Deliberation SAN-2019-001 of January 21, 2019 National Commission for Computing and Liberties Nature of the deliberation: Sanction Legal status: In force Date of publication on Légifrance: Tuesday January 22, 2019 Deliberation of the restricted committee no. SAN – 2019-001 of 21 January 2019 pronouncing a pecuniary penalty against the company XLThe National Commission for Computing and Liberties, meeting in its restricted formation composed of Mr. Jean-François CARREZ, Chairman, Mr. Alexandre LINDEN, Vice-Chairman, Ms. Dominique CASTERA, Mrs Marie-Hélène MITJAVILE and Mr Maurice RONAI, members; Having regard to Convention No. 108 of the Council of Europe of 28 January 1981 for the protection of individuals with regard to the automatic processing of personal data; Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 relating to the protection of personal data and the free movement of such data; Having regard to Law No. 78-17 of January 6 r 1978 amended relating to data processing, files and freedoms, in particular its articles 45 and following; January 1978 amended relating to data processing, files and freedoms; Having regard to deliberation no. 2013-175 of July 4, 2013 adopting the internal regulations of the National Commission for Data Processing and Freedoms; Having regard to decision no. 2018 -199C of 20 September 2018 from the President of the National Commission for Computing and Liberties to instruct the Secretary General to carry out or have carried out a mission to verify any processing relating to the use of the Android operating system for multifunction mobile including the creation of an account [...]; Having regard to the decision of the President of the National Commission for Computing and Freedoms appointing a rapporteur before the restricted committee, dated October 2, 2018; Having regard to the report by Mr François PELLEGRINI, commissioner rapporteur, of October 22, 2018; Having regard to the written observations submitted by company X on November 22, 2018; Having regard to the observations in response of the commissioner rapporteur of December 7, 2018; Having regard to the observations in response submitted by the company X on January 4, 2019 as well as the oral observations made during the restricted training session; Considering the other documents in the file; Were present at the restricted training session of January 15, 2019: Mr. François PELLEGRINI, commissioner, heard in his report; As representatives of company X.:[…] Mrs. Eve JULLIEN, government commissioner, having made no comments; The company having had the floor last; After having deliberated, has adopted the following decision: Facts and procedure company achieved a turnover of X in 2017. It has more than X. In France, it has an establishment, the company XSince it exists, the company has developed a plurality of services for companies and individuals (e.g. […]). The company also carries out an advertising management activity. In 2016, this operating system had X users in France. On May 25 and 28, 2018, the National

Commission for Computing and Freedoms (hereinafter CNIL or the Commission) was seized of two collective complaints filed pursuant to Article 80 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation, hereinafter GDPR or Regulation) respectively by the association None Of Your Business (hereafter NOYB) and the association La Quadrature du Net (hereafter LQDN). Cumulatively, these complaints include the complaints of 9,974 people. In its complaint, the NOYB association indicates in particular that users of x are required to accept the privacy policy and the general conditions of use of x services and that in the absence of such acceptance, they could not use their terminal. The LQDN association considers that, independently of the terminal used, x does not have valid legal bases to implement the processing of personal data for behavioral analysis and advertising targeting purposes. On June 1, 2018, the CNIL submitted the aforementioned complaints to its European counterparts via the European information exchange system with a view to designating a possible chief authority file in accordance with the provisions of article 56 of the GDPR. Pursuant to decision no. 2018-199C of September 20, 2018 of the President of the Commission, an online check was following September 1 in order to verify the compliance of any processing relating to the use of […], with the law of January 6, 1978 relating to data processing, files and freedoms (hereinafter the Data Protection Act or the law of January 6, 1978) and to the GDPR. Online inspection report no. 2018-199/1 was notified to companies X Y on September 24 and 25, 2018. CNIL on September 28, 2018. For the purpose of investigating these elements, the President of the CNIL appointed, on October 2, 2018, Mr. François PELLEGRINI as rapporteur on the basis of article 47 of the law of January 6, 2018. 1978. At the end of his investigation, the rapporteur notified the X Y companies, on October 22, 2018, of a report detailing the breaches relating to Articles 6, 12 and 13 of the GDPR that he considered constituted in this case. report proposed to the restricted formation of the CNIL to pronounce to the concont re of company X. a pecuniary penalty of 50 million euros, made public. It was also proposed that it be included in a publication, newspaper or medium that the restricted committee would designate. Also attached to the report was a summons to the restricted training session of January 10, 2019. The organization had one month to submit its written observations. By letter of November 7, 2018, the company requested a hearing to the rapporteur, which was not granted by letter dated November 13, 2018. On the same date, the company also made a request for a closed session and postponement of the meeting, to which it was not granted, by letter dated November 15, 2018. On November 22, 2018, the company produced written observations on the report. These observations were the subject of a response from the rapporteur on December 7, 2018. By letter dated December 11, 2018, the company, which had fifteen days from receipt of the

