Deliberation SAN-2022-025 of December 29, 2022 National Commission for Computing and Liberties Nature of the deliberation: Sanction Legal status: In force Date of publication on Légifrance: Thursday January 05, 2023 Deliberation of the restricted committee n°SAN-2022-025 of 29 December 2022 concerning APPLE DISTRIBUTION INTERNATIONALThe National Commission for Computing and Liberties, meeting in its restricted formation composed of Mr. Alexandre LINDEN, Chairman, Mr. Philippe-Pierre CABOURDIN, Vice-Chairman, Mr. Alain DRU and Mr. Bertrand du MARAIS, members; Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 relating to the protection of personal data and the free movement of such data (GDPR); Having regard to Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector; files and freedoms, in particular its articles 20 and following; Having regard to decree no. 2019-536 of May 29, 2019 taken for the application of law no. Having regard to deliberation no. 2013-175 of July 4, 2013 adopting the internal regulations of the National Commission for Computing and Freedoms; Having regard to decision no. 2021-113C of May 17, 2021 of the President of the National Commission for Data 'Informatique et des Libertés to instruct the Secretary General to carry out or have carried out the verification of the compliance of the processing of personal data implemented in the context of the use of the iOS operating systems (formerly "iPhone OS ") and MacOs to the provisions of Law No. 78-17 of January 6, 1978 relating to data processing, files and freedoms as amended and of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016; Having regard to the decision of the President of the National Commission for Computing and Liberties appointing a rapporteur to the restricted committee, dated January 10, 2022; Having regard to the report of Mr. François PELLEGRINI, commissioner rapporteur, notified to the company APPLE DISTRIBUTION INTERNATIONAL on July 27, 2022; Having regard to the written observations submitted by APPLE DISTRIBUTION INTERNATIONAL on September 19, 2022; Having regard to the rapporteur's response to these observations notified to APPLE DISTRIBUTION INTERNATIONAL on October 19, 2022; Having regard to the new written observations submitted by APPLE DISTRIBUTION INTERNATIONAL on November 21, 2022, as well as the oral observations made during the restricted training session of December 12, 2022; Considering the other documents in the file; Were present, during the restricted training session:- Mr François PELLEGRINI, statutory auditor, heard in his report;As representatives of the company APPLE DISTRIBUTION INTERNATIONAL:- […];The company APPLE DISTRIBUTION INTERNATIONAL having spoken last;The restricted committee adopted the following decision:I. Facts and procedure1. The APPLE Group (the APPLE INC. and

its subsidiaries, collectively the "APPLE Group") designs, manufactures and markets mobile communication and media devices, personal computers and sells a range of software, services and peripherals, network solutions , digital content and third-party applications in connection with these products.2. APPLE group products, which notably include the iPhone (multifunctional mobile telephone), are each supplied with a specific pre-installed operating system designed within the APPLE group (iOS for the iPhone).3. The APPLE group sells and delivers its digital content and applications through its online application stores, which are the App Store, the iTunes Store, the iBooks Store and the Mac App Store.4. APPLE INC. holds, as a general rule, directly or indirectly through intermediary entities, interests in all the subsidiaries of the group. These include the companies APPLE DISTRIBUTION INTERNATIONAL LTD (hereinafter the company "ADI"), APPLE FRANCE, APPLE RETAIL FRANCE and APPLE EUROPE INC. (hereinafter the company "AEI").5. ADI is located at Hollyhill Industrial Estate, Cork, Ireland and employs approximately […] staff. It presents itself as the entity responsible for the sales and distribution of APPLE group products in Europe. It also considers itself to be responsible for processing personal data in connection with the activity of the APPLE group's advertising platforms in the European Economic Area.6. For the year 2021, the ADI company achieved a turnover of around […] dollars, or around […] euros (according to the current exchange rate).7. APPLE FRANCE is located at 7, place d'Iéna in Paris (75116) and employs approximately […] employees. It does not sell or distribute products in France. Its role is to support the sales and marketing of products marketed by the ADI company with distribution partners on the French market, under a "sales and marketing assistance service contract" in force since October 1, 2018.8. APPLE RETAIL FRANCE is located at 3-5, rue Saint-Georges in Paris (75009). Its role is to sell and distribute APPLE.9 group products in France. The company AEI, which has its registered office in the State of Delaware, in the United States of America, has a branch in France which bears the same name (AEI), whose registered office is located at 7 place d'Iéna in Paris (75116).10. The company AEI, which has its registered office in the State of Delaware, in the United States of America, has a branch in France which bears the same name (AEI), whose registered office is located at 7 place d'Iéna in Paris (75116).11. On March 10, 2021, the National Commission for Computing and Liberties (hereinafter "the CNIL" or "the Commission") was seized by the association FRANCE DIGITALE of a complaint against APPLE. The complaint concerns the processing implemented by the APPLE group through its iOS and MacOs operating systems. In particular, it is stated in this complaint that the privacy setting "Personalized advertisements" present in the settings of devices marketed by the APPLE group and operating with the iOS and MacOs operating systems is activated by default, which does not allow users validly consent to

advertising targeting processing.12. Two online control missions on devices equipped with the iOS and MacOS operating system were carried out on June 8 and 16, 2021.13. Reports Nos. 2021-113/1 and 2021-113/2, drawn up by the delegation on the day of the inspections, were notified to the ADI and AEI companies on June 24, 2021. On this occasion, requests for additional information was sent to them. The ADI company responded by emails of July 5 and 12, 2021. On the other hand, by emails of June 30 and July 8, 2021, the AEI company indicated that it was unable to respond to the requests of the delegation, not playing a "a decisive role in the processing operations subject to control".14. A documentary check was also carried out with the companies ADI, AEI and APPLE FRANCE on July 13, 2021. These companies communicated their response to the CNIL, by emails of August 25, 2021. By emails of August 31, 2021, the companies APPLE FRANCE and AEI supplemented these responses by transmitting, each as far as it is concerned, the register of the processing operations carried out. On this occasion, a request for additional information was sent to ADI, which responded by email dated October 5, 2021.15. An on-site check, at the premises of the company APPLE FRANCE, was finally carried out on October 13, 2021 so that it could provide details on its relations with the company ADI, on the activity of the employees occupying the function of "Search Ads Platform Specialists" or "Search Ads Platform Specialists Managers" and on the operation of the "Apple Search Ads" service.16. Report no. 2021-113/3, drawn up by the delegation on the day of the inspection, was notified to the companies APPLE FRANCE and ADI, respectively on October 19 and December 14, 2021. On this occasion, a request for additional information was sent to APPLE FRANCE, which responded by email dated October 25, 2021.17. A request for additional information was sent to ADI by letter dated November 15, 2021, which responded by emails dated November 17 and December 3, 2021.18. By email of December 7, 2021, the CNIL sent a new request for additional information to ADI, which responded by email of December 22, 2021.19. For the purposes of examining these elements, the President of the Commission, on January 10, 2022, appointed Mr François PELLEGRINI as rapporteur on the basis of Article 22 of the law of January 6, 1978 as amended.20. By email of February 18, 2022, the company ADI requested a hearing in order to explain to the rapporteur the context of the complaint filed by the association FRANCE DIGITALE and to provide him with information relating to the framework in which s carry out the technical operations carried out on mobile terminals running the iOS.21 operating system. The rapporteur having responded favorably to this request, the hearing of the company took place on March 16, 2022 in the premises of the CNIL.22. The report n° CTX-2021-106 drawn up at the end of this hearing was notified by email to the company ADI on March 17, 2022. The communication of additional documents was again requested by the CNIL.23. On March 30, April 12 and June 3, 2022, ADI

