

Deliberation 2021-032 of March 18, 2021 Commission Nationale de l'Informatique et des Libertés Nature of the deliberation:

Authorization Legal status: In force Date of publication on Légifrance: Wednesday March 31, 2021 Deliberation n° 2021-032 of March 18, 2021 authorizing the implementation of an administrative arrangement aimed at regulating the transfer of personal data between the Haut Conseil du Commissariat aux comptes (H3C) and its American counterpart, the Public Company Accounting Oversight Board (PCAOB) The National Commission for Computing and Liberties, Seizure by the Haut Conseil du Commissariat aux comptes (H3C) of a request for authorization concerning the implementation of an administrative arrangement aimed at regulating the transfer of personal data with its American counterpart, the PCAOB; No. 108 of the Council of Europe for the protection of individuals with regard to automatic processing of personal data; Having regard to the regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 /EC, in particular its article 46.3.b; Having regard to Opinion 05/2021 of the European Data Protection Board (EDPS) on the draft administrative arrangement aimed at regulating the transfers of personal data between the H3C and the PCAOB; Having regard to EDPS Guidelines 02/2020 on Articles 46 (3) (a) and 46 (3) (b) of Regulation 2016/679 concerning the transfer of personal data between European and non-European public authorities ; Considering the modified law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms; -17 of January 6, 1978 relating to data processing, files and freedoms; Considering the project and a memorandum of understanding on the terms and conditions of cooperation between the H3C and its US counterpart; On the proposal of Mr. Philippe Pierre CABOURDIN, commissioner, and after hearing the observations of Mr. Benjamin TOUZANNE, government commissioner , Considering the following: Following the ENRON and WORLDCOM financial scandals, the United States Sarbanes-Oxley (SOX) law, adopted in 2002, reformed the rules applicable, among other things, to the audit of the accounts of companies using the savings in U.S. markets. As part of these new measures, the SOX Act established the Public Company Accounting Oversight Board ( PCAOB ), which, under the authority of the U.S Securities and Exchange Commission ( SEC ), is responsible for overseeing US or foreign-based auditors (auditors) who certify the accounts of companies listed on US markets. The PCAOB requires the ability to conduct joint audits, in with the competent national authorities responsible for foreign auditors, to ensure the way in which these auditors work in the field so that a logic of mutual trust and, where applicable, reciprocity can prevail. During these checks, the PCAOB requires access not only to audit reports, but also to all of the documentation used to prepare these reports. It is in this context that personal data may be

transmitted to the United States. Under the applicable European texts, the supervision of these transfers must be ensured by a bilateral agreement between the High Council of the accounts (H3C) and the PCAOB. On the basis of an agreement concluded in 2013 then renewed in 2016, the CNIL had, on the basis of the provisions applicable before the entry into force of the general regulations on data protection (hereinafter GDPR), authorized the H3C on November 29, 2012, then July 11, 2013, and finally December 1, 2016, to transfer to the PCAOB personal data contained in information and/or audit documents relating to the statutory auditors under their dual supervision, or collected during controls. The bilateral agreement governing the transfer of personal data having expired on December 13, 2019, the H3C and the PCAOB have thus undertaken its renegotiation. The Commission was seized by the H3C of a request for authorization, concerning an administrative arrangement aimed at supervising the transfer of personal data with its American counterpart, the PCAOB. The latest status of the draft arrangement was sent to the Commission on November 19, 2020. Indeed, under Article 46 of the GDPR, in the absence of an adequacy decision from the European Commission (Article 45 of the GDPR ), a transfer of personal data to a third country can only take place if appropriate safeguards have been provided by the data exporter and on the condition that the data subjects have enforceable rights and effective legal remedies. Subject to authorization by the Commission Nationale de l'Informatique et des Libertés, the appropriate guarantees referred to above may be provided by provisions to be incorporated into administrative arrangements between public authorities which provide for enforceable and effective rights for persons concerned (article 46.3.b of the GDPR). It is expected within the community formed by the European counterparts of the H3C that this administrative arrangement will be used as a model for the framework for their transfers of personal data with the PCAOB. Given the pan-European scope of this agreement, the CNIL decided to refer the matter to the EDPS for a formal opinion on the basis of Article 64.2 of the GDPR. On February 2, 2021, the EDPS issued a favorable opinion concerning the guarantees provided by this administrative arrangement, considering that these met the requirements of the GDPR. As a reminder, the measures and principles contained in this agreement are as follows: Definition of the principles and rights of the person concerned; Principle of purpose limitation; Principle of accuracy and minimization of data; Principle of transparency; Security measures and of confidentiality; Special categories of personal data or sensitive data; Guarantees relating to the rights of data subjects; Principle of limitation of data retention; Restrictions on subsequent transfers; Complaints mechanism; Supervision mechanism. With regard to these elements and with the favorable opinion of the EDPS, the Commission endorses the analysis of the EDPS and concludes that the provisions of the administrative arrangement, in this

case, provide appropriate guarantees in accordance with the GDPR. Furthermore, the Commission welcomes and takes note of the information communicated by the H3C according to which the latter will keep a register containing, inter alia res, the following elements concerning the administrative arrangement: information concerning the independent nature of the Redress Reviewer; information concerning the retention period of personal data transferred under the administrative arrangement; information on the notifications received by the H3C concerning personal data breaches in view of Section III (4) of the Administrative Arrangement; information on the results of periodic reviews by the Office of Internal Oversight and Performance Assurance (IOPA); information on notifications received by the H3C pursuant to Section III (6) of the Administrative Arrangement; number of dispute resolution requests received by H3C or regarding personal data transferred by H3C. This decision may be appealed to the Council of State within two months of its notification DECIDES: Art. 1: The administrative arrangement aimed at regulating the transfer of personal data between the H3C and its US counterpart, the PCAOB, in its version transmitted on November 19, 2020, is authorized. Art. 2: This decision will be published on the CNIL website.

President Marie-Laure DENIS