

**Agreement between  
the Commissione Nazionale per le Società e la Borsa in Italy and  
the Public Company Accounting Oversight Board in the United States of  
America on the Transfer of Certain Personal Data**

The Commissione Nazionale per le Società e la Borsa in Italy (CONSOB)

and

the Public Company Accounting Oversight Board (PCAOB),

each a “Party”, together the “Parties”,

acting in good faith, will apply the safeguards specified in this data protection agreement (“Agreement”) relating to the transfer of personal data,

recognizing the importance of the protection of personal data and of having robust regimes in place for the protection of personal data,

having regard to Article 46(3)(b) of 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 processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (“General Data Protection Regulation” or “GDPR”),

having regard to CONSOB’s responsibilities and authority under Legislative Decree n° 58/1998, Legislative Decree n° 39/2010, Regulation (EU) n° 537/2014 of the European Parliament and of the Council of 16 April 2014 on specific requirements regarding statutory audit of public-interest entities and repealing Commission Decision 2005/909/EC, Article 47 of Directive 2006/43/EC of the European Parliament and of the Council of 16 May 2006, amended by Directive 2014/56/EU of 16 April 2014, and the Commission Implementing Decision on the adequacy of the competent authorities of the United States of America pursuant to Article 47 paragraph 3 of Directive 2006/43/EC;

having regard to the PCAOB’s responsibilities and authority under the Sarbanes-Oxley Act of 2002, as amended (the “Sarbanes-Oxley Act”),

having regard to the relevant legal framework for the protection of personal data in the jurisdiction of the Parties and acknowledging the importance of regular dialogue between the Parties,

having regard to the need to process personal data to carry out the public mandate and the exercise of official authority vested in the Parties, and

having regard to the need to ensure efficient international cooperation between the Parties acting in accordance with their mandates as defined by applicable laws,

have reached the following understanding:

## **ARTICLE I- DEFINITIONS**

For purposes of this Agreement:

**(a) “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 his/her physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

**(b) “Processing of Personal Data” (“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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction of processing, erasure or destruction;

**(c) “The Italian Data Protection Authority”** means the Garante per la protezione dei dati personali pursuant to Article 2-*bis* of the Italian Data Protection Act;

**(d) “Sharing of Personal Data”** means the sharing of Personal Data by a receiving Party with a third party in its country consistent with Article VIII of the SOP;

**(e) “Special categories of Personal Data/Sensitive Data”** means data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and data concerning health or sex life or sexual orientation and data relating to criminal convictions and offences or related security measures based on Articles 9(1) and 10 of the GDPR in relation to individuals;

**(f) The “Italian Data Protection Act”** means Legislative Decree n° 196 of June 30, 1996, as subsequently amended;

**(g) “SOP” or “Statement”** means the Statement of Protocol between the PCAOB and CONSOB to facilitate cooperation and the exchange of information;

**(h) “Personal Data Breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;

**(i) “Profiling”** means any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

**(j) “Data Subject Rights”** in this Agreement refers to the following<sup>1</sup>:

- “Right not to be subject to automated decisions, including profiling” means a Data Subject’s right not to be subject to legal decisions being made concerning him or her based solely on automated processing;
- “Right of Access” means a Data Subject’s right to obtain from a Party confirmation as to whether or not Personal Data concerning him or her are being processed, and where that is the case, to access the Personal Data;
- “Right of Erasure” means a Data Subject’s right to have his or her Personal Data erased by a Party where the Personal Data are no longer necessary for the purposes for which they were collected or processed, or where the data have been unlawfully collected or processed;
- “Right of Information” means a Data Subject’s right to receive information on the processing of Personal Data relating to him or her in a concise, transparent, intelligible and easily accessible form;
- “Right of Objection” means a Data Subject’s right to object, on grounds relating to his or her particular situation, at any time to processing of Personal Data concerning him or her by a Party, except in cases where there are compelling legitimate grounds for the processing that override the grounds put forward by the Data Subject or for the establishment, exercise or defence of legal claims;
- “Right of Rectification” means a Data Subject’s right to have the Data Subject’s inaccurate personal data corrected or completed by a Party without undue delay;
- “Right of Restriction of Processing” means a Data Subject’s right to restrict the processing of the Data Subject’s Personal Data where the Personal Data are inaccurate, where the processing is unlawful, where a Party no longer needs the Personal Data for the purposes for which they were collected or where the Personal Data cannot be deleted.

