Agreement between

the Haut Conseil du Commissariat aux Comptes in France and

the Public Company Accounting Oversight Board in the United States of America on the Transfer of Certain Personal Data

The Haut Conseil du Commissariat aux Comptes (H3C)

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) 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 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 and 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,

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, location data, an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity;

(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 French Data Protection Authority" means the Commission Nationale de l'Informatique et des Libertés (CNIL);

(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 IV paragraph 6 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 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 **"French Data Protection Act"** means the amended Act n°78-17 of 6 January 1978 on information technology, data files and civil liberties;

(g) "SOP" or "Statement" means the Statement of Protocol between the PCAOB and the H3C 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[1]:

- "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;

[1] These rights arise from the GDPR (See GDPR Chapter III).

- "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 the H3C 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 the H3C 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 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.

WD

ARTICLE III – DATA PROCESSING PRINCIPLES

1. Purpose limitation: Personal Data transferred by the H3C 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 the H3C. 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 the H3C for any purpose other than as set forth in this Agreement.

2. Data quality and proportionality: The Personal Data transferred by the H3C must be accurate and must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed. 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 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).

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. The H3C also will provide to Data Subjects information relating to the transfer and further Processing of Personal Data. The H3C 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 the H3C 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 the H3C 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). If after consideration of any applicable exemptions to individual notification and in the light of discussions with the PCAOB, the H3C concludes that it is required under the GDPR to inform a Data Subject of the transfer of his/her Personal Data to the PCAOB, the H3C 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 the H3C 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 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 IV, paragraph 3 of the SOP 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.

The PCAOB has 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.

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 the H3C identify any Personal Data that has been transferred to the PCAOB and requesting that the H3C 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 the H3C:

Contact details for the H3C:

- by e-mail to **dpd@h3c.org**;

- by post to:
Haut conseil du commissariat aux comptes - Délégué à la protection des données
104 avenue du Président Kennedy - 75016 Paris (France)

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. 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 France 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.

The H3C 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. The H3C will inform the Data Subject of any such extension within one month of receipt of the request. If the H3C and/or the PCAOB does not take action on the request of the Data Subject, the H3C 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 French 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 the H3C, 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 the H3C to the PCAOB.

7. Onward Sharing of Personal Data: The PCAOB will only Share Personal Data received from the H3C with those entities identified in Article IV paragraph 6 of the SOP.[2] In the event that the PCAOB intends to Share any Personal Data with any third party identified in Article IV paragraph 6 of the SOP, other than 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 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 the H3C does not provide its written consent to such Sharing within a reasonable time, not to exceed 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

[2] Entities with whom the PCAOB is permitted by U.S. law to onward Share confidential information are described in Annex II.

written consent, the PCAOB will notify the H3C of its intention to Share. The H3C may then decide whether to suspend the transfer of Personal Data and, to the extent that it decides to suspend such transfers, the H3C will inform accordingly the French 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 France 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 the H3C 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 the H3C certain information related to his or her Personal Data that has been transferred by the H3C to the PCAOB in the course of cooperation pursuant to the SOP. It shall be the responsibility of the H3C to provide such information to the Data Subject in accordance with applicable legal requirements in the GDPR and the French Data Protection Act. Without prejudice to the previous paragraph, upon receipt of a request from a Data Subject, the H3C may request from the PCAOB information related to the PCAOB's onward Sharing of such Personal Data in order for the H3C to comply with its disclosure obligations to the Data Subject under the GDPR and French Data Protection Act. Upon receipt of such a request from the H3C, the PCAOB shall provide to the H3C 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 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.

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 the H3C by sending such information to dpd@h3c.org. The PCAOB will inform the H3C of reports it receives from Data Subjects on the Processing of his/her Personal Data that was received by the PCAOB from the H3C and will consult with the H3C 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 French data protection law. In situations where the H3C is of the view that the PCAOB has not acted consistent with the safeguards set out in this Agreement, the H3C 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, the H3C 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 the H3C 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 the H3C once the PCAOB's governing Board approves the disclosure of the summary to the H3C.

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 this Agreement, the H3C 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, the H3C will discuss the issue with the PCAOB and the PCAOB will respond without undue delay. In the event that the H3C suspends the transfer of Personal Data to the PCAOB, or resumes transfers after any such suspension, the H3C shall promptly inform the French 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 VI, paragraphs 2 and 3 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 Article IV 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 the H3C in connection with applying the relevant safeguards set forth in this Agreement.

The H3C will promptly notify the French Data Protection Authority of any amendment or termination of this Agreement.

ARTICLE V- OTHER

This Agreement shall be drawn up in English and in French, both texts being equally authoritative.

William D. Duhnke III
Chairman
Public Company Accounting Oversight Board

Date: 07 April, 2021

Florence Peybernes
Chair of the Board
Haut Conseil du Commissariat aux Comptes

Date: 7 April, 2021

Annexes to
the Agreement between the Haut Conseil du Commissariat aux Comptes in France 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[7] (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[8]; 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.

---

[7] 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.

[8] 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,[9] 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 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.

[9] 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.

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").[10]

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."[11]

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,

[10] 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.

[11] See IOPA Charter.

WD

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

K - WD

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.

Accord entre

le Haut Conseil du Commissariat aux Comptes en France et

le Public Company Accounting Oversight Board aux Etats-Unis d'Amérique sur le transfert de certaines données à caractère personnel

Le Haut Conseil du Commissariat aux Comptes (H3C)

Et

le Public Company Accounting Oversight Board (PCAOB),

individuellement une « Partie » et collectivement les « Parties »,

agissant de bonne foi, appliqueront les garanties précisées dans le présent accord (l' « Accord ») relatif au transfert de données à caractère personnel,

reconnaissant l'importance de la protection des données à caractère personnel et disposant de solides régimes de protection des données,

vu l'article 46(3) du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (« Règlement Général sur la Protection des Données, ou ci-après le « RGPD »),

vu le règlement (EU) 537/2014 du Parlement européen et du Conseil du 16 avril 2014 relatif aux exigences spécifiques applicables au contrôle légal des comptes des entités d'intérêt public et abrogeant la décision 2005/909/CE de la Commission et l'article 47 de la directive 2006/43/CE du Parlement européen et du Conseil du 17 mai 2006, modifié par la directive 2014/56/EU du 16 avril 2014,

vu les responsabilités et compétences du PCAOB résultant de la loi Sarbanes Oxley de 2002 telle que modifiée (la « Loi Sarbanes-Oxley »),

vu le cadre juridique applicable à la protection des données à caractère personnel dans la juridiction des Parties et reconnaissant l'importance d'un dialogue régulier entre les Parties,

vu la nécessité de traiter des données à caractère personnel pour l'exécution de leur mission et l'exercice de l'autorité officielle dont les Parties sont investies, et

vu la nécessité d'assurer une coopération internationale efficace entre les Parties agissant conformément à leurs mandats tels que définis par les lois applicables,

sont convenues de ce qui suit :