rapporteur's response, requested from the Chairman of the Restricted Committee the postponement of the meeting as well as an extension of the deadline to produce his new observations. The request was accepted by the President of the Restricted Committee on December 13, 2018, who decided, on the one hand, to postpone by two weeks - until January 7 - the deadline for the production of these observations and, on the other hand, to postpone the meeting to January 15, 2019. On January 4, 2019, the company produced new observations in response to those of the rapporteur. All of the observations were reiterated orally by the company and the rapporteur during the the restricted committee of January 15, 2019. II. Reasons for the decision1. On the competence of the CNILL, Article 55 paragraph 1 of the GDPR provides: Each supervisory authority is competent to exercise the missions and powers vested in it in accordance with this regulation on the territory of the Member State to which it belongs. Article 56(1) GDPR provides: Without prejudice to Article 55, the supervisory authority of the main establishment or single establishment of the controller or processor is competent to act as supervisory authority with regard to the cross-border processing carried out by that controller or processor, in accordance with the procedure provided for in Article 60. The company first argues that the CNIL is not competent to conduct this procedure and that it should have forwarded the complaints received to the Irish data protection authority (Data Protection Commission, hereinafter DPC) to which it would be up to […], as lead authority, to deal with these complaints relating to cross-border processing, in accordance with the cooperation procedure established in Article 60 of the GDPR. The company considers that company X must be considered as its main establishment within the European Union for some of the cross-border processing that it implements, and in particular those that are the subject of the complaints received by the CNIL. Consequently, according to her, the data protection authority should be regarded as its lead supervisory authority and be responsible, as such, for processing complaints received by the CNIL. To attest to the fact that company X is its main establishment within the Union, it specifies that this company has been the registered office of X for its European operations since 2003 and that it is the entity in charge of several organizational functions necessary to carry out these operations for the Europe, Middle East and Africa zone (general secretariat, taxation, accounting, internal audit, etc.). It also indicates that the conclusion of all advertising sales contracts with customers based in the European Union is the responsibility of this company. This company employs more than x employees and has, among other things, a dedicated team in charge of managing requests made within the European Union in connection with confidentiality and a person in charge of the protection of life. private. Finally, it specifies that an operational and organizational reorganization is underway with a view to making x the data controller for certain processing of personal data concerning

European nationals. It also considers that the definition of main establishment must be distinguished from that of data controller and that if the European legislator had wanted the notion of main establishment to be interpreted as the place where decisions concerning processing are taken, it would have expressly indicated this. given the cross-border nature of advertising personalization processing, the significant number of x users in Europe and the issues raised in connection with this processing, the cooperation and consistency mechanisms as provided for in Articles 60, 64 and 65 GDPR should have applied. It specifies in particular that the European Data Protection Board (hereinafter EDPS) should have been referred to in the event of doubt about the determination of the lead authority. Finally, the company considers that the informal discussions which may have place between the other European supervisory authorities on this procedure are without legal effect since they took place without his presence.On the quality of main establishment of the company XArticle 4 (16) of the GDPR defines the notion of main establishment as follows: (a) as regards a controller established in more than one Member State, the place of its central administration in the Union, unless the decisions as to the purposes and means of the data processing of a personal nature are taken in another establishment of the controller in the Union and that the latter establishment has the power to enforce these decisions, in which case the establishment having taken the e such decisions is considered the principal establishment . Recital 36 of the GDPR specifies: The main establishment of a controller in the Union should be determined according to objective criteria and should involve the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing within the framework of a stable system. The Restricted Committee considers that it follows from these provisions that, in order to be qualified as a main establishment, the establishment concerned must have decision-making power with regard to the processing of personal data in question. The status of main establishment presupposes the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing. Therefore, the existence of a main establishment is assessed in concrete terms, with regard to objective criteria, and the main establishment cannot automatically correspond to the registered office of the data controller in Europe. The Restricted Committee notes that this analysis is also that adopted by all the European supervisory authorities, as evidenced by the EDPS guidelines of 5 April 2017 concerning the designation of a lead supervisory authority of a controller or a processor (WP244). These indicate that: the central administration is the place where decisions are taken as to the purposes and means of the processing of personal data, and this place has the power to enforce these decisions . The Restricted Committee further notes that these same guidelines indicate that: The general regulations do not authorize the