## **ARTICLE II- PURPOSE AND SCOPE OF THE AGREEMENT**

The purpose of this Agreement is to provide appropriate safeguards with respect to Personal Data transferred by CONSOB to the PCAOB pursuant to Article 46(3)(b) of the GDPR and in the course of cooperation pursuant to the SOP. The Parties agree that the transfer of Personal Data by CONSOB to the PCAOB shall be governed by the provisions of this Agreement and are committed to having in place the safeguards described in this Agreement for the Processing of Personal Data in the exercise of their respective regulatory mandates and responsibilities. This Agreement is intended to supplement the SOP between the Parties.

Each Party confirms that it has the authority to act consistently with the terms of this Agreement and that it has no reason to believe that existing applicable legal requirements prevent it from doing so.

This Agreement does not create any legally binding obligations, confer any legally binding rights, nor supersede domestic law. The Parties have implemented, within their respective jurisdictions, the

---

<sup>1</sup> These rights arise from the GDPR (See GDPR Chapter III).

safeguards set out in this Agreement in a manner consistent with applicable legal requirements. Parties provide safeguards to protect Personal Data through a combination of laws, regulations and their own internal policies and procedures.

### **ARTICLE III – DATA PROCESSING PRINCIPLES**

**1. Purpose limitation:** Personal Data transferred by CONSOB to the PCAOB may be processed by the PCAOB itself only to fulfill 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 CONSOB. The onward Sharing, including the purpose for such Sharing, of such data by the PCAOB, will be consistent with the Sarbanes-Oxley Act, and is governed by paragraph 7 below. The PCAOB will not process Personal Data it receives from CONSOB for any purpose other than as set forth in this Agreement.

**2. Data quality and proportionality:** The Personal Data transferred by CONSOB must be accurate and must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed. CONSOB will transfer documents containing personal data to the PCAOB only on request and only if, in its request, the PCAOB states the reasons why it needs to access those documents. Consob will assess such requests, with the understanding that the PCAOB will use the personal data in accordance with Article II and Article III paragraph 1 of this Agreement.

A Party will inform the other Party if it learns that previously transmitted or received information is inaccurate and/or must be updated. In such case, the Parties will make any appropriate corrections to their respective files, having regard to the purposes for which the Personal Data have been transferred, which may include supplementing, erasing, restricting the processing of, correcting or otherwise rectifying the Personal Data as appropriate.

The Parties acknowledge 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 audit 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).

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 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 Agreement.

**3. Transparency:** Both Parties will provide general notice by publishing this Agreement on their websites. CONSOB also will provide to Data Subjects information relating to the transfer and further Processing of

Personal Data. CONSOB will in principle provide general notice to Data Subjects about: (a) how and why it may Process and transfer Personal Data; (b) the type of entities to which such data may be transferred, (c) the rights available to Data Subjects under the applicable legal requirements, including how to exercise those rights; (d) 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 (e) contact details for submitting a dispute or claim. This notice will be effected by publication of this information by CONSOB on its website along with this Agreement. The PCAOB also will publish on its website appropriate information relating to its processing of Personal Data, including information noted above, as described in this Agreement.

Individual notice will be provided to Data Subjects by CONSOB in accordance with the notification requirements and applicable exemptions and restrictions in the GDPR (as set forth in Articles 14 and 23 of the GDPR) and the Italian Data Protection Act. If after consideration of any applicable exemptions to individual notification and in the light of discussions with the PCAOB, CONSOB concludes that it is required under the GDPR to inform a Data Subject of the transfer of his/her Personal Data to the PCAOB, CONSOB will notify the PCAOB in advance of making such individual notification.