communicated the requested documents to the CNIL.24. On July 27, 2022, the rapporteur notified the company of a report proposing that the restricted committee impose an administrative fine of six million euros in respect of the breach of Article 82 of Law No. 78 -17 of January 6, 1978 relating to data processing, files and freedoms (hereinafter "the Data Protection Act") which he considered constituted in this case. He also proposed that this decision be made public, but that it would no longer be possible to identify the company by name after the expiry of a period of two years from its publication.25. On July 29, 2022, the company requested additional time to submit its observations in response.26. On August 4, 2022, the Chairman of the Restricted Committee rejected this request.27. On September 19, 2022, the company produced its observations in response to the sanction report.28. On October 19, 2022, the rapporteur sent his response to the company's observations.29. On October 24, 2022, the company requested additional time to submit its second observations in response.30. On October 26, 2022, the President of the Restricted Committee rejected this request.31. On 21 November 2022, the company produced new observations in response to those of the rapporteur.32. On November 22, 2022, the rapporteur informed the company and the chairman of the restricted committee of the closure of the investigation. On the same day, the chairman of the Restricted Committee sent a notice to attend the Restricted Committee meeting of December 8, 2022.33. On November 23, 2022, the company requested the postponement of the restricted training session.34. On November 24, 2022, the Chairman of the Restricted Committee granted this request, setting the date of the meeting for December 12, 2022.35. The rapporteur and the company ADI presented oral observations during the session of the restricted committee.II. Reasons for decisionA. On the competence of the CNIL1. On the material competence of the CNIL and the applicability of the "one-stop shop" mechanism provided for by the GDPR36. Under the terms of Article 82 of the Data Protection Act, which constitutes the transposition into domestic law of Article 5(3) of Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002 concerning the processing personal data and the protection of privacy in the electronic communications sector, "any subscriber or user of an electronic communications service must be informed in a clear and complete manner, unless he has been informed beforehand , by the controller or his representative: 1° The purpose of any action seeking to access, by electronic transmission, information already stored in his electronic communications terminal equipment, or to enter information in this equipment; 2° The means at his disposal to oppose it. These accesses or registrations can only take place on condition that the subscriber or the user has expressed, after having received this information, his consent which may result from appropriate parameters its connection device or any other device placed under its control. […] ".37. The rapporteur considers that the CNIL

is materially competent to control and initiate a sanction procedure concerning the operations of writing and / or reading information implemented by the company ADI, namely on the users' terminal equipment and which fall within the scope of the "ePrivacy" directive. company ADI, called "Search Ads" for the purpose of personalizing ads on the App Store. This allows developers to promote their application to users on the App Store based only on the following criteria: the "type of 'device' (iPad, iPhone or both), 'customer type' (new, old or all existing users), 'demographic profile' (gender and age range), 'location' (city , region or country) and the "campaign planning" (start and end date of an advertising campaign).39. If the parameter relating to the receipt of targeted advertising in the App Store is activated in the settings of the iPhone, the user will see in priority displayed at the top of the results of his search the applications promoted via the "Search" service. ads". Conversely, if this parameter is not activated, users will still receive an ad, which will then not be personalized but contextual, depending on the search performed.40. To do this, the rapporteur points out that the company has put in place a "technical architecture" which operates in several stages.41. The first step relates to data collection: when creating the Apple user account (commonly called "Apple Id"), a technical identifier named "directory services identifier" (hereinafter "DSID") is assigned to each account user. The DSID is created on the company's servers. It is used in particular to access iCloud and the content, information and services associated with the Apple user account.42. While browsing the App Store, the trace of the user's activity (i.e. the fact that the user searches, downloads or purchases applications in the App Store), as well as the information he has entered in his Apple ID account (i.e. the year of birth, the gender and the location of the user), are collected and associated with this DSID identifier on the servers Apple's "Apple Media Platforms" (hereinafter "AMP").43. If the setting for receiving targeted advertising in the App Store is enabled, this data is used to determine which segments a user will be assigned to and therefore which advertisements they will receive. A "segment" is a group of at least 5,000 users who share similar characteristics and have the setting for receiving targeted advertising in the App Store enabled in iPhone settings.44. The second step relates to the creation of identifiers specific to the personalization of ads aimed at promoting mobile applications on the App Store: in order to prevent the distribution and measurement of advertising content from involving the use of the identifier DSID, the user's device will generate two other identifiers locally on the user's terminal: on the one hand, the "device pack identifier" (hereinafter the "DPID") which is synchronized via iCloud in order to ensure that all devices of the same user have the same DPID; on the other hand the iADID which is specific to each device and does not require synchronization via iCloud.45. Finally, the third step relates to the display of personalized ads on the user's terminal: when the user searches for an application in the App Store,

his device sends an advertising request to the "Ad Platforms " containing the searched word, the DPID, the iADID and the identifiers relating to the segments concerning it, so that they determine the targeted advertising to be broadcast as a priority (all of these elements being available locally on the terminal, the process prevents the "Ad Platforms" servers from being able to identify the Apple account associated with each request). The iADID can also be used to count the number of "ad impressions" made on a device, i.e. the number of times a given advertisement is displayed.46. In view of these elements, the rapporteur maintains, on the one hand, that the company carries out read and/or write operations on user terminals in order to authenticate the DSID of a user account registered as active on Apple servers for the purpose of personalizing ads intended to promote mobile applications on the App Store and, on the other hand, that the company performs a reading operation of the DPID and the iAdId (as well as the list of segments associated with the person previously written in the terminal by the AMP servers) in the users' terminals during requests sent to the "Ad Platforms" servers.47. In defence, the company maintains that the processing for personalization purposes of ads on the App Store that it implements is carried out either on its servers and is not part of the scope of the CNIL's investigations, or on the terminal users solely for the purposes of "securely authenticating the user" or "protecting privacy" and therefore constitute operations covered by the exemptions to the collection of consent provided for by article 82 of the Data Protection Act and Freedoms.48. To examine the question of the material existence of read or write operations, the Restricted Committee considers that a distinction must be made between the DSID and the DPID/iAdId.a. On read and/or write operations related to DSID49. In defence, the company first acknowledges that "information is stored on a single Apple device to securely authenticate its user in relation to the DSID of an Apple account on Apple servers" but specifies that this "information is not not […] used for advertising purposes”. The company then states that "searches performed in the App Store by users are necessarily followed by operations allowing Apple to return the search results to the device used. However, operations in this context are not performed to create segments for advertising purposes, but simply to provide the requested service, i.e. the App Store". The company finally specifies that "all the information used by Apple to create the segments described in its observations n°1 for the purposes of personalization of advertisements is stored and kept on Apple's servers".50. The Restricted Committee notes firstly that it emerges from these elements that the company does not deny carrying out information writing operations on user terminals in order to authenticate the DSID of a user account registered as active on Apple servers.51. Next, the Restricted Committee notes that although the company maintains that no information is stored and/or read on the user's terminal in order to assign segments to them, the fact remains that it is in able to