ARTICLE I- DÉFINITIONS

Aux fins de l'Accord :

W · WD

(a) « **Données à Caractère Personnel** » désigne toute information se rapportant à une personne physique identifiée ou identifiable **(« Personne Concernée »)**, directement ou indirectement, en particulier par référence à un identifiant tel qu'un nom, des données de localisation, un numéro d'identification ou à un ou plusieurs facteurs spécifiques à son identité physique, physiologique, psychique, économique, culturelle ou sociale ;

(b) « **Traitement des Données à Caractère Personnel** » (« **Traitement** ») désigne toute opération ou tout ensemble d'opérations appliqués à des Données ou des ensembles de Données à Caractère Personnel, effectuées ou non à l'aide de procédés automatisés, tels que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation , l'effacement ou la destruction ;

(c) « **L'Autorité Française de Protection des Données** » désigne la Commission Nationale de l'Informatique et des Libertés (CNIL) ;

(d) « **Partage de Données à Caractère Personnel** » désigne le partage de Données à Caractère Personnel par une partie avec une partie tiers dans son pays conformément à l'Article IV paragraphe 6 du Protocole ;

(e) « **Catégories particulières de Données à Caractère Personnel/Données Sensibles** » désignent les données révélant l'origine raciale ou ethnique, les opinions politiques, convictions religieuses ou philosophiques, l'appartenance syndicale, les données concernant la santé ou la vie sexuelle et les données relatives à des infractions, à des condamnations pénales ou à des mesures de sureté au titre des articles 9(1) et 10 du RGPD relatif aux individus ;

(f) La « **Loi Informatique et Libertés** » désigne la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

(g) « **Protocole** » désigne le Protocole entre le PCAOB et le H3C afin de faciliter la coopération et l'échange des informations ;

(h) « **Violation de Données à Caractère Personnel** » désigne une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de Données à Caractère Personnel transmises, stockées ou traitées ;

(i) « **Profilage** » désigne toute forme de Traitement automatisé de Données à Caractère Personnel consistant à utiliser ces Données à Caractère Personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne ;

(j) « **Droits des Personnes Concernées** » désignent dans le présent Accord ce qui suit[1] :

- le « droit de ne pas faire l'objet de décisions fondées sur un traitement automatisé, y compris le profilage » désigne le droit d'une Personne Concernée de ne pas faire l'objet d'une décision produisant des effets juridiques la concernant, fondée exclusivement sur un traitement automatisé ;

[1] Ces droits découlent du RGPD (voir le chapitre III du RGPD).

- le « droit d'accès » désigne le droit d'une Personne Concernée d'obtenir d'une Partie la confirmation que des Données à Caractère Personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, d'accéder auxdites Données à Caractère Personnel ;

- le « droit à l'effacement » désigne le droit d'une Personne Concernée de voir ses Données à Caractère Personnel effacées par une Partie lorsque les Données à Caractère Personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées ou lorsque les données ont été collectées ou traitées de manière illicite ;

- le « droit à l'information » désigne le droit d'une Personne Concernée de recevoir des informations sur le traitement des Données à Caractère Personnel la concernant sous une forme concise, transparente, compréhensible et aisément accessible ;

- le « droit d'opposition » désigne le droit d'une Personne Concernée de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, au traitement de Données à Caractère Personnel la concernant par une Partie, sauf dans les cas où il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les motifs invoqués par la Personne Concernée, ou pour la constatation, l'exercice ou la défense de droits en justice ;

- le « droit de rectification » désigne le droit d'une Personne Concernée de faire rectifier ou compléter, dans les meilleurs délais, ses Données à caractère Personnel inexactes par une Partie ;

- le « droit à la limitation du traitement » désigne le droit d'une Personne Concernée de limiter le traitement de ses Données à Caractère Personnel lorsque celles-ci sont inexactes, lorsque le traitement est illicite, lorsque la Partie n'a plus besoin des Données à Caractère Personnel aux fins pour lesquelles elles ont été collectées ou lorsque les Données à Caractère Personnel ne peuvent être supprimées.

ARTICLE II - OBJET ET PORTÉE DE L'ACCORD

L'objet du présent Accord est de prévoir des garanties appropriées régissant les Données à Caractère Personnel transmises par le H3C au PCAOB en application de l'article 46(3)(b) du RGPD dans le cadre de la coopération prévue par le Protocole. Les Parties conviennent que la transmission des Données à Caractère Personnel par le H3C au PCAOB est régie par les dispositions de l'Accord et s'engagent à mettre en place les garanties prévues dans le présent Accord pour le Traitement des Données à Caractère Personnel lors de l'exercice de leurs fonctions de régulateur et responsabilités respectives. Le présent Accord est destiné à compléter le Protocole entre les Parties.

Chaque Partie reconnaît qu'elle dispose du pouvoir d'agir conformément aux dispositions du présent Accord et qu'elle n'a aucune raison de croire que des dispositions de la réglementation applicable y font obstacle.

Le présent Accord ne crée aucune obligation juridiquement contraignante, ne confère aucun droit juridiquement contraignant, et ne se substitue pas au droit national. Les Parties ont mis en œuvre, dans leurs pays respectifs, les garanties énoncées dans le présent Accord d'une manière compatible avec les exigences légales applicables. Les Parties fournissent des garanties pour protéger les Données à Caractère Personnel par le biais d'une combinaison de lois, de réglementations et de leurs propres politiques et procédures internes.

ARTICLE III – PRINCIPES DE TRAITEMENT DES DONNÉES

1. Limitation des finalités : Les Données à Caractère Personnel transmises par le H3C au PCAOB ne peuvent être traitées directement par le PCAOB que pour les besoins de ses missions de régulateur de l'audit, conformément à la Loi Sarbanes-Oxley, à savoir la surveillance des auditeurs, les contrôles et les enquêtes relatives aux cabinets d'audit inscrits et aux personnes qui leur sont associées, qui relèvent de la compétence du PCAOB et du H3C. Le Partage ultérieur de ces Données à Caractère Personnel par le PCAOB, y compris la finalité de ce Partage, sera conforme à la Loi Sarbanes-Oxley et est régi par le paragraphe 7 ci-dessous. Le PCAOB ne traitera pas des Données à Caractère Personnel transmises par le H3C à d'autres fins que celles énoncées dans le présent Accord.