**4. Security and confidentiality:** The Parties acknowledge that in **Annex I** the PCAOB has provided information describing its technical and organizational security measures deemed adequate by CONSOB to guard against accidental or unlawful destruction, loss, alteration, disclosure of, or access to, the Personal Data. The PCAOB agrees to notify CONSOB of any change to the technical and organizational security measures that would adversely affect the protection level afforded for Personal Data by this Agreement and will update the information in **Annex I** in accordance with Article VII, paragraph B.3 of the SOP if such changes are made. In the case that the PCAOB provides such notification to CONSOB, CONSOB would notify the Italian Data Protection Authority of such changes.

The PCAOB has provided to CONSOB 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.

In the case where a receiving Party becomes aware of a Personal Data Breach affecting Personal Data that has been transferred under this Agreement, 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.

**5. Data Subject Rights:** A Data Subject whose Personal Data has been transferred to the PCAOB can exercise his/her Data Subject Rights as defined in Article I(j) including by requesting that CONSOB identify any Personal Data that has been transferred to the PCAOB and requesting that CONSOB confirm with the PCAOB that his/her Personal Data is complete, accurate and, if applicable, up-to-date and the Processing is in accordance with the Personal Data Processing principles in this Agreement. A Data Subject may exercise his/her Data Subject Rights by making a request directly to CONSOB.

Contact details for CONSOB:

- by certified email to: consob@pec.consob.it

- by e-mail to: protocollo@consob.it;

- by post to: CONSOB, Commissione nazionale per le società e la borsa, via G.B. Martini n. 3 - 00198 Roma.

The Data Protection Officer for CONSOB can be contacted at CONSOB (e-mail: responsabileprotezionedati@consob.it).

The PCAOB will address in a reasonable and timely manner any such request from CONSOB concerning any Personal Data transferred by CONSOB to the PCAOB. Either Party may take appropriate steps, such as charging reasonable fees to cover administrative costs or declining to act on a Data Subject's request that is manifestly unfounded or excessive.

Should the Data Subject wish to contact the PCAOB, he/she may send an email to: personaldata@pcaobus.org.

Safeguards relating to Data Subject Rights are subject to a Party's legal obligation not to disclose confidential information pursuant to professional secrecy or other legal obligations. These safeguards 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 Italy 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 by law, and will continue only for as long as the reason for the restriction continues to exist.

CONSOB will provide information to the Data Subject on the action taken on a request under Articles 15 to 22 of the GDPR without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of requests. CONSOB will inform the Data Subject of any such extension within one month of receipt of the request. If CONSOB and/or the PCAOB does not take action on the request of the Data Subject, CONSOB will inform the Data Subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with the Italian Data Protection Authority and seeking a judicial remedy or before the complaint mechanism established within the PCAOB. Any dispute or claim brought by a Data Subject concerning the processing of his or her Personal Data pursuant to this Agreement may be made to CONSOB, the PCAOB or both, as applicable and as set out in Section 8.

The PCAOB agrees that it will not take a legal decision concerning a Data Subject based solely on automated processing of Personal Data, including Profiling, without human involvement.

**6. Special categories of Personal Data/Sensitive Data:** Special categories of Personal Data/Sensitive Data, as defined in clause I(e), shall not be transferred by CONSOB to the PCAOB.

**7. Onward Sharing of Personal Data:** The PCAOB will only Share Personal Data received from CONSOB with those entities identified in Article VIII paragraphs C and E.2 of the SOP.<sup>2</sup> In the event that the PCAOB intends to Share any Personal Data with any third party identified in Article VIII paragraphs C and E.2 of the SOP, other than the U.S. Securities and Exchange Commission, the PCAOB shall request the prior written consent of CONSOB and will only Share such Personal Data if the third party provides appropriate assurances that are consistent with the safeguards in this Agreement. 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 Personal Data. If CONSOB does not provide its written consent to such Sharing within a reasonable time, not to exceed ten days, the PCAOB will consult with CONSOB and consider any objections it may have. If the PCAOB decides to Share the Personal Data without CONSOB's written consent, the PCAOB will notify CONSOB of its intention to Share. CONSOB may then decide whether to suspend the transfer of Personal Data and, to the extent that it decides to suspend such transfers, CONSOB will inform accordingly the Italian Data Protection Authority. Where the appropriate assurances referred to above 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 Italy 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.