identify all requests relating to searches in the App Store to Apple servers as coming from a single terminal associated with a specific account.52. The Restricted Committee also notes that when asked about the said mechanism, during the hearing of March 16, 2022, the company indicated that "When the user searches the App Store and downloads applications or performs transactions through this platform, its activity is recorded by the server of said platform and is associated with its "directory services ID" (DSID), which is the technical identifier relating to the user's APPLE user account (a DSID corresponds to an APPLE ID)". In addition, during this hearing, the DSID was presented as "essential to securely authenticate a terminal and an Apple account". The Restricted Committee also notes that the rapporteur has described the processing in question, indicating in particular that "the DSID is the technical identifier relating to the user account of each user and allows the connection to be maintained when the user is browsing on various Apple services" and that this point has not been disputed by the company. It appears from these elements that "information", which is then linked to the DSID, is read on the user's terminal in order to associate his downloads and the results of his searches with his Apple account.53. Consequently, the Restricted Committee considers that the company carries out operations to read and/or write information on user terminals to authenticate the DSID of a user account registered as active on Apple.b servers. On the operations of reading the DPID and the iAdId in the user's terminal54. In defence, the company acknowledges that "technical measures, such as "storage" and "access" operations to the terminal […] are intended to replace the DSID by the DPID, in order to avoid to establish a link between the identity of the user (the DSID) and the relevant segments applicable to this user ", in accordance with the obligation of data protection by design provided for in Article 25 of the GDPR. With regard to the DPID identifier, it nevertheless specifies that this replacement operation takes place solely to protect "the privacy of its users". Regarding the identifier iAdId, it indicates that it "does not allow any tracking and that it is used only as an identifier for strengthening confidentiality, in the context of statistical measures".55. The Restricted Committee recalls again that the only action tending to access information already stored in the user's terminal equipment located in France entails the application of Article 82 of the Data Protection Act.56. The Restricted Committee therefore considers that if the replacement of information attached to the DSID by third-party identifiers (DPID and iAdId, which are generated directly by the user's telephone) has the advantage of avoiding the dissemination of the DSID to the "Ad Platforms" servers dedicated to APPLE advertising (and therefore to break the link between the identifier and the identity of the person concerned), the fact remains that these two new identifiers, (as well as the list of segments associated with the person previously written in the terminal by the AMP servers) are subsequently read in the user's terminal during the

construction of the requests sent to the "Ad Platforms" servers. They are indeed used during the steps relating to the selection and distribution of ads intended to promote targeted applications on the App Store as well as for counting the number of times an ad is displayed on a device (measurement of " advertising impressions"), which therefore clearly implies access to information already stored in the user's terminal equipment.57. Consequently, the Restricted Committee considers that the company is carrying out a reading operation of the DPID and the iAdId (as well as the list of segments associated with the person previously written in the terminal by the AMP servers) in the terminal of the user during requests sent to the "Ad Platforms" servers.c. On subsequent processing and the applicability of the "one-stop shop" mechanism provided for by the GDPR58. In defense, the company argues the inseparable nature of the operations of writing and / or reading identifiers that take place on the user's terminal equipment during their use of the App Store and subsequent use data collected by these identifiers for the purposes pursued by the data controller. Thus, the company considers that "the rapporteur does not respond to the analysis [...] according to which the CNIL would not be competent in application of the GDPR". It claims that operations to assign segments to a given user take place on the APPLE Group's AMP servers and not on the user's device, "provided an Apple device has authenticated with the server". It deduces from this that "this processing can therefore only be a "subsequent processing" carried out after any "reading" or "storage" operation carried out for authentication". Therefore, the company considers that, insofar as the CNIL has initiated a sanction procedure against it with regard only to the operations of writing and / or reading of identifiers which take place on the terminal equipment of the user during their use of the App Store, it is not justified in mobilizing, in its demonstration, elements related to the processing subsequent to these operations, in this case the activities carried out subsequently on the Apple servers which do not " not involve storing, or accessing, information on the user's device". It considers that this processing does not fall under Article 82 of the Data Protection Act but under the GDPR and that, insofar as its main establishment is located in Ireland, the competence to initiate such a procedure would belong to the authority of data protection authority, lead authority under Article 56 of the GDPR, competent to implement the mechanism for cooperation between supervisory authorities, known as the "one-stop shop" mechanism, provided for in Chapter VII of this regulation.59 . The Restricted Committee recalls first of all, that it is necessary to distinguish, on the one hand, the operations of reading and writing on a terminal, which are governed by the provisions of article 82 of the Data Protection Act and for which the French legislator has entrusted the CNIL with a mission of control and in particular the power to sanction any ignorance of this article and, on the other hand, the use which is subsequently made of the data produced or collected via these operations,

which is governed by the GDPR and can therefore, if necessary, be subject to the "one-stop shop" system.60. It then recalls that the Council of State, in its decision Société GOOGLE LLC and société GOOGLE IRELAND LIMITED of January 28, 2022, confirmed that the control of operations for accessing or recording information in user terminals in France of an electronic communications service, even resulting from cross-border processing, falls within the competence of the CNIL and that the one-stop-shop system provided for by the GDPR is not applicable: "it has not been provided for the application of the so-called "one-stop shop" mechanism applicable to cross-border processing, defined in Article 56 of this regulation, for the measures for the implementation and control of Directive 2002/58/EC of July 12, 2002, which fall within the scope of the competence of the national supervisory authorities under Article 15a of this directive. It follows that, with regard to the monitoring of access operations and the recording of information in user terminals in France of an electronic communications service, even resulting from cross-border processing, the measures for monitoring the application of the provisions transposing the objectives of Directive 2002/58/EC fall within the competence conferred on the CNIL by the law of January 6, 1978 […]" (EC, 10th and 9th chambers combined, January 28, 2022, GOOGLE LLC and GOOGLE IRELAND LIMITED, No. 449209, pt. 12). The Council of State reaffirmed this position in a judgment of June 27, 2022 (CE, 10th and 9th chambers combined, June 27, 2022, company AMAZON EUROPE CORE, n° 451423).61. Finally, the Restricted Committee notes that if the rapporteur's writings contain references to the consequences of writing and/or reading information on user terminals in order to authenticate the information attached to the DSID of a user account as well as those of the DPID and the iAdId for Internet users, they do not contain any analysis on the compliance with the GDPR of the subsequent processing of personal data carried out from the data collected by means of these tracers. Only the read and/or write operations of the DPID, DSID and iAdId identifiers and their purposes will be analyzed to determine whether article 82 of the Data Protection Act is applicable.62. Therefore, the Restricted Committee considers that the CNIL is competent to control and initiate a sanction procedure concerning the processing implemented by the company falling within the scope of the "ePrivacy" directive, provided that the processing is related to its territorial jurisdiction.2. On the territorial jurisdiction of the CNIL63. Under the terms of paragraph I, of article 3 of the Data Protection Act, which provides for the rule of territorial application of the requirements provided for in article 82 of the Data Protection Act: "Without prejudice, with regard to the processing falling within the scope of Regulation (EU) 2016/679 of 27 April 2016, the criteria provided for in Article 3 of this regulation, all the provisions of this law apply to the processing of personal data carried out in the context of the activities of an establishment of a controller or a processor on French territory,

