whether to suspend the transfer of personal data. This decision should be notified to the French Data Protection Authority. Furthermore, as an exception, where the appropriate assurances cannot be provided by the third party, the personal data may be shared with the third party with the consent of the H3C if sharing the personal data is for important reasons of public interest, as recognized in the United States and in France or in the European Union or if the sharing is necessary for the establishment, exercise or defense of legal claims.

23. Regarding the sharing of personal data with the U.S. Securities and Exchange Commission, the PCAOB will obtain from the former appropriate assurances that are consistent with the safeguards in the AA. In addition, the PCAOB will periodically inform the H3C of the nature of personal data shared and the reason it was shared if providing such information will not risk jeopardizing an ongoing investigation. Such restriction regarding information related to an ongoing investigation will continue only for as long as the reason for the restriction continues to exist.

24. Finally, a data subject may request from the H3C certain information related to his or her personal data that has been transferred by the H3C to the PCAOB. It shall be the responsibility of the H3C to provide such information in accordance with applicable legal requirements in the GDPR and the French Data Protection Act.

Redress:

25. Article III.8 of the AA provides for a redress mechanism. There are four layers of redress provided for the data subject in the AA. First, any dispute or claim brought by a data subject concerning the processing of his or her personal data pursuant to the AA may be made to the H3C, the PCAOB, or both, as may be applicable. Each Party will inform the other Party about any such dispute or claim, and will use its best efforts to amicably settle the dispute or claim in a timely fashion.

26. The PCAOB will inform the H3C of reports it receives from data subjects and will consult with the H3C on a response to the matter.

27. Secondly, if a Party or the Parties is/are not able to resolve a concern or complaint made by a data subject and the data subject's concern or complaint is not manifestly unfounded or excessive, the data subject, the Party or Parties may use a first layer of appropriate dispute resolution mechanism conducted by an independent function within the PCAOB, known as the Hearing Officer.

28. Thirdly, the decision reached through this dispute resolution mechanism may be submitted to a second independent review, which would be conducted by a separate independent function known as the Redress Reviewer. The decisions of both the Hearing Officer and the Redress Reviewer are binding on the PCAOB. These dispute resolution mechanisms are described in detail in Annex III of the AA.

29. In situations where the H3C is of the view that the PCAOB has not acted consistent with the safeguards set out in the AA, the H3C may suspend the transfers until the issue is satisfactorily addressed and may inform the Data Subject thereof.

30. Finally, in any case, the data subject may exercise his or her rights for judicial or administrative remedy (including damages) according to French data protection law.

Oversight mechanism:

31. Article III.9 of the AA provides for an oversight mechanism ensuring the implementation of the safeguards of the AA. This oversight mechanism consists of a combination of internal and external oversight.

32. With regards to the internal oversight, each Party will conduct periodic reviews of its own policies and procedures that implement the safeguards of the AA. Upon reasonable request from the other Party, a Party will review its policies and procedures to ascertain and confirm that the safeguards specified in this Agreement are being implemented effectively and send a summary of the review to the other Party.

33. Regarding the external review, upon request by the H3C to conduct an independent review of the compliance with the safeguards in the AA, the PCAOB will notify the Office of Internal Oversight and Performance Assurance ("IOPA"), which is an independent office of the PCAOB, to perform a review to ascertain and confirm that the safeguards in the AA are being effectively implemented. The details of the functioning of IOPA are provided in Annex IV of the AA. IOPA will provide a summary of the results of its review to the H3C once the PCAOB's governing Board approves the disclosure of the summary to the H3C.

34. Where the H3C has not received the IOPA's results of its review and is of the view that the PCAOB has not acted consistent with the safeguards specific to its obligations under the AA, the H3C may suspend the transfers to the PCAOB until the issue is satisfactorily addressed by the PCAOB. Such suspension must be notified to the French Data Protection Authority.

3 CONCLUSIONS/RECOMMENDATIONS

35. The EDPB welcomes the efforts made for this AA which includes a number of important data protection safeguards that are in line with the GDPR and also with the safeguards laid down in Guidelines 2/2020 of the EDPB. In order to make sure that these safeguards continue to ensure an appropriate level of data protection when data are transferred to the PCAOB, considering the unique nature of such non - binding agreements, the EDPB underlines the following:

- The French SA will monitor the AA and its practical application especially in relation to Articles III.7, 8 and 9 relating to onward transfers, redress and oversight mechanisms to ensure that data subjects are provided with effective and enforceable data subject rights, appropriate redress and that compliance with the AA is effectively supervised.
- The French SA shall only authorise this AA as a suitable data protection safeguard with a view to the cross-border data transfer, conditional to full compliance by the signatories with all the clauses of the AA.
- The French SA will suspend the relevant data flows carried out by the H3C pursuant to the authorisation, if the AA no longer provides for appropriate safeguards in the meaning of the GDPR.

4 FINAL REMARKS

36. This opinion will be made public pursuant to Article 64(5)(b) GDPR.

For the European Data Protection Board

The Chair

(Andrea Jelinek)