2. Qualité et proportionnalité des données : Les Données à Caractère Personnel transférées par le H3C doivent être exactes et adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont transférées puis traitées. Une Partie informera l'autre Partie si elle apprend que les informations précédemment transmises ou reçues sont inexactes et/ou doivent être mises à jour. Dans ce cas, les Parties apporteront toutes les corrections appropriées à leurs fichiers respectifs, en tenant compte des finalités pour lesquelles les Données à Caractère Personnel ont été transférées, ce qui peut impliquer de compléter, effacer, limiter le traitement, corriger ou rectifier d'une autre manière les Données à Caractère Personnel, selon les besoins.

Les Parties reconnaissent que le PCAOB examine principalement les noms et les informations concernant les activités professionnelles des personnes physiques responsables ou ayant participé aux missions d'audit sélectionnées pour revue lors d'un contrôle ou d'une enquête, ou ayant un rôle important dans la gestion du cabinet d'audit ou son contrôle qualité. Ces informations sont susceptibles d'être utilisées par le PCAOB afin d'évaluer le niveau de respect par les cabinets d'audit inscrits et les personnes qui leur sont associées, de la Loi Sarbanes-Oxley, des législations sur les valeurs mobilières relatives à la préparation et à la publication des rapports d'audit, des règlements du PCAOB et de la SEC, et des normes d'exercice professionnel applicables relatives à l'exécution de la mission d'audit, l'émission des rapports d'audit et les questions s'y rapportant concernant les émetteurs (telles que définies par la Loi Sarbanes-Oxley).

Les Données à Caractère Personnel ne doivent pas être conservées sous une forme permettant l'identification des Personnes Concernées pour une durée excédant celle nécessaire aux fins pour lesquelles les données ont été collectées ou pour lesquelles elles sont traitées ultérieurement, ou excédant la durée requise par les lois et règlements applicables. Les Parties mettront en place des procédures appropriées d'élimination des enregistrements pour toutes les informations reçues dans le cadre du présent Accord.

3. Transparence : Les deux Parties fourniront une information générale en publiant le présent Accord sur leurs sites internet. Le H3C communiquera également aux Personnes Concernées des informations relatives au transfert et au traitement ultérieur des Données à Caractère Personnel. Le H3C fournira principalement aux Personnes Concernées une information générale sur les points suivants : (a) la finalité et la façon dont il peut traiter et transférer des Données à Caractère Personnel ; (b) le type d'entités auxquelles ces Données à Caractère Personnel peuvent être transférées, (c) les droits conférés aux Personnes Concernées en application des textes légaux applicables, y compris les modalités d'exercice de ces droits ; (d) les informations sur les délais ou limitations portant sur l'exercice de ces droits, y compris les limitations applicables en cas de transfert transfrontalier de Données à Caractère Personnel ; et (e) les coordonnées de la personne auprès de laquelle un différend ou une réclamation peut être soumis. L'information sera réalisée par

la publication par le H3C de ces informations sur son site internet aux côtés du présent Accord. Le PCAOB publiera également sur son site internet les informations appropriées relatives au traitement qu'il réalisera sur les Données à Caractère Personnel, y compris les informations mentionnées ci-dessus, comme décrit au présent Accord.

Une notification individuelle sera fournie par le H3C aux Personnes Concernées conformément aux règles de notification et aux dérogations et limitations applicables en vertu du RGPD (telles que prévues aux Articles 14 et 23 du RGPD). Dans l'hypothèse où le H3C estimerait, après avoir examiné les dérogations applicables à la notification individuelle, et après échange avec le PCAOB, qu'il est tenu, conformément aux dispositions du RGPD, d'informer une Personne Concernée du transfert de ses Données à Caractère Personnel au PCAOB, le H3C informera le PCAOB avant de procéder à cette notification individuelle.

4. Sécurité et confidentialité : Les Parties reconnaissent que, dans l'**Annexe I**, le PCAOB a fourni des informations décrivant ses mesures de sécurité techniques et organisationnelles jugées adéquates par le H3C pour protéger les Données à Caractère Personnel contre la destruction, la perte, l'altération, la divulgation ou l'accès de manière accidentelle ou illicite. Le PCAOB s'engage à informer le H3C de toutes les modifications apportées aux mesures techniques et organisationnelles de sécurité, qui affecteraient négativement le niveau de protection des Données à Caractère Personnel accordées aux Personnes Concernées par le présent Accord et à mettre à jour les informations fournies dans l'**Annexe I** conformément à l'article IV, paragraphe 3 du Protocole, si de telles modifications sont apportées. Lorsque le PCAOB fournira une telle information au H3C, le H3C informera l'Autorité Française de Protection des Données des modifications intervenues.

Le PCAOB a fourni au H3C une description des lois et/ou règlements applicables en matière de confidentialité et sur les conséquences de toute divulgation illégale d'informations non publiques ou confidentielles ou en cas de violations présumées de ces lois et/ou règlements.

Dans l'hypothèse où une Partie destinataire aurait connaissance d'une Violation de Données à Caractère Personnel transférées dans le cadre du présent Accord, elle notifiera l'autre Partie de la Violation de Données à Caractère Personnel sans délai excessif et si possible au plus tard 24 heures après avoir pris connaissance du fait que cette violation affecte des Données à Caractère Personnel. La Partie notifiant la Violation devra également mettre en œuvre, dès que possible, les moyens raisonnables et appropriés pour remédier à la Violation de Données à Caractère Personnel et réduire autant que possible ses éventuelles conséquences négatives.

5. Droits des Personnes Concernées : Une Personne Concernée dont les Données à Caractère Personnel ont été transférées au PCAOB peut exercer ses Droits des Personnes Concernées comme prévu à l'Article I(j), y compris en demandant au H3C d'identifier les Données à Caractère Personnel qui ont été transférées au PCAOB et en demandant au H3C d'obtenir confirmation de la part du PCAOB que les données sont complètes, exactes, et, le cas échéant, mises à jour et que le Traitement est conforme aux principes de Traitement des Données à Caractère Personnel du présent Accord. Une Personne Concernée peut exercer ses Droits des Personnes Concernées en adressant une demande directement au H3C :

Coordonnées du H3C :

- par courriel : dpd@h3c.org ;

- par courrier :

Haut conseil du commissariat aux comptes – Délégué à la protection des données
104 avenue du Président Kennedy – 75016 Paris (France)

Le PCAOB traitera d'une manière raisonnable et en temps utile toute demande de cette nature adressée par le H3C et portant sur des Données à Caractère Personnel transférées par le H3C au PCAOB. Chacune des Parties pourra prendre des mesures appropriées telles que la facturation de frais raisonnables pour couvrir les coûts administratifs ou le refus de donner suite à une demande manifestement infondée ou excessive d'une Personne Concernée.

Si la Personne Concernée souhaite contacter le PCAOB, elle peut envoyer un e-mail à : personaldata@pcaobus.org.