Before Sharing Personal Data with the U.S. Securities and Exchange Commission, the PCAOB will obtain from the U.S. Securities and Exchange Commission appropriate assurances that are consistent with the safeguards in this Agreement. In addition, the PCAOB will periodically inform CONSOB of the nature of Personal Data Shared and the reason it was Shared if the PCAOB has Shared any Personal Data subject to this Agreement with the U.S. Securities and Exchange Commission, 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.

A Data Subject may request from CONSOB certain information related to his or her Personal Data that has been transferred by CONSOB to the PCAOB in the course of cooperation pursuant to the SOP. It shall be the responsibility of CONSOB to provide such information to the Data Subject in accordance with applicable legal requirements in the GDPR and the Italian Data Protection Act. Without prejudice to the previous paragraph, upon receipt of a request from a Data Subject, CONSOB may request from the PCAOB information related to the PCAOB's onward Sharing of such Personal Data in order for CONSOB to comply with its disclosure obligations to the Data Subject under the GDPR and Italian Data Protection Act. Upon receipt of such a request from CONSOB, the PCAOB shall provide to CONSOB 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.

**8. Redress:** Any dispute or claim brought by a Data Subject concerning the processing of his or her Personal Data pursuant to this Agreement may be made to CONSOB, the PCAOB, or both, as may be

---

<sup>2</sup> Entities with whom the PCAOB is permitted by U.S. law to onward Share confidential information are described in **Annex II.**

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.

Any concerns or complaints regarding the Processing of Personal Data by the PCAOB may be reported directly to the PCAOB Center for Enforcement Tips, Referrals, Complaints and Other Information, specifically through the Tips & Referral Center, where information may be provided through an online form on the web site, or via electronic mail, letter or telephone, or, alternatively may be provided to CONSOB by sending such information to the contact details indicated in paragraph 5. The PCAOB will inform CONSOB of reports it receives from Data Subjects on the Processing of his/her Personal Data that was received by the PCAOB from CONSOB and will consult with CONSOB on a response to the matter.

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 received through the Tips & Referral Center and the Data Subject's concern or complaint is not manifestly unfounded or excessive, a Data Subject, the Party or Parties may use an appropriate dispute resolution mechanism conducted by an independent function within the PCAOB. 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 dispute resolution mechanism and the process for the second review are described in **Annex III** to this Agreement. Under this Agreement, the Data Subject may exercise his or her rights for judicial or administrative remedy (including damages) according to Italian data protection law. In situations where CONSOB is of the view that the PCAOB has not acted consistent with the safeguards set out in this Agreement, CONSOB 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 transfers, CONSOB will discuss the issue with the PCAOB and the PCAOB will respond without undue delay.

**9. Oversight:** Each Party will conduct periodic reviews of its own policies and procedures that implement the safeguards over Personal Data described in the Agreement. 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.

Upon request by CONSOB to conduct an independent review of the compliance with the safeguards in the Agreement, 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 this Agreement are being effectively implemented. IOPA will conduct the review according to the procedures and standards established and used by IOPA to perform its regular mandate, as further described in **Annex IV** to this Agreement. For purposes of its independent review, IOPA will be informed of any dispute or claim brought by a Data Subject concerning the processing of his or her Personal Data pursuant to section 8 of this Article, including PCAOB staff actions taken to implement decisions resulting from a dispute resolution mechanism. IOPA will provide a summary of the results of its review to CONSOB once the PCAOB's governing Board approves the disclosure of the summary to CONSOB.



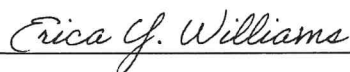
Where CONSOB has not received IOPA's results of its review and is of the view that the PCAOB has not acted consistent with the safeguards specific to its obligations under this Agreement, CONSOB may suspend the transfer of Personal Data to the PCAOB under this Agreement until the issue is satisfactorily addressed by the PCAOB. Before suspending transfers, CONSOB will discuss the issue with the PCAOB and the PCAOB will respond without undue delay. In the event that CONSOB suspends the transfer of Personal Data to the PCAOB, or resumes transfers after any such suspension, CONSOB shall promptly inform the Italian Data Protection Authority.

