

# DATA PROTECTION AGREEMENT BETWEEN THE DUTCH AUTHORITY FOR THE FINANCIAL MARKETS AND THE PUBLIC COMPANY ACCOUNTING OVERSIGHT BOARD ON THE TRANSFER OF CERTAIN PERSONAL DATA

## I. DEFINITIONS

For the purpose of this Agreement:

- (1) **‘personal data’** means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
- (2) **‘processing’** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- (3) **‘restriction of processing’** means the marking of stored personal data with the aim of limiting their processing in the future;
- (4) **‘controller’** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- (5) **‘processor’** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- (6) **‘third party’** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data;
- (7) **‘personal data breach’** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- (8) **‘sensitive data’** are special categories of personal data. Sensitive data is the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation and data relating to offences, criminal convictions or security measures in relation to individuals;
- (9) **‘Statement of Protocol’** (“SOP”) means the document by that name, dated and agreed upon by the Parties to facilitate cooperation and the exchange of information.
- (10) **‘Party’** or **‘Parties’** means the Public Company Accounting Oversight Board and/or the Dutch Authority for the Financial Markets (which is the same meaning as in SOP).

## II. DATA PROCESSING PRINCIPLES<sup>1</sup>

The Parties agree that the transmission of personal data by the AFM to the PCAOB shall be governed by the following provisions:

**1. Purpose limitation:** Personal data transmitted by the AFM to the PCAOB may be processed by the PCAOB itself only for the purposes permitted or required by the Sarbanes Oxley Act of 2002, as amended (the “Sarbanes-Oxley Act”), i.e., for the purposes of oversight, inspections and investigations of registered accounting firms and their associated persons subject to the regulatory jurisdiction of the PCAOB and the AFM. The onward transfer of such data which may be for other purposes is governed by paragraph 7 below.

**2. Data quality and proportionality:** Both parties will endeavor to ensure that it transmits to the other party personal data that is accurate. Each party will inform the other party if it learns that previously transmitted information was inaccurate and/or must be updated. In such case the other party will make any appropriate corrections in its files. The parties acknowledge that the PCAOB primarily seeks the names, and information relating the professional activities, of the individual persons who were responsible for or participated in the audit engagements selected for review during an inspection or who play a significant role in the firm’s management and quality control (the “Auditor Information”).

Such information would be used in order to assess the degree of compliance of the registered accounting firm and its associated persons with the Act, the securities laws relating to the preparation and issuance of audit reports, the rules of the PCAOB, the rules of the SEC and relevant professional standards in connection with its performance of audits, issuance of audit reports and related matters involving issuers (as defined in the Sarbanes Oxley Act).

The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed. The Parties agree that providing the Auditor Information to the PCAOB in the context of the Sarbanes-Oxley Act is considered as adequate, relevant and not excessive in relation to the purposes for which it is transferred and further processed. However, the disclosure of other types of personal data, if requested by the PCAOB, shall be considered by the AFM on a case by case basis.

The personal data must be kept 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 such time as otherwise required by applicable laws, rules or regulations.

**3. Transparency:** The AFM will provide to data subjects information relating to the transfer and further processing of personal data as required by the Dutch Data Protection Act (which is the implementation of the EU Data Protection Directive 95/46 EC) to May 25, 2018 and thereafter as required by *the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the*

---

<sup>1</sup> *The AFM has informed the PCAOB of the AFM’s responsibilities under the Regulation (EU) 2016/679 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 [General Data Protection Regulation] with respect to personal data transmitted by the PCAOB to the AFM.*

*processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).*

The Parties acknowledge that the purpose and use by the PCAOB of the personal data are set forth in the Sarbanes-Oxley Act, as further described in **Appendix I**.

**4. Security and confidentiality:** The Parties acknowledge that in **Appendix II**, the PCAOB has provided information describing technical and organizational security measures deemed adequate by the Parties to guard against accidental or unlawful destruction, loss, alteration, disclosure of, or access to, the personal data.

The PCAOB agrees to update the information in **Appendix II** if changes are made to its technical and organizational security measures that would weaken the protection provided for personal data.

Any person acting under the authority of the data controller, including a processor shall not process the data except at the data controller's request.

The AFM has informed the PCAOB of the AFM's responsibilities under the Dutch Data Protection Act (which is the implementation of the EU Data Protection Directive 95/46 EC) to May 25, 2018 and thereafter as required by the *General Data Protection Regulation* with respect to personal data transmitted by the PCAOB to the AFM.

In the case of a personal data breach, the Party shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify the personal data breach to the other Party.

**5. Rights of access, rectification or deletion:** The Parties acknowledge that the transfer of personal data would occur in the context of the PCAOB's exercise of its official regulatory authority pursuant to the Sarbanes-Oxley Act, and that the rights of data subjects to access personal data held by the PCAOB therefore may be restricted in order to safeguard the PCAOB's ability to monitor, inspect or otherwise exercise its regulatory functions with respect to the audit firms and associated persons under its regulatory jurisdiction. However, a data subject whose personal data has been transferred to the PCAOB may request that the AFM identify any personal data that has been transferred to the PCAOB and request that the AFM confirm with the PCAOB that the data is complete, accurate and, if applicable, up-to-date and the processing is in accordance with the data processing principles in this agreement. If the data turns out to be incomplete, inaccurate or outdated or the processing is not in accordance with the data processing principles in this agreement, the data subject has the right to make a request for rectification, erasure or blocking the data, through the AFM.

**6. Sensitive data:** Sensitive data shall not be transferred by the AFM to the PCAOB except with the consent of the data subject.

**7. Onward transfer:** In the event that the PCAOB intends to transfer any personal data to a Third Party (except the U.S. Securities and Exchange Commission) the PCAOB shall comply with the process set forth in Article IV (7) of the SOP. It shall be the responsibility of the AFM to provide relevant information to the data subject, if required by EU or Dutch law.

**8. Redress:** The Parties acknowledge that the PCAOB has provided information set forth in **Appendix III**, describing the consequences for the unlawful disclosure of non-public or

confidential information. The Parties acknowledge that the AFM has provided information set forth in **Appendix IV**, describing the laws and regulations in the Netherlands relevant to information access and confidentiality.

Any suspected violations of the Sarbanes-Oxley Act or the Board's rules (including its Ethics Code) may be reported to (1) the PCAOB Officer of Internal Oversight and Performance Assurance ("IOPA"); (2) the PCAOB Center for Enforcement Tips, Complaints and other Information, both of which are further described in **Appendix III**, through web site or by telephone, or (3) the U.S. Securities and Exchange Commission.



James R. Doty  
Chairman

Public Company Accounting  
Oversight Board

Dated as of: 10 July 2017



Gerben J. Everts  
Member of the Executive Board

Dutch Authority for the Financial Markets

Dated as of: 10 July 2017