Administrative Arrangement



Approval decision of the Data Protection "Agreement between the Dutch Financial Authority, Autoriteit Financiële Markten (AFM), and the Public Company Accounting Oversight Board (PCAOB) in the United States of America on the Transfer of Certain Personal Data"

Having regard to Article 63, Article 64(2)(3)-(8) and Article 46(3)(b) of Regulation 2016/679/EU of the European Parliament and 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 ("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 European Economic Area (EEA) and non-EEA public authorities and bodies adopted on 15 December 2020;

Having regard to the 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 (hereby called PCAOB) adopted by the EDPB on February 2nd 2021;

Having regard to Article 58(3)(i) 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 ("GDPR");

Whereas:

- 1. The Autoriteit Financiële Markt ("hereby called **AFM**") has submitted by an official request addressed to the Autoriteit Persoonsgegevens ("**AP**") on September 28th 2023, a Data Protection Agreement between AFM and the PCAOB on the transfer of certain personal data" ("DPA") intended to frame the transfers of personal data from the AFM to the PCAOB in accordance with Article 46(3)(b) GDPR.
- 2. The EDPB has already issued an Opinion on the same matter under the form of 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) on February 2nd 2021.
- 3. Saving national specificities, the arrangement between the H3C and the PCAOB contains the same guarantees as the one provided by the DPA between the AFM and the PCAOB. The AP must regardless authorise any new agreement. The DPA between the AFM and the PCAOB is in all material the same as the arrangement between the H3C and the PCAOB.
- 4. As in the arrangement between the H3C and the PCAOB, the exchange of personal data between the AFM 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, 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 AFM.
- 5. The DPA and its Annexes include the following guarantees:



Definitions of concepts and data subject rights:

6. Article I of the DPA contains the relevant definitions necessary to determine the scope of the DPA 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".

Principle of purpose limitation and prohibition of any further use:

- 7. Article III.1 of the DPA provides that personal data transferred by the AFM to the PCAOB may be processed by the PCAOB itself only to fulfil its audit regulatory functions in accordance with the Sarbanes Oxley Act, i.e., 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 AFM. 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 DPA.
- 8. Article III.2 of the DPA provides that 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 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:

- 9. According to Article III.2 of the DPA provides that the personal data transferred by the AFM must be accurate, adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.
- 10. 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:

11. As provided by Article III.3 of the DPA, a general notice to data subjects will be provided by both the AFM and the PCAOB by publishing the DPA itself on their websites. In addition to the DPA, AFM 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, including restrictions that apply in the case of cross-border transfers of personal data, and the contact details for submitting a dispute or claim. This notice will be effected by publication of this information by the AFM on its website alonside the DPA. The PCAOB will also publish on its website appropriate information relating to its processing of Personal Data, including information noted above, as described in the DPA. Furthermore, individual notice will be provided to data subjects by the AFM in accordance with the GDPR (articles 14-23) and article 41 of the Dutch Implementation Act. If after consideration os any applicable exemptions to individual notification and in light of discussions with the PCAOB, the AFM concludes that it is required under the GDPR to inform a data subject of the transfer of his/her personal data to the PCAOB, then the AFM will notify the PCAOB in advance of making such individual notification.

Principle of data retention:

12. Article III.2 of the DPA 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 the DPA.

Security and confidentiality measures:

- 13. Article III.4 of the DPA envisages that the PCAOB has provided information (Annex I) describing its technical and organizational security measures deemed adequate by the AFM to guard against accidental or unlawful destruction, loss, alteration, disclosure of, or access to the personal data. The PCAOB agrees to notify the AFM of any change to the technical and organizational security measures that would adversely affect the protection level afforded for personal data by the DPA and to update the information in Annex I in accordance with Article IV, paragraph A.3 of the SOP if such changes are made. 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 AFM, the AFM would notify the Dutch Data Protection Authority (Autoriteit Persoonsgegevens) of such changes.
- 14. The PCAOB has also provided to the AFM 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.
- 15. Where a receiving Party becomes aware of a personal data breach affecting personal data that has been transferred under the DPA, 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 personal data breach to the other Party. The notifying Party shall also, as soon as possible, use reasonable and appropriate means to remedy the personal data breach and minimize the potential adverse effects.