whether or not the processing takes place in France. The rapporteur considers that the CNIL has territorial jurisdiction pursuant to these provisions when the processing covered by this procedure, consisting of operations to read and/or write information in the mobile terminals of users residing in France during of the use of the App Store, is carried out within the "framework of the activities" of the companies APPLE RETAIL FRANCE and APPLE FRANCE, which constitute the "establishment" on French territory of the company ADI, which participate in the promotion and the marketing of ADI's products and their advertising solutions in France.65. In defence, the company contests the territorial jurisdiction of the CNIL insofar as there is no "indissociable link" between the activities of the company APPLE RETAIL FRANCE and the processing in question. The company considers in this sense that "the mere sale of computer equipment does not create […] a link with the processing operations carried out by the software present on this equipment". It therefore considers that the second criterion of territorial application of the Data Protection Act, provided for in paragraph I of its article 3, is not fulfilled, namely that the processing in question is carried out "in the context of the activities of this establishment". Similarly, with regard to the company APPLE FRANCE, the company ADI also considers that the territorial jurisdiction of the CNIL is not established. It argues that there cannot be an "indissociable link" between the activities of APPLE FRANCE and the processing in question insofar as "the hiring of "Search Ads Specialists" in France" did not have the effect to generate a significant difference in income and that they are not "promoting and marketing advertising tools".66. The Restricted Committee recalls that under Article 3 of the Data Protection Act, the CNIL is competent to exercise its powers when the two criteria provided for in this article are met, in this case, the existence of an establishment of the data controller on French territory and the existence of processing carried out within the framework of the activities of this establishment.67. With regard firstly to the existence of an establishment of the data controller on French territory, the Court of Justice of the European Union (CJEU) has, in its Weltimmo judgment of 1 October 2015, specified that " the concept of "establishment", within the meaning of Directive 95/46, extends to any real and effective activity, even minimal, carried out by means of a stable installation", the criterion of stability of the installation being examined with regard to the presence of "human and technical resources necessary for the provision of the concrete services in question". The CJEU considers that a company, an autonomous legal person, from the same group as the controller, can constitute an establishment of the controller within the meaning of these provisions (CJEU, 13 May 2014, Google Spain, C-131/12, pt 48).68. In this case, the Restricted Committee notes that the companies APPLE RETAIL FRANCE and APPLE FRANCE are both subsidiaries of the company APPLE INC and have stable premises located in France. It further notes that

APPLE FRANCE employs around […] people. Consequently, the companies APPLE RETAIL FRANCE and APPLE FRANCE each constitute an establishment of the company ADI within the meaning of Article 3 of the aforementioned Data Protection Act.69. Secondly, with regard to the existence of processing carried out in the context of the activities of this establishment, the Restricted Committee recalls that it is not necessary for the processing in question to be carried out "by this establishment" (CJEU , May 13, 2014, Google Spain, C-131/12, pt. 57), i.e. by the companies APPLE RETAIL FRANCE or APPLE FRANCE, as data controllers, and that it suffices that the 'one and/or the other of these establishments sufficiently facilitate or promote the deployment in French territory of the processing of personal data implemented by the data controller established in another Member State (the company ADI) so that there is an obligation to respect the law territorially applicable in France and to establish the jurisdiction of the national supervisory authority.70. In this sense, the Restricted Committee notes that, in its AMAZON EUROPE CORE decision of June 27, 2022, the Council of State recalled that "it follows from the case law of the Court of Justice of the European Union, in particular from its judgment of 5 June 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH (C-210/16), that in view of the objective pursued by this directive [the "e-Privacy" directive], consisting to ensure effective and complete protection of the fundamental rights and freedoms of natural persons, in particular the right to the protection of privacy and the protection of personal data, a processing of personal data may be regarded as carried out " within the framework of the activities "of a national establishment, not only if this establishment itself intervenes in the implementation of this processing, but also in the case where the latter is limited to ensuring, on the territory of a Member State , the promotion and sale of advertising space making it possible to make profitable the services offered by the data controller consisting in collecting personal data by means of connection tracers installed on the terminals of visitors to a site "(CE, 10th and 9th chambers combined, June 27, 2022, company AMAZON EUROPE CORE, n° 451423, pt. 10). The Council of State considered in this same decision that this was the case when the activities of the establishment of the data controller consist of the promotion and marketing of advertising tools controlled and operated by the data controller operating in particular thanks to the data collected through connection tracers placed on the terminals of users of the site operated by the data controller (pt. 15 of the aforementioned decision).71. First of all, with regard to the company APPLE RETAIL FRANCE, the Restricted Committee notes that the information and identifiers deposited and/or read by the company ADI make it possible to supply the advertising tools that the latter develops and which, in particular, part of the App Store integrated into phones sold by APPLE RETAIL FRANCE. The operating system