Les garanties relatives aux Droits des Personnes Concernées sont subordonnées aux obligations légales incombant aux Parties de ne pas divulguer d'informations confidentielles en vertu du secret professionnel ou d'autres obligations légales. Ces garanties peuvent être limitées afin d'éviter tout préjudice ou atteinte à l'exercice des missions de supervision ou de sanction dont sont chargées les Parties dans le cadre de l'exercice de l'autorité publique dont elles sont investies, telles que la surveillance ou l'évaluation du respect des lois applicables ou la prévention des infractions présumées ou les enquêtes s'y rapportant ; pour des motifs importants d'intérêt public général reconnus comme tels aux Etats-Unis et en France ou dans l'Union européenne, y compris dans l'esprit de réciprocité de la coopération internationale ; ou pour la supervision des personnes physiques et des entités réglementées. Toute limitation devra être nécessaire et prévue par la loi, et ne sera maintenue que tant que le motif de la limitation subsistera.

Le H3C fournira des informations à la Personne Concernée sur les suites données à une demande effectuée en vertu des articles 15 à 22 du RGPD dans les meilleurs délais, en tout état de cause, dans un délai d'un mois à compter de la réception de la demande. Ce délai pourra être prolongé de deux mois si nécessaire, en tenant compte de la complexité et du nombre des demandes. Le H3C informera la Personne Concernée de cette prorogation dans un délai d'un mois à compter de la réception de la demande. Si le H3C et/ou le PCAOB ne donne pas suite à la demande de la Personne Concernée, le H3C informera la Personne Concernée sans délai et au plus tard dans le mois suivant la réception de la demande des raisons de l'absence de suites données à sa demande et de la possibilité de former un recours auprès de l'Autorité Française de Protection des Données et de former un recours juridictionnel ou de recourir au mécanisme de plainte mis en place au sein du PCAOB. Tout litige ou réclamation introduit par une Personne Concernée relative au traitement de ses Données Personnelles en vertu du présent Accord peut être soumis au H3C, au PCAOB ou aux deux Parties, selon le cas, et conformément au Paragraphe 8.

Le PCAOB accepte de ne pas prendre, au sujet d'une Personne Concernée, de décision juridique qui soit fondée uniquement sur un traitement automatisé de Données à Caractère Personnel, y compris le Profilage, sans intervention humaine.

6. Catégories Particulières de Données à Caractère Personnel / Données Sensibles : Les Catégories Particulières de Données à Caractère Personnel / Données Sensibles, telles que définies à l'alinéa I (e), ne seront pas transférées par le H3C au PCAOB.

7. Partage ultérieur des Données à Caractère Personnel : Le PCAOB ne partagera les Données à Caractère Personnel reçues du H3C qu'avec les entités identifiées à l'article IV, paragraphe 6, du

Protocole.[2] Lorsque le PCAOB a l'intention de partager des Données à Caractère Personnel avec une tierce partie identifiée à l'Article IV, paragraphe 6 du Protocole, autre que la *Securities and Exchange Commission* des États-Unis, le PCAOB demandera le consentement écrit préalable du H3C et ne partagera ces Données à Caractère Personnel que si la tierce partie fournit des assurances appropriées conformes aux garanties prévues par le présent Accord. Lors de la demande d'un tel consentement écrit préalable, le PCAOB indiquera le type de Données à Caractère Personnel qu'il a l'intention de partager, les raisons pour lesquelles il a l'intention de les partager et les finalités de ce partage. Si le H3C ne donne pas son consentement écrit à ce partage dans un délai raisonnable ne dépassant pas dix jours, le PCAOB consultera le H3C et examinera toutes les objections qu'il pourrait avoir. Si le PCAOB décide de partager les Données à Caractère Personnel sans le consentement écrit du H3C, le PCAOB informera le H3C de son intention de procéder à un tel partage. Le H3C peut alors décider de suspendre le transfert de Données à Caractère Personnel et, dans la mesure où il décide de suspendre ces transferts, il en informera l'Autorité Française de Protection des Données. Lorsque la tierce partie ne peut fournir les assurances appropriées mentionnées ci-dessus, les Données à Caractère Personnel peuvent être partagées avec la tierce partie dans des cas exceptionnels, lorsque la communication des données répond à des motifs importants d'intérêt général, tels que reconnus aux Etats-Unis et en France ou dans l'Union européenne, y compris dans l'esprit de réciprocité de la coopération internationale, ou si ce partage est nécessaire pour constater, exercer, ou défendre des droits en justice.

Préalablement à tout partage de Données à Caractère Personnel avec la *Securities and Exchange Commission*, le PCAOB obtiendra de la *Securities and Exchange Commission* des assurances appropriées cohérentes avec les garanties prévues dans le présent Accord. En outre, si le PCAOB a partagé des Données à Caractère Personnel soumises au présent Accord avec la Securities and Exchange Commission des Etats-Unis, le PCAOB informera périodiquement le H3C de la nature des Données à Caractère Personnel partagées et de la raison pour lesquelles elles ont été partagées, dans la mesure où la fourniture de cette information ne risque pas de mettre en péril une enquête en cours. Cette restriction concernant les informations relatives à une enquête en cours ne sera maintenue que tant que le motif de la restriction subsistera.

Une Personne Concernée peut demander au H3C certaines informations relatives à ses Données à Caractère Personnel qui ont été transférées par le H3C au PCAOB dans le cadre de la coopération prévue par le Protocole. Il incombe au H3C de fournir ces informations à la Personne Concernée conformément aux dispositions du RGPD et de la Loi Informatique et Libertés. Sans préjudice du paragraphe précédent, dès réception d'une demande d'une Personne Concernée, le H3C peut demander au PCAOB des informations relatives au partage ultérieur des Données à Caractère Personnel par le PCAOB afin de permettre au H3C de se conformer à ses obligations d'information de la Personne Concernée au titre du RGPD et de la Loi Informatique et Libertés. Dès réception d'une telle demande du H3C, le PCAOB fournira au H3C toute information dont il dispose concernant le Traitement des Données à Caractère Personnel par une tierce partie avec laquelle le PCAOB a partagé ces Données à Caractère Personnel.

8. Recours : Tout différend ou réclamation introduit par une Personne Concernée à propos du Traitement de ses Données à Caractère Personnel en vertu du présent Accord peut être soumis au H3C, au PCAOB, ou aux deux Parties, selon le cas applicable. Chaque Partie informera l'autre Partie

[2] Les entités avec lesquelles le PCAOB est autorisé par la loi américaine à partager ultérieurement des informations confidentielles sont décrites à l'**Annexe II**.