choice of jurisdiction (forum shopping)(…). Conclusions cannot be based exclusively on statements by the organization in question. It is therefore necessary to assess the decision-making powers available to company X to determine whether it can be qualified as a main establishment. effective services by x in Europe, in particular through the sale of advertising services. However, if these elements attest to this participation, the Restricted Committee considers that they do not allow the qualification of company x as main establishment. The elements provided do not in themselves demonstrate that company x would have had, on the date of the initiation of the proceedings, any decision-making power as to the purposes and means of the processing covered by the confidentiality policy presented at user when creating his account, when configuring his mobile phone under x. These elements only reveal the involvement of this entity in the context of various activities of the company (financial and accounting activities, sale of advertising space, signing of contracts, etc.). The Restricted Committee also notes that company x is not mentioned in the company's Confidentiality Rules dated 25 May 2018 as being the entity where the main decisions are taken as to the purposes and means of the processing covered by the privacy policy presented to the user when creating his account, when configuring his mobile phone under x. It also points out that company x has not appointed a data protection officer who would be in charge of the processing of personal data that it could implement in the European Union. It further notes that operating system x is developed solely by company x. Finally, the Restricted Committee notes that the company itself indicated, by letter dated 3 December 2018 addressed to the DPC, that the transfer responsibility of x. to company x on certain processing of personal data concerning European nationals would be finalized on January 31, 2019. It subsequently specified that it would update its confidentiality rules which will come into effect on January 22, 2019. In view of all of these elements, the Restricted Committee considers that company x cannot be considered as the main establishment of company x. in Europe within the meaning of Article 4 (16) of the GDPR, since it is not established that it has decision-making power as to the processing covered by the privacy policy presented to the user when the creation of his account when configuring his mobile phone under x. In the absence of a main establishment allowing the identification of a lead authority, the CNIL was competent to initiate this procedure and to exercise all of its powers under Article 58 of the GDPR.b) On the application of cooperation and consistency proceduresIn the first place, the company argues that the CNIL should have referred the matter to the EDPS because of the uncertainty as to the identification of the supervisory authority that must act as lead authority. The Restricted Committee considers first of all that the absence of a main establishment of a data controller within the European Union does not by itself generate uncertainty about the i Identification of a supervisory authority that can

act as lead authority. It only follows from this absence of a main establishment that the identification of a lead authority is not necessary, and that the single window mechanism is not intended to apply. The Restricted Committee then notes that the CNIL immediately communicated the complaints received to all the supervisory authorities, via the European information exchange system, with a view to identifying a possible lead authority, in accordance with the provisions of Article 56 of the GDPR. The Restricted Committee notes that, in the context of this procedure, no supervisory authority, nor the Chairman of the Committee, deemed it necessary to seize the EDPS due to uncertainties about the identification of the lead authority or the competence of the CNIL. It also observes that the analysis concluding that the company x. in Europe for the processing referred to in the complaints, and the resulting absence of a lead authority, was shared by the DPC. It thus notes that the DPC publicly affirmed on August 27, 2018 - in an Irish Times press article - that it was not the lead authority for the processing operations which could be implemented by the company. : the Data Protection Commission is not the "primary regulator" of x (nor, in data protection terms, its "lead supervisory authority") [...] x, a US company, is the data controller and x absolutely cannot take advantage of the one-stop-shop mechanism. […]. The current position is that x is subject to control by all European control authorities […]. It therefore does not follow from the investigation that there would have been doubts or divergent points of view within the supervisory authorities such as to require a referral to the EDPS, in accordance with Article 65 of the GDPR. Furthermore, given the guidelines already adopted at European level to guide national authorities in identifying the possible lead authority, there was no new question justifying referral to the EDPS by the CNIL pursuant to Article 64. Considering all of these elements, the Restricted Committee considers that the CNIL was not required to refer the matter to the EDPS with a view to identifying a lead authority. Secondly, if the company maintains that the CNIL should have cooperated in the investigation of the complaints and the appropriate follow-up to them, the Restricted Committee recalls, as previously stated, that the CNIL communicated, upon receipt, complaints to all the supervisory authorities of the European Union, via the European information exchange system, with a view to identifying a possible lead authority. cooperation procedure has indeed been engaged with the supervisory authorities, in accordance with the provisions of Article 56 of the GDPR, initially on the sole issue of identifying the respective powers of these authorities. The Restricted Committee observes that this stage of Dissemination of information and determination of a possible lead authority is a prerequisite for the possible application of the one-stop-shop mechanism provided for in Article 60 of the GDPR. The training then notes that this approach and the resulting exchanges did not lead to the identification of a main establishment or, consequently, a lead authority, no