embedded in mobile terminals is marketed in France on ADI company products only through APPLE RETAIL FRANCE. The latter, whose mission is to market specifically in France the terminals manufactured by the APPLE group, by also offering a set of services, helps to promote the products of the APPLE group. Thus, insofar as each telephone sold by APPLE RETAIL FRANCE contains the App Store application by default, the Restricted Committee considers that the latter's activity directly and necessarily contributes to people with an iPhone being able to access the App Store and carry out searches there, the results of which will be personalized by the company ADI.72. In addition, with regard to the company APPLE FRANCE, the Restricted Committee notes that, within the framework of the "Search Ads" service implemented by the company ADI allowing developers to promote their application to users on the App Store, APPLE FRANCE employs "Search Ads Specialists". According to the company, their role is "to assist app publishers to help them understand the tools provided by Apple in Search Ads, and to make recommendations on how best to optimize their campaign and structure these by assisting them, for example, with the choice of keywords to use for the campaign depending on the application to be promoted and helping them to choose targeting criteria (geography, age, etc.)". Therefore, the information and identifiers deposited and / or read by the ADI company allow developers who want their applications to be presented in the App Store to better target their audience. The fact that the "Search Ads Specialists" only generated an "insignificant difference in income" or do not themselves directly carry out an activity of "promotion and marketing of advertising tools" is irrelevant.73. Consequently, the Restricted Committee considers that an inseparable link is established between, on the one hand, the operation of reading and/or writing information to authenticate the DSID of a user account as well as those of the DPID identifiers and iAdId in mobile terminals equipped with the iOS operating system of users residing in France when using the App Store by ADI and, on the other hand, the activities of APPLE FRANCE companies in that they advises application developers in their advertising campaigns and APPLE RETAIL FRANCE as a promoter of the iOS .74 operating system. The Restricted Committee notes that the two criteria provided for in Article 3, paragraph I, of the Data Protection Act are therefore met.75. It follows that French law is applicable and that the CNIL is materially and territorially competent to exercise its powers, including that of imposing sanctions concerning processing falling within the scope of the "ePrivacy" directive. B. On the procedure76. In defence, the company first argues that the sanction procedure is based on obsolete facts or which have not been the subject of findings. It states that the "report focuses on version 14.6 of iOS, the operating system for iPhones, which is not the up-to-date [iOS 15] version" and that, therefore, "contrary to what as the Reporter asserts […] the setting for personalized ads was therefore in no way activated "by default" at

the date of the Report. In addition, iOS 15 was available during the majority of the procedure of control and instruction preceding the communication of the report". During the session before the Restricted Committee, the company also argued that insofar as the CNIL's delegation of control did not create an account when initializing the telephone during its investigations, for this reason, she could not materially observe the reading and/or writing operations on which the rapporteur relies to characterize her breach of article 82 of the Data Protection Act.77. The company then argues that the procedure followed by the CNIL does not respect the right to a fair trial as well as the principles of predictability and legal certainty, as guaranteed by Articles 6 and 7 of the Convention for the Protection of Human Rights. man and fundamental freedoms. With regard to the right to a fair trial, the company considers first of all that its right not to participate in its own incrimination has been violated insofar as, during the investigation phase, it voluntarily transmitted documents which were then retained as "prosecuting evidence against her" in the context of the sanction procedure. She argues that these elements were obtained by coercion or pressure because she was obliged to respond to requests from the CNIL in application of Article 18 of the Data Protection Act. Therefore, it considers that the Restricted Committee should close the procedure as it stands. The company then considers that it did not have the time necessary to fairly prepare its defense because its requests to obtain an extension of the deadline to respond to the rapporteur were systematically refused. She argues that "distance delays" should have been applied simply because she is not in metropolitan France. It further argues that the principle of equality of arms was not respected because it was not given sufficient time to prepare the English translations of the "essential documents of the sanction proceedings", namely the report and the rapporteur's response. Finally, the company argues that the "rapporteur did not include in his writings the letter from Apple to the CNIL dated March 30, 2022 in which it presented detailed observations on the minutes of the hearing of the March 16, 2022 […]". Regarding the violation of the principles of foreseeability and legal certainty, ADI considers that it "could not reasonably have foreseen that it [APPLE RETAIL FRANCE] was going to be implicated in these proceedings" whereas she has "never received a request or question from the CNIL". It therefore requests that the elements relating to this entity be excluded.1. On the facts on which the proceedings are based78. The Restricted Committee notes first of all that version 14.6 of the iPhone operating system was the system available on the day of the online check of June 16, 2021 and that it is therefore legitimate for the analysis of the compliance of processing implemented has related to this system. While the Restricted Committee notes the efforts that the company has made during the procedure to create new parameters requesting users to accept that information be entered and/or read in their terminal, the fact remains

that the breach identified by the rapporteur is limited to version 14.6 of the iPhone operating system, based on the findings made by the CNIL's delegation of control. The Restricted Committee finds that the materiality of the operations of reading and/or writing information on the user's terminal within the meaning of Article 82 of the Data Protection Act, emerges from the responses provided by the company to documentary checks and the existence of these operations is therefore established on file for users of versions prior to version 14.6.79. Consequently, the Restricted Committee considers that it follows from these elements that the procedure is not based on "obsolete facts".2. On respect for the right to a fair trial and the principles of foreseeability and legal certainty80. The Restricted Committee considers first of all that, contrary to what the company maintains, the elements referred to in its writings were not obtained by coercion or pressure. It stresses that the right not to contribute to one's own incrimination is intended in particular to avoid, by the exercise of pressure to obtain evidence, miscarriages of justice. It also notes that according to the case law of the European Court of Human Rights, the right not to incriminate oneself "does not extend to the use, in criminal proceedings, of data which can be obtained from the accused by the use of coercive powers but which exist independently of the will of the suspect, for example documents obtained under a warrant" (ECHR, Saunders v. United Kingdom, 17 December 1996).81. In this case, all the information collected by the CNIL was collected as part of a control procedure based on Article 19 of the Data Protection Act, through document and on-site checks. , as well as in the context of a hearing which was requested by the company. If the provisions of article 18 of the law "Informatique et Libertés" oblige the controlled bodies to provide the CNIL with the information requested, the restricted committee notes on this point that the information provided by the company contained exclusively elements of objective facts , describing the technical architecture of its "Search Ads" processing.82. The Restricted Committee then recalls that when the delegation of control requests information, in particular factual information, from an organization, no accusation has yet been brought against it, so that the "adversarial" phase, as understood by the case law of the European Court of Human Rights, has not yet begun. The Restricted Committee also notes that the company then had every opportunity to challenge the findings established by the delegation of control and their analysis by the rapporteur.83. Next, with regard to the right to have the time and facilities necessary for the preparation of one's defence, the Restricted Committee recalls that this right is one of the components of the right to a fair trial contained in Article 6 of the Safeguard Convention of human rights and fundamental freedoms and which must, in accordance with the case law of the European Court of Human Rights, be analyzed in the light of its function in the general context of the proceedings (see, inter alia, Mayzit v. Russia, 20 January 2005).84. In addition,