#### ARTICLE IV- ENTRY INTO EFFECT AND TERMINATION

This Agreement comes into force from the date of signature and shall remain in force only during the period the SOP is also in force. The Parties may consult and revise the terms of this Agreement under the same conditions as set forth in Article X, paragraph B of the SOP.

This Agreement may be terminated by either Party at any time. After termination of this Agreement, the Parties shall continue to maintain as confidential, consistent with Articles VII and VIII of the SOP, any information provided under the SOP. After termination of this Agreement, any Personal Data previously transferred under this Agreement will continue to be handled by the PCAOB according to the safeguards set forth in this Agreement. The Parties acknowledge that, under section 105(b)(5) of the Sarbanes-Oxley Act, termination of this Agreement and the SOP would limit the PCAOB's ability to share confidential information with CONSOB in connection with applying the relevant safeguards set forth in this Agreement.

CONSOB will promptly notify the Italian Data Protection Authority of any amendment or termination of this Agreement.



Erica Y. Williams  
Chair  
Public Company Accounting Oversight Board

Date: 5/30/23



Paolo Savona  
Chairman  
Commissione Nazionale per le Società e la Borsa

Date: 4.6.2023

**Annexes to  
the Agreement between the Commissione Nazionale per le Società e la Borsa in Italy and  
the Public Company Accounting Oversight Board in the United States of America  
on the Transfer of Certain Personal Data**

**Annex I:** PCAOB Description of Information Technology Systems/Controls [CONFIDENTIAL]

**Annex II:** List of Entities with whom the PCAOB is permitted to onward share confidential information

**Annex III:** Description of Applicable Dispute Resolution Processes (Redress)

**Annex IV:** Description of Oversight over PCAOB implementation of DPA safeguard

## Annex II

### List of Entities with whom the PCAOB is permitted to onward share confidential information

The third parties with whom the PCAOB may onward share personal data referenced in Article III, section 7 of the Data Protection Agreement are enumerated in Section 105(b)(5)(B) of the Sarbanes-Oxley Act of 2002, as amended, which states:

(B) Availability to government agencies.— Without the loss of its status as confidential and privileged in the hands of the Board, all information referred to in subparagraph (A) [of Section 105(b)(5)] may—

(i) be made available to the [Securities and Exchange Commission]; and

(ii) in the discretion of the Board, when determined by the Board to be necessary to accomplish the purposes of this Act or to protect investors, be made available to—

(I) the Attorney General of the United States;

(II) the appropriate Federal functional regulator<sup>3</sup> (as defined in section 509 of the Gramm-Leach-Bliley Act (15 U.S.C. 6809)), other than the [Securities and Exchange Commission], and the Director of the Federal Housing Finance Agency, with respect to an audit report for an institution subject to the jurisdiction of such regulator;

(III) State attorneys general in connection with any criminal investigation;

(IV) any appropriate State regulatory authority<sup>4</sup>; and

(V) a self regulatory organization, with respect to an audit report for a broker or dealer that is under the jurisdiction of such self regulatory organization,

each of which shall maintain such information as confidential and privileged.

---

<sup>3</sup> The term ‘Federal functional regulator’ in (B)(ii)(II) above is defined in 15 U.S.C. § 6809 to include:

- the Board of Governors of the Federal Reserve System,
- the Office of the Comptroller of the Currency, the Board of Directors of the Federal Deposit Insurance Corporation,
- the Director of the Office of Thrift Supervision,
- the National Credit Union Administration Board, and
- the Securities and Exchange Commission.

Other than the SEC, these are the various regulators of financial institutions in the United States.

<sup>4</sup> The term ‘State regulatory authorities’ under PCAOB Rule 1001(a)(xi) means “the State agency or other authority responsible for the licensure or other regulation of the practice of accounting in the State or States having jurisdiction over a registered public accounting firm or associated persons thereof....” These would largely be the State Boards of Accountancy in the U.S.

## Annex III

### Description of Applicable Dispute Resolution Processes (Redress)

The PCAOB's redress mechanism referenced in the data protection agreement (DPA) allows a data subject to seek redress of unresolved claims or disputes about the PCAOB's processing of his or her personal data received under the DPA. The redress mechanism includes two levels of review. As described in the DPA, the first level of review will take place in front of an independent function within the PCAOB (the PCAOB Hearing Officer) and the second level of review will take place in front of an independent function contracted by the PCAOB (a hearing officer outsourced from an independent entity).