Safeguards relating to data subject rights:

- Article III.5 of the DPA 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(h) of the DPA including by requesting that the AFM identifies any personal data that has been transferred to the PCAOB. In addition, data subjects may request directly to the AFM 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 personal data processing principles in this DPA. The PCAOB will address in a reasonable and timely manner any such request from the AFM concerning any Personal Data transferred by the AFM to the PCAOB. The data subject can also contact the PCAOB directly. Either Party may take appropriate steps, such as charging reasonable fees to cover administrative costs or declining to act on a data subjects' request that is manifestly unfounded and excessive.
- 17. Any restriction to these rights are subject to a Party's legal obligation not to disclose confidential information pursuant to professional secrecy or other legal obligations. Such restrictions may be restricted to prevent 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 the Netherlands or in the European Union, including in the spirit of reciprocity of international cooperation; or for the supervision of regulated individuals and entities. The restriction should be necessary and provided for by law, and will continue only for as long as the reason for the restriction continues to exist.

Automated decision making:

18. 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:

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

Restrictions on onward transfers:

20. According to Article III.7 of the DPA, the PCAOB will only share Personal Data received from the AFM with those entities identified in Annex II, other than the U.S. Securities and Exchange Commission, the PCAOB will request the prior written consent of the AFM and will only share such personal data if the third party provides appropriate assurances that are consistent with the safeguards in the DPA. When requesting such prior written consent, the PCAOB should indicate the type of personal data that it intends to share and the reasons and purposes for which the PCAOB intends to share the personal data. If the AFM does not provide its written consent to such sharing within a reasonable time, not to exceed ten days, the PCAOB will consult with the AFM and consider any objections it may have. If the PCAOB decides to share the personal data without the AFM written consent, the PCAOB will notify the AFM of its intention to share and the AFM may then decide whether to suspend the transfer of personal data, and to the extent that it decides to suspend such transfers, the AFM will



inform accordingly the Dutch Data Protection Authority. Where the appropriate assurances cannot be provided by the third party, the personal data may be shared with the third party in exceptional cases if sharing the personal data is for important reasons of public interest, as recognized in the United States and in the Netherlands or in the European Union, including in the spirit of reciprocity of international cooperation, or if the sharing is necessary for the establishment, exercise or defense of legal claims.

- 21. 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 DPA. In addition, the PCAOB will periodically inform the AFM 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.
- 22. A data subject may request from the AFM certain information related to his or her personal data that has been transferred by the AFM to the PCAOB in the course of cooperation pursuant to the SOP. It shall be the responsibility of the AFM to provide such information to the data subject in accordance with applicable legal requirements in the GDPR and the Dutch GDPR implementation Act. Without prejudice to the previous paragraph, upon receipt of a request from a data subject, the AFM may request from the PCAOB information related to the PCAOB's onward sharing of such personal data in order for the AFM to comply with its disclosure obligations to the data subject under the GDPR and the Dutch GDPR Implementation Act. Upon receipt of such request from the AFM, the PCAOB shall provide to the AFM any information that has been made available to the PCAOB concerning the processing of such personal data by a third party with whom the PCAOB has shared such personal data.

Redress:

- 23. Article III.8 of the DPA provides for a redress mechanism. There are four layers of redress provided for the data subject in the DPA. First, any dispute or claim brought by a data subject concerning the processing of his or her personal data pursuant to the DPA may be made to the AFM, 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.
- 24. The PCAOB will inform the AFM of reports it receives from data subjects on the processing of his/her personal data that was received by the PCAOB from the AFM and will consult with the AFM on a response to the matter.
- 25. Secondly, if a Party or the Parties is/are not able to resolve a concern or complaint made by a data subject regarding the processing of personal data by the PCAOB and the data subject's concern or complaint is not manifestly unfounded or excessive, the Party or Parties may use an appropriate dispute resolution mechanism conducted by an independent function within the PCAOB.
- 26. 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. The decisions of both



reviews are binding on the PCAOB. These dispute resolution mechanisms are described in detail in Annex III of the DPA.