pursuant in particular to Article 40 of Decree No. 2019-536 of May 29, 2019, the implementation of the principle of adversarial proceedings means that any document, argument, exhibit or reply letter must be communicated to the implicated, to the rapporteur and to the Restricted Committee. This article provides that the data controller who is notified of a report proposing a sanction has, first of all, a period of one month to send his observations to the restricted committee and to the rapporteur. When the circumstances of the case or the complexity of the case justify it, the president of the restricted committee may decide, at the request of the body in question, to extend this period, within the limit of one month. This same article then grants the data controller a second period of one month to respond to the rapporteur's observations in response. These deadlines are such as to guarantee respect for the rights of the defence. Finally, the data controller may present oral observations during the session before the Restricted Committee.85. In the present case, the Restricted Committee notes that the company was given a period of one month and 23 days to produce its observations, it being recalled that Article 40 of Decree No. 2019-536 of May 29, 2019 imposes a minimum period of one month. Moreover, as recalled by the Council of State in its GOOGLE LLC decision of June 19, 2020, "no rule or principle imposes the institution, in terms of administrative sanction procedure, of a distance period, applicable to applicants domiciled outside metropolitan France" (CE, 10th and 9th chambers combined, June 27, 2022, company GOOGLE LLC, n° 430810, pt 13). Finally, given that the company had a new deadline to submit written observations to the rapporteur's response, and that it had the option of expressing itself again before the restricted committee, the latter considers that 'the company's rights of defense have not been infringed.86. In addition, with regard to the questioning of the company APPLE RETAIL FRANCE in the procedure, the Restricted Committee notes that the decision of the President of the Commission to initiate sanction proceedings only concerns the company APPLE DISTRIBUTION INTERNATIONAL. It therefore considers that, contrary to what is claimed, the company APPLE RETAIL FRANCE is not implicated in these proceedings. It also considers that the elements introduced by the rapporteur in his writings concerning this company did not hinder the preparation of the company ADI in its defence, insofar as they had been communicated by the company ADI itself concerning its membership of the APPLE group or were publicly accessible to the trade and companies register concerning its corporate purpose.87. Finally, the Restricted Committee considers that the "omission" of the letter of March 30, 2022, to use the terms of the company, does not deprive it of procedural guarantees. This exhibit submitted to the proceedings by the company ADI was examined by the Restricted Committee, which, moreover, is not in possession of any exhibits of which the company was not aware.88. Consequently, the Restricted Committee considers that it follows from these elements that the

right of society to a fair trial as well as the principles of foreseeability and legal certainty have been respected.C. On the breach of the provisions of article 82 of the Data Protection Act with regard to version 14.6 of iOS89. As recalled in point 36, Article 82 of the Data Protection Act constitutes the transposition into domestic law of Article 5(3) of the "ePrivacy" Directive.90. The rapporteur, to propose to the restricted committee to consider that the company has failed to comply with its obligations resulting from article 82 of the Data Protection Act, relies on the fact that the operations of reading and/or writing information to authenticate the DSID of a user account and the DPID and iAdId identifiers on the user's terminal for advertising purposes, requires that the latter has given his prior consent, under the conditions provided for by the provisions of article 82 of the amended law of 6 January 1978, as clarified by article 4, paragraph 11, of the GDPR.91. However, the rapporteur first notes that it emerges from the observations made that at the end of the initialization process of the telephone equipped with the iOS 14.6 version of the operating system, no mechanism intended to obtain the prior consent of the user operations consisting of reading the aforementioned information and identifiers on his terminal has been presented to him. The rapporteur then notes that once the initialization of the phone was completed, the delegation found that the tab entitled "Personalized advertisements" in the menu relating to "Apple Advertising" in the privacy settings was activated. He therefore considers that the user journey of the iOS 14.6 version of the operating system did not allow valid consent to be obtained under the conditions provided for by the aforementioned Article 82.92. The rapporteur then notes that the company indicated that it had deployed an update to the iOS operating system on September 20, 2021. This update required new users and those already equipped with an APPLE-branded mobile terminal, for which the "Personalised Ads" setting was enabled and who could install the update, to be chosen when first launching the App Store. This choice is manifested by a positive act and it is advisable to click on the "Enable personalized advertisements" button or the "Disable personalized advertisements" button, and therefore relates to the acceptance by the user that his personal data may be subject to processing for the purpose of targeted advertising. It notes that this new window constitutes an improvement in terms of obtaining consent, insofar as a choice relating to targeted advertising is offered to the user and could, therefore, constitute a valid mechanism for obtaining consent to read the aforementioned information and identifiers on the user's terminal, pursuant to article 82 of the aforementioned law. Nevertheless, the rapporteur notes that the statement "Apple does not track your activities" is misleading, insofar as operations for reading and/or writing the aforementioned information and identifiers on the user's mobile terminal are implemented at advertising purposes. Therefore, it makes this compliance subject to three conditions: that the window be written in French,

that the mention "Apple does not follow your activities" be amended and that no identifier be used for advertising purposes before consent of the user has been validly collected via this window.93. In defence, the company first argues, as developed in point 47, that the processing it implements does not fall within the scope of the "ePrivacy" directive or benefits from the exemption the collection of consent within the meaning of article 82 of the Data Protection Act. The company then argues that the new window intended to collect consent under the new iOS 15 version of the operating system has always been available in French. It considers that the information provided cannot be considered misleading or insufficiently precise but indicates in any case to supplement the mention "Apple does not follow your activities" by "Apple does not follow your activities on apps and company sites third parties". It specifies that this modification will be effective by March 2023. Finally, it confirms that no identifier is stored in the terminal or read for advertising purposes before this window is presented to the user.94 . Firstly, the Restricted Committee recalls, as it has developed in points 49 and following, that it considers that the company ADI performs read and/or write operations on the user's terminal. 95. The Restricted Committee recalls that Article 82 of the Data Protection Act requires consent to operations for reading and writing information in a user's terminal but provides for specific cases in which certain tracers benefit from an exemption. consent: either when the sole purpose of this is to allow or facilitate communication by electronic means, or when it is strictly necessary for the provision of an online communication service at the express request of the user.96 . The Restricted Committee notes in this respect that the Commission specifies, in its guidelines of September 17, 2020, that "the use of the same tracker for several purposes, some of which do not fall within the scope of these exemptions, requires obtain the prior consent of the persons concerned, under the conditions set out in these guidelines. For example, in the case of a service offered via a platform requiring user authentication ("logged-in universe"), the publisher of the service may use a cookie to authenticate users without asking for their consent (because this cookie is strictly necessary for the provision of the online communication service). On the other hand, it may not use this same cookie for advertising purposes other than if the latter have actually consented beforehand to this specific purpose".97. The Restricted Committee considers that in order to determine whether the operations of reading and/or writing multi-purpose identifiers, such as DSID, DPID and iAdId identifiers, on the user's terminal requires the prior collection of their consent, it must be determined whether the purposes announced by the company are all exempt from obtaining consent.98. With regard to the information attached to the DSID, the Restricted Committee considers that if this identifier is created for each user account on the servers of the APPLE group, "information" is read on the terminal equipment of the latter to allow the association of the queries made to a