#### 1. First Level of Redress – PCAOB Hearing Officer

The PCAOB Hearing Officer serves as the independent, impartial reviewer of fact in a formal administrative proceeding requiring an authoritative decision. The PCAOB Hearing Officer is an attorney who is employed by the PCAOB and subject to the PCAOB Ethics Code and the restrictions under Section 105(b)(5) of the Sarbanes-Oxley Act (Act), including with respect to handling of confidential and non-public information, but is independent of all PCAOB Divisions and Offices responsible for requesting and processing personal data in connection with the PCAOB's oversight activities. In exercising his or her duties, the PCAOB Hearing Officer has a responsibility to act with honor and integrity so that all rulings, decisions, conclusions and judgments therein are fair and impartial. These fundamental attributes of necessary and appropriate authority, independence, objectivity, impartiality, and fairness are applicable to the redress mechanism.

The following features of the PCAOB's Office of the Hearing Officer and PCAOB rules are designed to ensure the PCAOB Hearing Officer's independence:

- The PCAOB's Office of the Hearing Officer hires and maintains its own staff, and both the PCAOB Hearing Officer and staff are kept physically separate from other PCAOB staff. The PCAOB is obligated to provide appropriate funding and resources to the PCAOB's Office of the Hearing Officer.
- Board members and PCAOB staff are specifically prohibited from attempting to improperly influence the PCAOB Hearing Officer's decisions (in the litigation of a matter, staff may only provide evidence and arguments on notice and with opportunity for all parties to participate). Breaches of this requirement would subject staff to discipline under the PCAOB Ethics Code.
- A PCAOB Hearing Officer may not be terminated or removed from a case to influence the outcome of a proceeding, and termination of the PCAOB Hearing Officer requires approval of the U.S. Securities and Exchange Commission.
- All decisions about the PCAOB Hearing Officer's performance and compensation may not consider the outcome of proceedings.

The PCAOB Hearing Officer would independently review the merits of a formal complaint as to whether the PCAOB staff complied with the safeguards described in the DPA when processing the data subject's personal data and issue an authoritative decision within a reasonable time.

Under the first level of redress, a data subject would submit a formal complaint to the PCAOB Office of the Hearing Officer describing with specificity the data subject's claims or disputes about the PCAOB's processing of his or her personal data. The PCAOB staff involved in the processing of the data subject's personal data would file a response to the complaint, and the PCAOB counterpart to the DPA may submit a response to describe its involvement with respect to the processing and transfer of the personal data at issue. The data subject would receive a copy of all responses submitted to the PCAOB Hearing Officer, except that any information that is confidential under Section 105(b)(5) of the Act would have to be redacted. The PCAOB Hearing Officer would review the formal complaint and responses and make an authoritative decision on any disputed facts presented as to whether PCAOB staff complied with the safeguards described in the DPA when processing the personal data at issue.

The first level of redress would conclude when the PCAOB Hearing Officer issues a written decision regarding the data subject's complaint. If the PCAOB Hearing Officer concludes the PCAOB staff did not comply with the safeguards in the DPA that are the subject of the complaint, the PCAOB Hearing Officer will order the PCAOB staff to comply with the respective safeguards. The PCAOB Hearing Officer's decision in favor of the data subject is binding on the PCAOB staff, and the PCAOB or its staff may not seek further review of the PCAOB Hearing Officer's decision. All parties involved would receive the results of the administrative proceeding, and the data subject would receive a form of the formal decision prepared in compliance with the confidentiality restrictions under Section 105(b)(5) of the Act. When informed of the PCAOB Hearing Officer's decision, the data subject also will be provided with notice of the second level of redress described below and information about the process for commencing such second level of redress.