WD

d'un tel différend ou réclamation et mettra en œuvre ses meilleurs efforts pour régler ce différend ou cette réclamation à l'amiable dans les meilleurs délais.

Toute question ou plainte concernant le Traitement des Données à Caractère Personnel par le PCAOB peut être adressée directement au « *Center for Enforcement Tips, Referrals, Complaints and Other Information* » du PCAOB, notamment par l'intermédiaire du « *Tips and Referral Center* », via le formulaire en ligne sur le site internet, par courrier électronique, lettre ou téléphone, ou peut être adressées au H3C, en envoyant ces informations à dpd@h3c.org. Le PCAOB informera le H3C des demandes qu'il reçoit de la part des Personnes Concernées sur le Traitement de Données à Caractère Personnel partagées par le H3C et il consultera le H3C sur la réponse à apporter.

Si une Partie ou les Parties ne sont pas en mesure de répondre à une question ou à une plainte déposée par une Personne Concernée concernant le Traitement de Données à Caractère Personnel par le PCAOB et reçue via le « *Tips and Referral Center* », et si la question ou la demande déposée par la Personne Concernée n'est pas manifestement infondée ou excessive, la Personne Concernée, la Partie ou les Parties peuvent utiliser un mécanisme approprié de règlement des différends mené par un organe indépendant au sein du PCAOB. La décision prise par le biais de ce mécanisme de règlement des différends peut être soumise à un deuxième examen indépendant, qui serait mené par un organe indépendant distinct. Le mécanisme de règlement des différends et le processus du deuxième examen sont décrits à l'**Annexe III** du présent Accord. Aux termes du présent Accord, la Personne Concernée peut exercer ses droits de recours judiciaire ou administratif (y compris en matière d'indemnisation) conformément à la loi française de protection des données. Dans les situations où le H3C est d'avis que le PCAOB n'a pas agi conformément aux garanties énoncées dans le présent Accord, le H3C peut suspendre le transfert de Données à Caractère Personnel jusqu'à ce que le problème soit résolu de manière satisfaisante et peut en informer la Personne Concernée. Avant de suspendre les transferts, le H3C consultera le PCAOB et le PCAOB répondra au problème soulevé dans les meilleurs délais.

9. Surveillance : Chaque partie procédera à l'examen périodique de ses politiques et procédures qui mettent en œuvre les garanties relatives aux Données à Caractère Personnel décrites dans le présent Accord. Sur demande légitime de l'autre Partie, une Partie examinera ses politiques et procédures afin de vérifier et de confirmer la mise en œuvre effective des garanties spécifiées dans le présent Accord et enverra une synthèse de l'examen à l'autre Partie.

Sur demande du H3C de procéder à un examen indépendant du respect des garanties prévues par l'Accord, le PCAOB demandera à l'*Office of Internal Oversight and Performance Assurance* (« IOPA »), organe indépendant au sein du PCAOB, d'effectuer un examen pour vérifier et confirmer que les garanties prévues dans le présent Accord sont effectivement mises en œuvre. L'IOPA procèdera à l'examen conformément aux procédures et aux normes établies et utilisées par l'IOPA pour réaliser ses missions courantes, comme détaillé à l'**Annexe IV** du présent Accord. Aux fins de son examen indépendant, l'IOPA sera informé de tout litige ou réclamation soulevé par une Personne Concernée concernant le Traitement de ses Données à Caractère Personnel conformément à la section 8 du présent article, y compris des mesures prises par le personnel du PCAOB pour mettre en œuvre les décisions résultant d'un mécanisme de règlement des différends. L'IOPA fournira une synthèse des résultats de son examen au H3C une fois que le conseil d'administration du PCAOB aura approuvé la communication de la synthèse au H3C.

Dans le cas où le H3C n'aurait pas reçu les résultats de l'examen réalisé par l'OIPA et qu'il serait d'avis que le PCAOB n'a pas agi conformément aux garanties prévues dans le présent Accord, le H3C pourra

hr WP

suspendre le transfert de Données à Caractère Personnel au PCAOB en vertu du présent Accord jusqu'à ce que le problème soit traité de manière satisfaisante par le PCAOB. Avant de suspendre les transferts, le H3C consultera le PCAOB qui répondra dans les meilleurs délais. Dans le cas où le H3C suspendrait le transfert de Données à Caractère Personnel au PCAOB, ou reprendrait les transferts après une telle suspension, le H3C en informera rapidement l'Autorité Française de Protection des Données.

ARTICLE IV - ENTRÉE EN VIGUEUR ET RÉSILIATION

Le présent Accord entre en vigueur à compter de la date de sa signature et ne restera en vigueur que durant la période d'application du Protocole. Les Parties peuvent consulter et réviser les termes de l'Accord dans les mêmes conditions que celles énoncées à l'article VI, paragraphes 2 et 3 du Protocole.

Le présent Accord peut être résilié par l'une ou l'autre des Parties à tout moment. Après la résiliation du présent Accord, les Parties continueront à maintenir confidentielles, conformément à l'article IV du Protocole, les informations fournies au titre du Protocole. Postérieurement à la résiliation du présent Accord, les Données à Caractère Personnel précédemment transférées en vertu du présent Accord continueront à être traitées par le PCAOB conformément aux garanties énoncées dans le présent Accord. Les Parties reconnaissent qu'en vertu de l'article 105(b)(5) de la loi Sarbanes-Oxley, la résiliation du présent Accord et du Protocole pourrait limiter la capacité du PCAOB à partager des informations confidentielles avec le H3C, en lien avec l'application des garanties énoncées dans le présent Accord.

Le H3C informera sans délai l'Autorité Française de la Protection des Données de toute modification ou résiliation du présent Accord.

ARTICLE V- DIVERS

Le présent Accord est établi en langues anglaise et française, les deux textes faisant également foi.