user account (i.e. whether the user searches, downloads, or purchases apps from the App Store) and later assigns that unique user to segments at the within a universe requiring authentication (so-called “authenticated” or “logged-in” universe), in this case the App Store. Even if the main function of this "information" would be to allow the authentication of a user within a logged-in universe - and would be qualified as an essential purpose because it is strictly necessary for the provision of an online communication service to at the express request of the user -, the fact that the information collected thanks to these trackers can be used to allow segmentation for advertising purposes necessarily prevents the said trackers from entering the categories of trackers whose reading is exempt from obtaining consent within the meaning of the aforementioned article 82. The Restricted Committee therefore considers that the company accesses information aimed at maintaining the authenticated connection, for several purposes: on the one hand, authentication and then maintaining the user within the authenticated universe of the App Store and on the other hand, the collection of traces of user activity within the framework of the App Store in order to assign or reassign him to one or more segments which will then be used to send him advertisements personalized to promote mobile applications on the App Store.99. As regards the replacement of information attached to the DSID by the identifiers DPID and iAdId on the user's terminal, the Restricted Committee notes first of all that the reading of the identifiers DPID and iAdId which are stored in the user's terminal equipment and sending them to the company's servers are intended to serve ads for targeted applications based on the user's profile. Therefore, the Restricted Committee considers that these operations pursue an advertising purpose and thus do not have the exclusive purpose of allowing or facilitating communication by electronic means, nor are they strictly necessary for the provision of an online communication service. at the express request of the user, within the meaning of article 82 of the Data Protection Act.100. Next, with regard to the argument that the steps relating to the replacement of information attached to the DSID by the DPID and the iAdId are implemented in order to respect the principles of protection of privacy and that in their absence , the company could link the information relating to the advertisements broadcast to the identity of the user, which would infringe his privacy, the Restricted Committee points out that, in fact, the technical architecture underlying the "Search Ads" service allows in itself to make further processing related to the personalization of ads less intrusive for the data subjects. On the other hand, it considers that, since article 82 of the Data Protection Act applies, it is necessary to comply with the conditions thereof, in particular those relating to the collection of consent prior to any reading operation taking place on the user's terminal equipment, excluding operations related to the operation of electronic communications or strictly necessary for the provision of a service requested by the user. In other

words, the Restricted Committee considers that the fact of implementing other measures to protect privacy from the design stage does not make it possible to circumvent the rule set by article 82 of the Data Protection Act. 101. Therefore, it considers that these operations require that the user has given his prior consent, under the conditions provided for by the provisions of article 82 of the law of January 6, 1978 as amended, as clarified by article 4, paragraph 11, GDPR.102. Secondly, the Restricted Committee notes that the consent of individuals must be unambiguous and that it follows from the "Planet 49" decision of October 1, 2019 of the CJEU that the use of pre-ticked boxes cannot be considered as a clear positive act aimed at giving consent (CJEU, 1 Oct. 2019, C-673/17). Moreover, in the context of the guidelines of September 17, 2020, the Commission took care to specify that "consent must be manifested through a positive action by the person previously informed of the consequences of his choice and having the means of expressing it ".103. In this case, the Restricted Committee notes that it appears from the findings made in the section entitled "Apple Advertising", that the advertising targeting parameters are pre-ticked by default. It considers that by being authorized "by default", advertising targeting processing cannot be considered as having been accepted by a positive act of the users.104. The Restricted Committee also recalls that this step of obtaining consent comes late in the phase of taking control of the phone by the user and that it is optional because it is not integrated into the initialization process of the phone. Also, this step is only accessible after the user has clicked on the "Settings" icon on the iPhone, gone to the "Privacy" menu, and then clicked on the section labeled "Advertising". Apple". It considers that it is difficult for the user to succeed in validly accepting or refusing these operations, insofar as the user who has completed the initialization process for his telephone (a fortiori when the process includes a large number of 'steps as in the present case) may legitimately think that they no longer need to carry out any other configurations before consulting the App Store.105. Finally, the Restricted Committee considers that the company implements data processing on a considerable scale given the preponderant place occupied by the Apple operating system on the French market for mobile operating systems and the proportion use of smartphones by telephone users in France. It also notes that this targeting is based on people's areas of interest and lifestyle and that, therefore, the company's use of browsing and profile data from the App Store to carry out targeting advertising is significant. Therefore, the Restricted Committee considers, in view of the extent of the processing deployed and the imperative need for users to retain control of their data, that they must be put in a position to give their valid consent.106. Consequently, the Restricted Committee considers that ADI is accessing information already stored or read on users' terminals for the purpose of personalizing ads in the App Store without first obtaining their consent, in disregard of the

provisions of Article 82 of the Data Protection Act.D. On the new window intended to collect consent under the new version iOS 15 of the operating system107. The Restricted Committee notes that the new device intended to collect consent under the new iOS 15 version of the operating system is written in French. It notes that the company undertakes to complete the statement "Apple does not track your activities" by March 2023. Finally, it notes that no identifier is no longer used for the purposes of personalizing ads on the App Store before this window is presented to the user.108. Consequently, the Restricted Committee considers that this new window constitutes a mechanism making it possible to obtain prior valid consent to the reading of the aforementioned information and identifiers on the user's terminal, pursuant to article 82 of the law of January 6 1978 modified.109. The Restricted Committee considers that a breach of the obligations arising from Article 82 of the Data Protection Act is constituted for the past on version 14.6 of the operating system since it was the company's responsibility to obtain the consent users prior to the operations of writing and/or reading information on their terminal equipment for the purpose of personalizing ads intended to promote mobile applications on the App Store.110. It notes that, in the context of this procedure, the company has justified having taken measures to comply with the obligations arising from Article 82 of the Data Protection Act, which does not, however, call into question the existence of the breach for past facts.III. On corrective measures and their publicity111. Under the terms of III of article 20 of the Data Protection Act: "When the data controller or its subcontractor does not comply with the obligations resulting from regulation (EU) 2016/679 of April 27, 2016 or from this law , the President of the National Commission for Computing and Liberties may also, if necessary after having sent him the warning provided for in I of this article or, if necessary in addition to a formal notice provided for in II, seize the restricted formation of the commission with a view to the pronouncement, after adversarial procedure, of one or more of the following measures: (…) 7° With the exception of cases where the processing is implemented by the State, an administrative fine not to exceed 10 million euros or, in the case of a company, 2% of the total worldwide annual turnover of the previous financial year, whichever is higher. 5 and 6 of article 83 of regulation (EU) 2016/679 of April 27, 2016, these ceilings are increased, respectively, to 20 million euros and 4% of said turnover. The Restricted Committee takes into account, in determining the amount of the fine, the criteria specified in the same Article 83. "112. Under the terms of Article 83 of the GDPR, as referred to in Article 20, paragraph III, of the Data Protection Act:" 1. Each supervisory authority shall ensure that the administrative fines imposed under this article for breaches of this regulation referred to in paragraphs 4, 5 and 6 are, in each case, effective, proportionate and deterrents.2. Depending on the specific characteristics of each case, administrative fines are imposed in