## 2. Second Level of Redress – Hearing Officer Outsourced from an Independent Entity

The second level of redress established by the PCAOB will afford a data subject an opportunity to seek a review of the formal decision issued by the PCAOB Hearing Officer. The PCAOB will utilize the services of an independent entity, with whom the PCAOB has contracted for similar services in the past,<sup>5</sup> to provide hearing officer services for the second level of redress. These hearing officers are experienced attorneys, who, while performing services for the PCAOB under the agreement, are subject to PCAOB rules -- including the PCAOB Ethics Code and independence and impartiality measures under PCAOB adjudicatory rules. Pursuant to a contract, upon the PCAOB's request, the independent entity would provide one of its hearing officers to preside independently and impartially over any redress matter. A hearing officer retained to preside over the second level of redress would be designated as a "redress reviewer" and would execute an enforceable non-disclosure agreement with the PCAOB to confirm the retained hearing officer will adhere to the confidentiality restrictions under Section 105(b)(5) of the Act when reviewing confidential information received during the redress proceeding.

To obtain a second level of redress, the data subject must file a petition with the PCAOB's Office of the Secretary no later than 30 days after service of the PCAOB Hearing Officer's decision. The petition shall identify alleged errors or deficiencies in the PCAOB Hearing Officer's decision from the first level of

---

<sup>5</sup> Because the PCAOB has not, to date, employed more than one Hearing Officer, the PCAOB contracted with another regulatory body to obtain access to their hearing officers. When additional hearing officers were needed, their hearing officers have acted as independent consultants/contractors of the PCAOB and presided over certain disciplinary proceedings. The second level of redress would be conducted by one of these hearing officers, or under a similar arrangement.

redress. The PCAOB's Secretary will promptly (within 30 days) issue an order assigning the matter to the independent entity, which will designate a hearing officer to serve as the redress reviewer.

The redress reviewer will receive supporting arguments and any additional supporting documentation from each party involved (including the data subject, PCAOB counterpart to the DPA, and PCAOB staff). As with the first level of redress, the data subject will receive a copy of all responses submitted to the redress reviewer, except that any information that is confidential under Section 105(b)(5) of the Act would be redacted.

Based on the parties' submissions and the underlying record, the redress reviewer shall consider whether the PCAOB's Hearing Officer's findings and conclusions were arbitrary and capricious, or otherwise not in accordance with the DPA. At the conclusion of the review and within a reasonable time, the redress reviewer shall issue a written decision addressing the data subject's challenges to the underlying decision. If the decision concludes that the PCAOB staff did not comply with the safeguards in the DPA, the redress reviewer will order the PCAOB staff to comply with the respective safeguards. The redress reviewer's decision shall serve as the final determination in the matter.

## Annex IV

### Oversight over PCAOB implementation of DPA safeguards

Under the DPA, independent oversight over the PCAOB's compliance with the safeguards provided in the DPA is provided by the PCAOB's Office of Internal Oversight and Performance Assurance ("IOPA" or the "Office").<sup>6</sup>

IOPA is an independent office within the PCAOB that is charged with "providing internal examination of the programs and operations of the PCAOB to help ensure the internal efficiency, integrity, and effectiveness of those programs and operations. The assurance provided by the Office is intended to promote the confidence of the public, the Securities and Exchange Commission, and Congress in the integrity of PCAOB programs and operations."<sup>7</sup>

To achieve its mission, among other actions, IOPA must identify risks to the efficiency, integrity, and effectiveness of PCAOB programs and operations, and, based on its risk assessment, conduct performance and quality assurance reviews, audits, and inquiries to detect and deter waste, fraud, abuse, and mismanagement in PCAOB programs and operations; and recommend constructive actions that, when implemented, reduce or eliminate identified risks, and promote compliance with applicable laws, regulations, and PCAOB rules and policies.

IOPA's activities include, among others:

- Providing ongoing quality assurance with regard to the design and operating effectiveness of PCAOB programs;
- Conducting inquiries relating to PCAOB programs and operations; and
- Receiving and reviewing allegations of wrongdoing lodged against PCAOB personnel as well as tips and complaints of potential waste, fraud, abuse, or mismanagement in PCAOB programs or operations.