other obligation of cooperation was subsequently imposed on the CNIL, in particular under Article 60 of the GDPR. Finally, the Restricted Committee recalls that, for the sake of consistency, in accordance with the guidelines set out in Article 63 of the GDPR, the CNIL has informed and consulted its European counterparts on several occasions on the investigations it has carried out, and has taken the utmost account of the guidelines adopted by the EDPS with a view to ensuring uniform application of the Regulation. In view of these elements, the Restricted Committee considers that the cooperation and consistency procedures do not have not been disregarded. Moreover, the Restricted Committee notes that except for express provisions, which is not the case in this case concerning the determination of the lead authority, the au Supervisory authorities are not required to inform data controllers when implementing cooperation actions or to enable them to participate in exchanges between authorities. 2. On the procedureIn the first place, the company maintains that the admissibility of the complaints lodged by the associations None Of Your Business and La Quadrature du Net has not been established. The restricted committee considers the question of the admissibility of the aforementioned complaints. in any event, no influence on the legality of this procedure, referral to the panel not necessarily being subject to receipt of a complaint and which may result from a self-referral by the Commission on the basis findings made by the services of the latter. It recalls that the CNIL's mission is to monitor the application of the regulation and to ensure compliance with it and that it has, to do this, the power to carry out investigations, in accordance with Article 57 1. a) and h) of the GDPR. Moreover, the Restricted Committee notes that Article 80 of the GDPR provides for the possibility for a person to appoint a non-profit association, which has been validly constituted in accordance with the right to a Member State, whose statutory objectives are in the public interest and is active in the field of the protection of the rights and freedoms of data subjects in the context of the protection of personal data to lodge a complaint on their behalf .With regard to LQDN, the Restricted Committee notes that it is a French association created on January 3, 2013. It appears from its statutes that this association has the particular purpose of carrying out actions to ensure the defense of the rights and fundamental freedoms ns the digital space [...] . With regard to NOYB, it notes that it is a non-profit association validly constituted on Austrian territory since 12 June 2017. It appears from its statutes that its purpose is in particular to represent the rights and interests of users in the digital domain (including consumer rights, fundamental privacy rights, data protection, freedom of expression, freedom of information and the fundamental right to an effective remedy). The panel also notes that these two associations received from the persons who seized them a representation mandate under Article 80 of the GDPR.Secondly, the company argues that the proceedings brought against it disregarded its right to a fair trial

as provided for in particular in Article 6 of the Convention for the Protection of Human Rights and Fundamental Freedoms. On this point, it maintains on the one hand, that the report proposing a sanction as well as the the responses provided by the rapporteur to her observations were sent to her only in French and, secondly, that the refusal to extend the time limit opposed to her to produce her first observations limited the time she had to prepare her defence. It also considers that the postponement of the meeting and the additional time which was finally granted to it to produce its second observations were still not sufficient. The Restricted Committee notes first of all that the notification of a sanction report in French responds to the legal obligation set out in article 111-1 of the code of relations between the public and the administration which provides that the use of the French language is prescribed in exchanges between the public and the administration, in accordance the provisions of Law No. 94-665 of August 4, 1994 relating to the use of the French language. In addition, no legal or supranational provision requires the CNIL to translate the documents it produces. Moreover, the company has an establishment on French territory, company x. This company has several hundred employees and has been notified of all the documents relating to the procedure. It also notes that the main documents in support of the procedure (Privacy Rules, Terms of Use, etc.) were the company's own documents, which were also available in English on other media. elements, the Restricted Committee considers that the company had in any event sufficient material and human resources enabling it to translate the documents into English in sufficient time to read them and formulate its observations within the time limit given to it The Restricted Committee then recalls that Article 75 of Decree No. 2005-1309 of October 20, 2005, as amended, provides that the data controller has a period of one month to make observations in response to the report submitted to him. was sent, then of a new deadline of fifteen days following the deadline given to the rapporteur to provide his answer. 2 requests made by the company on December 11, 2018 to obtain an extension of time to produce its observations in response to the information provided by the rapporteur and a postponement of the meeting. This postponement allowed him to benefit from an additional period of fifteen days to produce his second observations compared to the period initially planned and thus prepare his defense for the session of the Restricted Committee. It was also able to present its oral observations on the day of the Restricted Committee session in addition to its written submissions. Finally, the Restricted Committee recalls that the findings of fact made in the context of this procedure essentially related to institutional documents drawn up by the company itself. In view of these elements, the Restricted Committee considers that the rights of defense of company x have been guaranteed.3. On the scope of the investigations In defence, the company first of all argues that the rapporteur has confused operating