addition to or instead of the measures referred to in points (a) to (h) and (j) of Article 58(2). In deciding whether to impose an administrative fine and in deciding the amount of the administrative fine, due account shall be taken in each individual case of the following elements: (a) the nature, gravity and the duration of the breach, taking into account the nature, scope or purpose of the processing concerned, as well as the number of data subjects affected and the level of damage they have suffered; b) the fact that the breach has was committed willfully or negligently; c) any action taken by the controller or processor to mitigate the harm suffered by data subjects; d) the degree of liability of the controller or processor, taking into account the technical and organizational measures they have implemented pursuant to Articles 25 and 32; e) any relevant breach previously committed by the controller or processor; f) the degree of cooperation established with the control with a view to remedying the breach and mitigating its possible negative effects; g) the categories of personal data concerned by the breach; h) the manner in which the supervisory authority became aware of the breach, in particular whether and to what extent the controller or processor has notified the breach; (i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor; subcontractor concerned for the same purpose, compliance with these measures; j) the application of codes of conduct approved pursuant to Article 40 or certification mechanisms approved pursuant to Article 42; andany other aggravating or mitigating circumstances applicable to the circumstances of the case, such as financial benefits obtained or losses avoided, directly or indirectly, as a result of the breach. "A. On the imposition of an administrative fine113. In defence, the company considers, primarily, that no violation of article 82 of the Data Protection Act can be blamed on it and, since no fine cannot be pronounced against it. It recalls in this respect that the processing for personalization purposes of ads on the App Store that it implements is carried out either on its servers and is not part of the scope of the investigations. of the CNIL, or on the user's terminal solely for the purposes of "protection of privacy" and therefore falls within the scope of the exemptions provided for in Article 82 of the Data Protection Act.The company considers, in the alternative, that the amount of the fine proposed by the rapporteur is disproportionate and that several criteria provided for in Article 83(2) of the GDPR are ineffective in this case, in particular those referring to the nature, gravity and scope of the treatment and the level of harm suffered by people. She then argues that the window intended to collect consent in the new iOS 15 version of the operating system has always been available in French for users who have selected this language, contrary to what the rapporteur maintained. It further submits that worldwide turnover is not a relevant criterion to be taken into account in deciding the amount of the fine in itself and that its sole function is to prevent the amount retained by the restricted training does not exceed the limit provided for

by the GDPR. She added that the amount proposed by the rapporteur corresponds to […]. Lastly, it notes that the fine proposed by the rapporteur bears no relation to the fines it has already imposed.114. In view of the elements developed above, the Restricted Committee considers that the aforementioned facts, constituting a breach of Article 82 of the Data Protection Act, justify the imposition of an administrative fine against the company ADI , legal person responsible for processing. It recalls that the changes made by the company to the window intended to collect consent in the new iOS 15 version of the operating system since September 2021 have no impact on the imposition of a fine insofar as this is intended to penalize the facts observed during checks concerning the iOS 14.6 version of the iPhone operating system.115. The Restricted Committee recalls that Article 20, paragraph III, of the Data Protection Act gives it jurisdiction to impose various sanctions, in particular an administrative fine, the maximum amount of which may be equivalent to 2% of the total worldwide annual turnover of the previous financial year carried out by the data controller. It adds that the determination of the amount of this fine is assessed in the light of the criteria specified by Article 83 of the GDPR.116. In the present case, the Restricted Committee considers that the breach in question justifies the imposition of an administrative fine on the company for the following reasons.117. First of all, the Restricted Committee notes the seriousness of the breach, insofar as the personalization parameters of the advertisements being pre-checked by default, the company carried out operations to read and/or write information or identifiers on the terminals of users located in France for the purpose of personalizing advertisements without first obtaining their consent and deprived them of the possibility of exercising their choice in accordance with the provisions of the aforementioned article 82.118. The Restricted Committee considers that the seriousness of the breach is accentuated by the fact that this step of obtaining consent occurred late in the phase of handling the telephone by the user and that it was optional because it was not integrated into the process of phone initialization.119. The Restricted Committee observes that the seriousness of the breach must also be assessed with regard to the scope of the read and write operations in question and the number of persons concerned.120. Regarding the scope of read and write operations, the Restricted Committee notes that the Apple App Store is the only official distribution channel for mobile applications on iOS devices for developers, since the company does not allow apps to be downloaded outside of its App Store. People using version iOS 14.6 of the iPhone operating system are therefore dependent on the choices made by ADI with respect to the protection of their privacy.121. With regard to the number of people concerned by the operations of reading and/or writing the aforementioned information and identifiers on their mobile terminal, it appears from the information provided by the company that 27.5 million mobile terminals

equipped with the system of operating have connected to the French App Store using an IP address registered in France between July 5, 2020 and July 5, 2021 (for free or paid downloads, re-downloads or updates). While this number does not mean that 27.5 million users have not consented to the reading and/or writing operations of the aforementioned information and identifiers on their mobile terminal, it reflects the important place occupied by the company on the mobile phone operating system market.122. Next, the Restricted Committee considers that the company ADI, which achieved a worldwide turnover for the year 2021 of approximately […] dollars, or approximately […] euros (according to the current exchange rate), drew of the breach resulted in a definite financial advantage. This is because, as noted earlier, read and/or write operations allow the company to present users, when they search the App Store, with personalized ads promoting apps. The Restricted Committee notes that if the main activity of the company lies in the sale and distribution of APPLE group products in Europe, the personalization of advertisements precisely makes it possible to increase its income. However, by not obtaining the consent of users to the operations of reading and/or writing the aforementioned information and identifiers, the company increases the number of users from whom the personalization of the advertisements will be carried out.123. The Restricted Committee nevertheless notes, as a mitigating circumstance, that the steps relating to the replacement of information attached to the DSID by the DPID and the iAdId are implemented in order to comply with the principles of protection of privacy and that in their absence, the company could link the information relating to the advertisements served to the identity of the user, which would further infringe his privacy.124. It follows from all of the foregoing and from the criteria duly taken into account by the Restricted Committee, in view of the maximum amount incurred established on the basis of 2% of turnover, that it is justified to impose a fine administrative up to 8 million euros.B. Publicity of the decision125. In defence, the company maintains that such a measure would be neither necessary nor proportionate with regard to the alleged breach which it refutes and its compliance under the new consent collection window available under the iOS 15 version of the system. operating.126. The Restricted Committee considers that, given what has been explained above, it is justified to pronounce an additional sanction of publicity. Account is also taken of the preponderant place occupied by the Apple operating system on the French market for mobile operating systems and the proportion of use of smartphones by telephone users in France, the seriousness of the breach and the the interest that this decision represents for informing the public, in determining the duration of its publication. FOR THESE REASONS APPLE DISTRIBUTION INTERNATIONAL an administrative fine in the amount of 8,000,000 (eight million) euros for breach of article 82 of the Data Protection Act; make public, on the CNIL website and on the Légifrance website , its

deliberation, which will no longer identify the company by name at the end of a period of two years from its publication.

Chairman Alexandre LINDEN This decision may be subject to appeal before the Council of State within four months of its notification.