William D. Duhnke III
Président
Public Company Accounting Oversight Board

Date : 07 avril 2021

Florence Peybernes
Présidente du Collège
Haut Conseil du Commissariat aux Comptes

Date : 7 avril 2021

Annexes à
l'Accord entre le Haut Conseil du Commissariat aux Comptes (France) et le Public Company Accounting Oversight Board (États-Unis d'Amérique) sur le transfert de certaines données personnelles

Annexe I : Description des systèmes et des contrôles des technologies de l'information du PCAOB [CONFIDENTIEL]

Annexe II : Liste des entités avec lesquelles le PCAOB est autorisé à effectuer un partage ultérieur des informations confidentielles

Annexe III : Description des processus applicables au règlement des différends (recours)

Annexe IV : Surveillance de la mise en œuvre par le PCAOB des garanties prévues par l'accord de protection des données (DPA)

W- WO

Annexe II

Liste des entités avec lesquelles le PCAOB est autorisé à effectuer un partage ultérieur des informations confidentielles

Les parties tiers avec lesquels le PCAOB peut procéder à un partage ultérieur des données personnelles référencées à l'article III, paragraphe 7 de l'accord relatif à la protection des données (DPA) sont énumérées dans la version amendée de l'article 105 (b) (5) (B) de la loi Sarbanes-Oxley de 2002, qui dispose :

> (B) Accès des agences gouvernementales – Toutes les informations visées au sous-paragraphe (A) de l'article 105(b)(5) peuvent, sans pour autant perdre leur statut confidentiel et privilégié entre les mains du Collège :
>
> (i) être mises à la disposition de la Securities and Exchange Commission, et
>
> (ii) être mises à la disposition, à la discrétion du Collège s'il décide que ladite communication est nécessaire afin de réaliser l'objet de la présente Loi ou de protéger les investisseurs, du :
>
> (I) Procureur Général des Etats-Unis ;
>
> (II) Régulateur opérationnel Fédéral compétent[7] (tel que défini en section 509 de la Loi Gramm-Leach-Bliley (15 U.S.C. 6809)), à l'exclusion de la Securities and Exchange Commission et du Directeur de la Federal Housing Finance Agency, en ce qui concerne un rapport d'audit réalisé pour une institution soumise à la juridiction dudit régulateur ;
>
> (III) Procureur général de l'état dans lequel se déroule une enquête pénale ;
>
> (IV) Toute autorité étatique régulatrice compétente[8] ; et
>
> (V) un organisme d'autorégulation, compétent pour ce qui concerne les rapports d'audit émis par un courtier ou un négociant soumis à la juridiction de cet organisme d'autorégulation,
>
> et chacun d'entre eux devra conserver ces informations de manière confidentielle et privilégiée.

---

[7] Le terme «Régulateur opérationnel Fédéral compétent» dans la section (B) (ii) (II) est défini dans l'article 15 U.S.C. § 6809 et comprend :

- Le Conseil des gouverneurs du Système fédéral de réserve,
- Le Bureau du contrôleur de la monnaie,
  Le conseil des directeurs de la Federal Deposit Insurance Corporation,
- Le directeur de l'Office of Thrift Supervision,
- Le National Credit Union Administration Board, et
- La Securities and Exchange Commission.

Outre la SEC, ce sont les différents régulateurs des institutions financières aux États-Unis.

[8] L'expression « autorité étatique régulatrice » au sens de la règle 1001 (a) (xi) du PCAOB signifie « l'agence d'Etat ou toute autre autorité responsable de l'agrément ou de la réglementation de l'exercice de la comptabilité au niveau fédéral ou au niveau des États, et ayant compétence sur les entités de contrôle légal enregistrées ou les personnes qui y sont associées ». Il s'agirait principalement des Conseils de la Comptabilité des Etats aux États-Unis.

Annexe III

Description des processus applicables au règlement des différends (recours)

Le mécanisme de recours du PCAOB mentionné dans l'accord relatif à la protection des données (DPA) permet à une personne concernée d'exercer un recours relatif à des réclamations ou des litiges non résolus concernant le traitement par le PCAOB de ses données personnelles reçues en application du DPA. Le mécanisme de recours comprend deux niveaux d'examen. Comme décrit dans le DPA, le premier niveau d'examen se déroulera devant une personne exerçant une fonction indépendante au sein du PCAOB (le *Hearing Officer* du PCAOB). Le deuxième niveau d'examen se déroulera devant un organe indépendant lié contractuellement au PCAOB (un conseiller-auditeur d'une entité extérieure indépendante).

1. Premier niveau de recours – *Hearing Officer* du PCAOB

Le *Hearing Officer* du PCAOB agit en tant qu'examinateur indépendant et impartial des faits dans une procédure administrative formelle exigeant une décision faisant autorité. Le *Hearing Officer* du PCAOB est un avocat employé par le PCAOB et soumis au code de déontologie du PCAOB et aux dispositions de l'article 105 (b) (5) de la loi Sarbanes-Oxley (loi), y compris en ce qui concerne le traitement des informations confidentielles et non publiques. Il est indépendant de tous les services du PCAOB chargés de l'obtention et du traitement des données à caractère personnel dans le cadre des activités de supervision du PCAOB. Dans l'exercice de ses fonctions, le *Hearing Officer* du PCAOB a la responsabilité d'agir avec honorabilité et intégrité afin que ses décisions et ses conclusions soient justes et impartiales. Ces principes fondamentaux d'autorité nécessaire et appropriée, d'indépendance, d'objectivité, d'impartialité et d'équité s'appliquent au mécanisme de recours.

Les caractéristiques suivantes du service du *Hearing Officer* du PCAOB et les règles du PCAOB, sont conçues pour garantir l'indépendance du *Hearing Officer* du PCAOB:

- Le service du *Hearing Officer* du PCAOB recrute et emploie son propre personnel. Le *Hearing Officer* et son personnel sont situés dans des locaux physiquement séparés du reste du personnel du PCAOB. Le PCAOB est tenu de fournir un financement et des ressources appropriés au service du *Hearing Officer* du PCAOB,

- Il est expressément interdit aux membres du conseil d'administration et au personnel du PCAOB de tenter d'exercer une influence indue sur les décisions du *Hearing Officer* du PCAOB. (Dans le cadre d'un litige, le personnel ne peut fournir des preuves et des éléments qu'après en avoir avisé toutes les parties et leur avoir laissé la possibilité de réagir). Le non-respect de cette exigence exposerait le personnel à des mesures disciplinaires en vertu du code de déontologie du PCAOB,

- Il ne peut être mis fin aux fonctions du *Hearing Officer* du PCAOB, et une affaire ne peut lui être retirée, dans le but d'influencer l'issue d'une procédure. La cessation des fonctions du *Hearing Officer* du PCAOB nécessite l'approbation de la *Securities and Exchange Commission* des États-Unis,

- Les décisions concernant les résultats et la rémunération du *Hearing Officer* du PCAOB ne tiennent pas compte des de l'issue des procédures.

Le *Hearing Officer* du PCAOB examine de manière indépendante le bien-fondé d'une plainte formelle liée au respect par le personnel du PCAOB des garanties décrites dans le DPA lors du traitement des données personnelles d'une personne concernée. Il rend une décision faisant autorité dans un délai raisonnable.