system x when these are separate services that implement different processing activities. It indicates in particular that when configuration of their mobile device under x, users have a clear choice whether or not to create an x account and that the Privacy Policy explains to them how x services can be used with or without an x account (e.g. viewing x videos without creating an account etc.). It then argues that the scope of the control chosen by the CNIL - namely the creation of an account x when configuring a new device using the operating system x - is limited in that it represents a case of figure which only concerns 7% of users. Finally, it indicates that the findings were made on an old version of the x operating system. First of all, the restricted training indicates that it does not call into question the existence of separate services, linked respectively to operating system x and to account x, implementing different processing activities. know the course of a user and the documents to which he could have access during the initial configuration of his mobile equipment using the operating system x. This journey included the creation of an account. These facts therefore relate to the processing covered by the privacy policy presented to the user when creating his account when configuring his mobile phone under x. Then, if it is true that the user does have a choice to create an account and has the ability to use some of the company's services without having to create an account, however, she finds that when setting up a device under x, the ability to create an x or to connect to an existing account appears naturally at the start of the configuration process, without any specific action by the user. The user is also invited to create or connect to an account x insofar as when on the Learn More or Skip links available at this device setup step, they are presented with the following information: Your device works best with account x , If you don't have account x, you won't be able to not s perform the following actions […] Enable device protection features . The Restricted Committee thus considers that this path, when creating an account, creates a continuum of use between the processing carried out by the operating system and those carried out through account x, and justifies the scenario retained for the online control. This succession of information and choices presented to the user does not, however, prevent a differentiated analysis, with regard to the legal framework, of the different processing activities in question on the basis of all the facts observed in the context of this scenario. Also, regarding the company's comments that this scenario only affects 7% of users - most users of a device running x logging into a pre-existing account - the restricted training recalls that under the terms of Article 11. I.2 of the Data Protection Act, the CNIL has wide discretion as to the scope of the checks it may undertake. A specific control scenario, such as the one used in this case, can make it possible to make findings reflecting a more general confidentiality policy. Moreover, the Restricted Committee notes that the company indicates in its observations dated December 7, 2018 that: the scope of the processing of personal data that

is carried out for Account holders x when using a device under x is largely similar to the processing that occurs for Account holders […] when they use the x services on a computer or on a device not running under x and that [..] Presenting the same Privacy Policy and Terms of Use helps to ensure consistency and knowledge of users and, to Importantly, serves as a reminder to existing account holders of the nature of data collection and the purposes for which it is being collected. Consequently, users who would configure their mobile under x by associating an already existing account with it find themselves, with regard to the information communicated to them, in a similar situation to users who would create an account. Finally , with regard to the version of the operating system x used to make the findings, the Restricted Committee notes that the argument put forward by the company is irrelevant since it appears from the documents provided by the company that the course of a user is similar in a more recent version of the operating system. Moreover, the Restricted Committee notes that the statistics for the distribution of the use of successive versions of the Android operating system, made available on the official website of the Android developers (https://developer.android.com/about/dashboards/) demonstrate that the version used during the check is among the most used versions (porta statistics nt over a period of one week in October 2018 based on the connection data of terminals having connected to x).4. On the breach of the transparency and information obligationsArticle 12 of the General Data Protection Regulation provides: 1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 as well as to carry out any communication under Articles 15 to 22 and Article 34 with regard to the processing to the data subject in a concise, transparent, comprehensible and easily accessible manner, in clear and simple terms, in particular for any information intended specifically for a child. Information is provided in writing or by other means including, where appropriate, electronically. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is demonstrated by other means. 1 of Article 13 of the same text provides that: When personal data relating to a data subject are collected from this person, the data controller shall provide him, at the time the data in question is obtained, with all the following information: the identity and contact details of the controller and, where applicable, of the controller's representative; where applicable, the contact details of the data protection officer; the purposes of the processing for which the data are intended data as well as the legal basis for the processing; where the processing is based on Article 6(1)(f), the legitimate interests pursued by the controller or by a third party; the recipients or categories of recipients personal data, if any; and where applicable, the fact that the controller intends to transfer personal data to a third country or to an international organization, and the existence or absence of an adequacy decision given by the