- 27. In situations where the AFM is of the view that the PCAOB has not acted consistent with the safeguards set out in the DPA, the AFM may suspend the transfer of personal data under this agreement until the issue is satisfactorily addressed and may inform the Data Subject thereof. Before suspending such transfers, the AFM will discuss the issue with the PCAOB and the PCAOB will respond without undue delay.
- 28. Finally, in any case, the data subject may exercise his or her rights for judicial or administrative remedy (including damages) according to Dutch law.

Oversight mechanism:

- 29. Article III.9 of the DPA provides for an oversight mechanism ensuring the implementation of the safeguards. This oversight mechanism consists of a combination of internal and external oversight.
- 30. With regards to the internal oversight, each Party will conduct periodic reviews of its own policies and procedures that implement the safeguards of the DPA. Upon reasonable request from the other Party, a Party will review its policies and procedures to ascertain and confirm that the safeguards specified in the DPA are being implemented effectively and send a summary of the review to the other Party.
- 31. Regarding the external review, upon request by the AFM to conduct an independent review of the compliance with the safeguards in the DPA, 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 DPA are being effectively implemented. The details of the functioning of IOPA are provided in Annex IV of the DPA. IOPA will provide a summary of the results of its review to the AFM once the PCAOB's governing Board approves the disclosure of the summary to the AFM.
- 32. Where the AFM 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 DPA, the AFM may suspend the transfers to the PCAOB until the issue is satisfactorily addressed by the PCAOB. Before suspending transfers, the AFM will discuss the issue with the PCAOB and the PCAOB will respond without undue delay. In the event that the AFM suspends the transfer of the Personal Data to the PCAOB, or resumes transfers after such suspension, the AFM shall promptly inform the Dutch Data Protection Authority.

THE AUTORITEIT PERSOONSGEGEVENS DECIDES THE FOLLOWING:

- 33. The AP authorises the DPA under the procedure described under article 64(3) and under article 10.4 of the EDPB Rules of Procedure adopted on October 8th, 2020.
- 34. The AP authorises the DPA for a period until **31 July 2028**, conditional to a valid Commission Implementing Decision (EU) 2022/1297 of 22 July 2022 on the adequacy of the competent authorities of the United States of America pursuant to Directive 2006/43/EC of the European Parliament and of the Council.

- 35. The AP will monitor the DPA 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 DPA is effectively supervised.
- 36. The AP shall only authorise this administrative arrangement 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 DPA, Annexes and SOP.
- 37. The AP will suspend the relevant data flows carried out by the AFM pursuant to the authorisation, if the administrative arrangement (DPA, Annexes and SOP) no longer provides for appropriate safeguards in the meaning of the GDPR.

The Hague, 1 August 2024,

On behalf of the Autoriteit Persoonsgegevens,



Director of Legal Affairs and Legislative Advice

Right to object

Within six weeks after this decision is sent, a notice of objection may be lodged. ¹ This notice must be signed and dated, and include the name and address of the person submitting it, a description of the decision against which the objection is being lodged and the grounds on which it is based. The notice of objection should be addressed to the Autoriteit Persoonsgegevens, Department of International Transfers, PO Box 93374, 2509 AJ The Hague, The Netherlands² or via our web form on the website, see https://www.autoriteitpersoonsgegevens.nl/over-deautoriteit-persoonsgegevens/bezwaar-maken.

Please note that submitting a notice of objection will not automatically suspend the effect of this decision.

¹ The Dutch General Administrative Act applies to this procedure.

² Article 6:7 in conjunction with article 6:8 (1) of the Dutch General Administrative Act.