W WD

Au stade du premier niveau de recours, une personne concernée soumet une plainte formelle au service du *Hearing Officer* du PCAOB décrivant avec précision les réclamations ou les litiges concernant le traitement par le PCAOB de ses données personnelles. Le personnel du PCAOB impliqué dans le traitement des données personnelles de la personne concernée produit une réponse à la plainte. L'homologue du PCAOB signataire de l'accord de protection des données peut soumettre une réponse pour décrire son implication dans le traitement et le transfert des données personnelles en question. La personne concernée reçoit une copie de toutes les réponses soumises au *Hearing Officer* du PCAOB, à l'exception de toute information confidentielle en vertu de l'article 105 (b) (5) de la loi Sarbanes-Oxley. Le *Hearing Officer* du PCAOB examine la plainte formelle et les réponses. Il prend une décision faisant autorité sur tous les faits contestés présentés afin de déterminer si le personnel du PCAOB a respecté les garanties décrites dans l'accord de protection des données lors du traitement des données à caractère personnel examinées.

Le premier niveau de recours prend fin lorsque le *Hearing Officer* du PCAOB rend une décision écrite concernant la plainte de la personne concernée. Si le *Hearing Officer* du PCAOB conclut que le personnel du PCAOB ne s'est pas conformé aux garanties prévues par l'accord de protection des données, le *Hearing Officer* du PCAOB ordonne au personnel du PCAOB de se conformer à ces mêmes garanties. La décision du *Hearing Officer* du PCAOB en faveur de la personne concernée est opposable au personnel du PCAOB, et le PCAOB ou son personnel ne peut pas demander une révision de la décision du *Hearing Officer* du PCAOB. Toutes les parties concernées reçoivent les résultats de la procédure administrative. La personne concernée reçoit une notification de la décision formelle préparée conformément aux exigences de confidentialité prévues à l'article 105 (b) (5) de la loi Sarbanes-Oxley. Lorsqu'elle est informée de la décision du *Hearing Officer* du PCAOB, la personne concernée reçoit une information relative au deuxième niveau de recours décrit ci-dessous, et quant à la procédure à suivre pour engager ce deuxième niveau.

2. Deuxième niveau de recours – Agent d'audition d'une entité indépendante

Le deuxième niveau de recours établi par le PCAOB permet à la personne concernée de demander une révision de la décision formelle rendue par le *Hearing Officer* du PCAOB. Le PCAOB utilise les services d'une entité indépendante, à laquelle le PCAOB a eu recours dans le passé pour des services similaires[9], comme agent d'audition pour le deuxième niveau de recours. Les agents d'audition sont des avocats expérimentés qui, lorsqu'ils fournissent des services dans le cadre d'un accord avec le PCAOB, sont soumis aux règles de ce dernier, y compris au code de déontologie du PCAOB et aux mesures d'indépendance et d'impartialité prévues par les règles juridictionnelles du PCAOB. En vertu d'un contrat, à la demande du PCAOB, l'entité indépendante met à disposition l'un de ses agents d'audition pour traiter de manière indépendante et impartiale tout sujet de recours. Un agent d'audition retenu pour traiter le deuxième niveau de recours est nommé « *examinateur du recours* ». Il signe un accord exécutoire de confidentialité avec le PCAOB aux termes duquel l'agent d'audition confirme qu'il respectera les exigences de confidentialité prévues par l'article 105 (b) (5) de la loi Sarbanes-Oxley lors de l'examen des informations confidentielles reçues au cours de la procédure de recours.

Pour accéder au deuxième niveau de recours, la personne concernée doit déposer une requête auprès du secrétariat du PCAOB au plus tard 30 jours après la notification de la décision du *Hearing Officer* du PCAOB. La requête doit identifier les erreurs ou les lacunes alléguées dans la décision du *Hearing Officer* du PCAOB issue du premier niveau de recours. Le secrétaire du PCAOB émet dans les

[9] A ce jour, le PCAOB n'a jamais employé plus d'un seul Hearing Officer (« agent d'audition »), il a passé un contrat avec un autre organisme de régulation pour pouvoir bénéficier des services des agents d'audition de ce dernier. Lorsque le recours à des agents d'audition supplémentaires a été nécessaire, les agents de cet organisme ont agi en tant que consultants ou entrepreneurs indépendants du PCAOB. Ils ont mené certaines procédures disciplinaires. Le deuxième niveau de recours est confié à l'un de ces agents d'audition, ou dans le cadre d'un arrangement similaire.

WD

plus brefs délais (sous 30 jours) une ordonnance attribuant l'affaire à l'entité indépendante, qui désigne un agent d'audition pour assurer les fonctions d'examinateur du recours.

L'examinateur du recours reçoit les éléments, ainsi que toute documentation supplémentaire à l'appui, de chaque partie impliquée (y compris la personne concernée, l'homologue du PCAOB signataire du DPA, et le personnel du PCAOB). Comme pour le premier niveau de recours, la personne concernée reçoit une copie de toutes les réponses soumises à l'examinateur du recours, étant précisé que toute information confidentielle en vertu de l'article 105 (b) (5) de la loi Sarbanes-Oxley sera expurgée.

En se fondant sur les contributions des parties et sur dossier, l'examinateur du recours détermine si les constatations et les conclusions du *Hearing Officer* du PCAOB sont arbitraires et inconséquentes, ou non conformes au DPA. A l'issue de son examen et dans un délai raisonnable, l'examinateur du recours rend une décision écrite quant aux contestations de la personne concernée à l'encontre de la décision de premier niveau. Si la décision conclut que le personnel du PCAOB n'a pas respecté les garanties de l'accord de protection des données, l'examinateur du recours ordonne au personnel du PCAOB de s'y conformer. La décision de l'examinateur du recours est rendue en dernier ressort.

Annexe IV

Surveillance de la mise en œuvre par le PCAOB des garanties prévues par l'accord de protection des données (DPA)

Dans le cadre du DPA, une surveillance indépendante du respect par le PCAOB des garanties prévues dans l'accord est assurée par le service de la supervision interne et de garantie de l'exécution du PCAOB (Office of Internal Oversight and Performance Assurance ci-après «IOPA» ou le «service»).[10]

L'IOPA est un service indépendant au sein du PCAOB. Il est chargé de « fournir un examen interne des programmes et des opérations du PCAOB afin de contribuer à garantir l'efficience, l'intégrité et l'efficacité internes de ces programmes et opérations. La garantie fournie par le service vise à favoriser la confiance du public, de la *Securities and Exchange Commission* et du Congrès des Etats-Unis dans l'intégrité des programmes et des opérations du PCAOB. »[11]

Pour accomplir sa mission, l'IOPA doit, entre autres actions, identifier les risques portant sur l'efficience, l'intégrité et l'efficacité des programmes et opérations du PCAOB. Sur la base de son évaluation des risques, il doit effectuer des examens, des audits et des enquêtes sur la performance et l'assurance qualité, afin de détecter et dissuader tout gaspillage, fraude, abus ou mauvaise gestion dans les programmes et opérations du PCAOB. Il doit recommander des actions constructives qui, une fois mises en œuvre, réduisent ou éliminent les risques identifiés et favorisent la conformité aux lois, réglementations, règles et procédures internes du PCAOB.