In order to carry out its work, pursuant to the IOPA Charter, the Director and staff of IOPA must "be free, both in fact and appearance, from personal, external, and organizational impairments to independence." In order to promote such independence, unlike other PCAOB employees (who generally report to a single individual at the PCAOB), the Director reports directly to all five members of the PCAOB Board. Under the IOPA Charter, the "[e]valuation of the Director's performance and the setting of his/her compensation shall be based on the Director's management of the Office, effective execution of the Office's work, ... and shall not be based on the nature of the results from the Office's reviews, audits, and inquiries." In addition, IOPA's independence is promoted by the fact that the Director's term in office is limited to a single five-year term, and IOPA itself is subject to a regular external quality assurance review. IOPA also may report to the PCAOB's General Counsel, including the Ethics Officer, regarding its work, including the results of inquiries into tips, complaints, and/or allegations of professional or ethical misconduct. Finally,

---

<sup>6</sup> DPA Sec. 9 states that, upon request from the PCAOB's counterpart to the DPA to conduct an independent review of the compliance with the safeguards in the DPA, the PCAOB will notify IOPA to perform a review to ascertain and confirm that the safeguards in the DPA are being effectively implemented.

<sup>7</sup> See [IOPA Charter](#), which is available on the PCAOB website.

IOPA has guaranteed unrestricted access to all personnel and records, reports, audits, reviews, documents, papers, recommendations, or other materials of the PCAOB.

Should IOPA become aware of “particularly serious or flagrant problems, abuses, or deficiencies relating to the administration of PCAOB programs and operations and that warrant immediate ... Board attention,” IOPA must immediately report such information to the PCAOB Board, and such information also must be reported to the SEC within seven calendar days.

In order to conduct its work, IOPA follows accepted standards and requirements. These include the mandatory guidance of the Institute of Internal Auditors, such as the (i) International Standards for the Professional Practice of Internal Auditing, (ii) Core Principles for the Professional Practice of Internal Auditing, (iii) Definition of Internal Auditing, and (iv) Code of Ethics.

With respect to the DPA, IOPA has the ability to conduct a review of the PCAOB’s compliance with relevant data protection safeguards:

- On IOPA’s own initiative, e.g. based on its assessment of risks to the PCAOB’s programs and operations;
- In response to tips, complaints, and/or allegations of professional or ethical misconduct; or
- Upon request of the PCAOB Board (e.g. to comply with the requirement under the DPA that the PCAOB ask for a review by IOPA upon a request).

In order to conduct such a review, as noted above, IOPA has unrestricted access to all PCAOB documentation relating to the relevant PCAOB activities.

In conducting its review, IOPA will follow its standard auditing process, in accordance with the Institute of Internal Auditors’ International Standards, consisting of the following phases.

**Planning** – Determine the audit objectives and appropriate audit criteria. (Audit criteria would be based on the safeguard provisions described in the data protection agreement.) Also, preliminarily assess risk to accomplishing management’s objectives and identify controls in place to mitigate the risks. Determine appropriate audit scope relative to the processes and control procedures to be reviewed and tested. Design substantive compliance tests to be performed to assess the design and operating effectiveness of the stated data protection safeguards.

**Execution** – Following the documented audit program, perform the test work. Test work will generally consist of review of policies and procedures and information system process flow descriptions; interviews with process and control owners; walkthroughs/demonstrations of safeguards and related controls; auditor re-performance of certain safeguards/controls; auditor testing of safeguards/controls based on representative sample selections and review of supporting documentation evidencing control design and operation.

**Quality Review** – IOPA management will supervise on-going work, and review and approve work product generated by the staff. IOPA management will determine the propriety of any audit issues raised and the adequacy of supporting evidence.

**Reporting** – IOPA will draft a report disclosing the results of its review. Recommendations will be made to ameliorate the noted issues. The report will include PCAOB staff’s written response, indicating concurrence with the noted audit observations, corrective actions taken or planned, and target dates for



completion. Reports will be reviewed by the PCAOB Governing Board and will be provided to the PCAOB's counterpart to the DPA after the PCAOB's Governing Board approves the nonpublic disclosure of the report to that counterpart. Board approval addresses only the nonpublic disclosure of IOPA's findings, as required by the PCAOB's Ethics Code, and does not include Board involvement in determining the content of IOPA's report, including the results of the review.

***Follow-Up*** – At the appropriate time, IOPA will follow-up on PCAOB staff's corrective actions to verify that they have been satisfactorily completed.