Les activités de l'IOPA comprennent, notamment :

- La fourniture d'une assurance qualité continue relative à la conception et l'efficacité opérationnelle des programmes du PCAOB,
- La conduite des enquêtes relatives aux programmes et aux opérations du PCAOB,
- La réception et l'examen des allégations d'actes répréhensibles déposées contre le personnel du PCAOB, ainsi que les conseils et les plaintes quant au gaspillage, à la fraude, aux abus ou à la mauvaise gestion potentiels dans les programmes ou opérations du PCAOB.

Afin de mener ses travaux, conformément à la Charte de l'IOPA, le directeur et le personnel de l'IOPA doivent « être préservés, dans les faits et en apparence, de toute altération personnelle, extérieure et organisationnelle affectant leur indépendance ». Afin de promouvoir cette indépendance, contrairement aux autres employés du PCAOB (qui relèvent généralement d'une seule personne au sein du PCAOB), le directeur rend compte directement aux cinq membres du conseil d'administration du PCAOB. En vertu de la charte de l'IOPA, « l'évaluation de la performance du directeur et la fixation de sa rémunération sont basées sur la gestion du service par son directeur, l'exécution effective des travaux du service [...] et ne sont pas fondées sur la nature des résultats des examens, audits et enquêtes réalisés par le service ». En outre, l'indépendance de l'IOPA est favorisée par le fait que le mandat du directeur est limité à un seul mandat de cinq ans et que l'IOPA lui-même est soumis à un contrôle externe d'assurance qualité régulier. L'IOPA peut également rapporter au directeur juridique du PCAOB, y compris au responsable de la déontologie (« Ethics Officer »), pour ce qui concerne ses missions, y compris les résultats de ses enquêtes sur les conseils, les plaintes et/ou les allégations de faute professionnelle ou déontologiques. Enfin, l'IOPA dispose d'une garantie d'accès

[10] La section 9 de l'accord de protection des données prévoit que, lorsque l'homologue du PCAOB signataire de l'accord demande un examen indépendant du respect des garanties prévues dans l'accord, le PCAOB ordonne à l'IOPA d'effectuer un examen afin de vérifier et confirmer que les garanties prévues dans l'accord sont effectivement mises en œuvre.

[11] Voir IOPA Charter.

kr- WP

illimité à tout le personnel ainsi qu'aux dossiers, rapports, audits, examens, documents, papiers, recommandations et autres éléments du PCAOB.

Dans le cas où l'IOPA aurait connaissance de « problèmes, abus ou carences particulièrement graves ou flagrants et liés à l'administration des programmes et des opérations du PCAOB, et que ceux-ci requièrent l'attention immédiate du conseil d'administration », l'IOPA doit immédiatement les signaler au conseil d'administration du PCAOB. Ils doivent également être signalés à la *Securities Exchange Commission* dans un délai de sept jours calendaires.

Afin de mener ses travaux, l'IOPA applique des normes et exigences acceptées. Celles-ci comprennent les lignes directrices obligatoires de l'institut des Auditeurs internes des Etats Unis, l'Institute of Internal Auditors, telles que (i) les normes internationales pour la pratique professionnelle de l'audit interne, (ii) les principes fondamentaux pour la pratique professionnelle de l'audit interne, (iii) la définition de l'audit interne, et (iv) le code de déontologie.

Au sujet du DPA, l'IOPA a la possibilité de procéder à un examen du respect par le PCAOB des garanties prévues par le DPA et relatives la protection des données concernées :

- De la propre initiative de l'IOPA, par exemple en se fondant sur son évaluation des risques pesant sur les programmes et opérations du PCAOB,
- En réponse à des conseils, des plaintes et/ou des allégations de faute professionnelle ou déontologique,
- Ou à la demande du conseil d'administration du PCAOB (par exemple pour se conformer à disposition du DPA qui prévoit que le PCAOB requiert un examen par l'IOPA, sur demande).

Afin de mener cet examen, et comme indiqué ci-dessus, l'IOPA dispose d'un accès illimité à toute la documentation du PCAOB relative aux activités concernées du PCAOB.

Dans le cadre de son examen, l'IOPA suit une démarche d'audit conforme aux normes internationales de l'Institute of Internal Auditors qui comprend les phases qui suivent.

Planification – Détermination des objectifs d'audit et des critères appropriés (les critères d'audit sont fondés sur les garanties décrites dans l'accord sur la protection des données). En outre, évaluation préliminaire des risques liés à la réalisation des objectifs de la direction et identification des contrôles en place pour atténuer les risques. Détermination du périmètre de l'audit par rapport aux processus et aux procédures de contrôle à examiner et à tester. Conception des tests substantifs de conformité à effectuer pour évaluer la conception et l'efficacité opérationnelle des garanties de protection des données.

Exécution – À la suite du programme d'audit documenté, réalisation des tests. Les tests comprennent généralement un examen des règles internes, des procédures et des descriptions des flux des processus du système d'information, des entretiens avec les responsables des processus et des contrôles, des présentations/démonstrations des garanties de protection et des contrôles connexes, la réexécution par l'auditeur de certain(e)s sauvegardes ou contrôles, un test par l'auditeur des sauvegardes/contrôles sur la base d'échantillons représentatifs, un examen des documents justificatifs attestant la conception et la réalisation des contrôles.

Examen de la qualité – La direction de l'IOPA supervise le travail en cours et examine et approuve le produit du travail du personnel. La direction de l'IOPA détermine la pertinence de chaque problème soulevé au cours de l'audit et l'adéquation des preuves apportées à cette occasion.

Rapports – L'IOPA rédige un rapport qui présente les résultats de son examen. Des recommandations sont faites pour améliorer les problèmes relevés. Le rapport comprend la réponse écrite du personnel du PCAOB, son accord avec les observations d'audit relevées, les mesures correctives prises ou prévues et les dates prévues pour les mettre en place. Le rapport est examiné

WP

par le conseil d'administration du PCAOB. Il est fourni à l'homologue du PCAOB signataire de l'accord, après l'approbation de la diffusion (non-publique) du rapport à cet homologue par le conseil d'administration du PCAOB. Cette approbation porte uniquement sur la divulgation non-publique des conclusions de l'IOPA, comme l'exige le code de déontologie du PCAOB. Elle n'inclut pas de participation du conseil d'administration dans l'élaboration du contenu du rapport de l'IOPA, ou d'influence sur les résultats de l'examen.

Suivi – Au moment opportun, l'IOPA effectue un suivi des actions correctives menées par le personnel du PCAOB afin de vérifier qu'elles ont été mises en place de manière satisfaisante.