Commission or, in the case of transfers referred to in Article 46 or 47, or in the second subparagraph of Article 49(1), a reference to the appropriate or adapted guarantees and the means of obtaining a copy or where they were made available; […] . The rapporteur considers that the information provided to users by the company does not meet the objectives of accessibility, clarity and understanding set by article 12 and that certain information made compulsory by article 13 is not provided to users. In defence, the company considers that the information it disseminates to its users meets the requirements of articles 12 and 13 of the GDPR. It considers first of all that the document entitled Rules of confidentiality and conditions of use, accessible during the creation of an account, constitutes first-level information in accordance with the EDPS guidelines on transparency within the meaning of EU Regulation 2016/679 (WP260) of 25 May 2018. It specifies that this document provides a good overview of the processing implemented and that the mention of the legal basis of this processing does not have to appear in this first level of information. Information regarding the retention period of the data can be found in the section Exporting and deleting your information in the Privacy Policy. The company then argues that the information of persons must, with regard to Articles 12 and 13 of the Regulation, be assessed in a global manner. As such, it explains that the information it provides also operates, in addition to the documents entitled Privacy Policy and Terms of Use, Privacy Policy and Terms of Use, through several other methods. She explains that additional information messages may appear when creating an account under each of the privacy settings. In addition, an electronic message is sent to the user at the time of the creation of his account indicating in particular that: You can at any time modify the confidentiality and security parameters of your account x, create reminders to remember to check your privacy settings or verify your security settings. This electronic message contains clickable links referring to various configuration tools. These other control tools, which are made available to the user after the creation of his account from the account management interface include For example, a tool called x that allows users to choose privacy settings that are right for them, including personalized ads, location history, web activity and apps. before a tool x which allows users to have an overview of the use they make of the services offered by x such as xx.Finally, the company recalls that when a user clicked on Create an account without you have disabled the personalized ads settings, an account creation confirmation pop-up window will appear to remind you that the account is configured to include personalized ads features ization. The company indicates that the user journey is thus configured to slow down the progress of users who would not have spontaneously chosen more protective settings for privacy. company in its user information policy, in the sense of greater transparency and greater control over their data expected by them. For the following reasons, however, it considers

that the requirements of the GDPR, the implementation of which must be assessed in the light of the concrete scope of the processing of personal data in question, have not been complied with. the Restricted Committee recalls that pursuant to the provisions of Article 12 of the Rules, information must be provided in an easily accessible manner . This accessibility requirement is informed by the Transparency Guidelines, in which the EDPS considered that A key aspect of the principle of transparency highlighted in these provisions is that the data subject should be able to determine at the advances what the scope and consequences of the processing encompass in order not to be caught unawares at a later stage as to how his personal data has been used. […] More particularly, with regard to complex, technical or unforeseen data processing, the G29 position is that data controllers should […] define separately and clearly the main consequences of the processing: in other words, what effect the specific processing described in a privacy statement or notice will actually have on the data subject. The Restricted Committee also recalls that the accessibility obligation set out in Article 12 is partly based on the ergonomic choices made by the controller. In this case, the Restricted Committee notes that the general architecture of the information chosen by the company does not allow compliance with the obligations of the Regulations. Indeed, the information that must be communicated to people pursuant to Article 13 is excessively scattered in several documents: Privacy Policy and Terms of Use, displayed during account creation, then Terms of Use and Rules of confidentiality which are accessible in a second time by means of clickable links appearing on the first document. These various documents include buttons and links that must be activated to find additional information. Such an ergonomic choice leads to a fragmentation of information, thus forcing the user to multiply the clicks necessary to access the various documents. They must then carefully review a large amount of information before they can identify the relevant paragraph(s). The work provided by the user does not stop there, however, since he will still have to cross-check and compare the information collected in order to understand what data is collected according to the different settings he may have chosen. The Restricted Committee notes that, given this architecture, some information is difficult to find. documentary resources. First, he must read the general Privacy Policy and Terms of Use document, then click on the More options button and then on the Find out more link to display the Ad Personalization page. He will thus have access to an initial description of the processing relating to the personalization of advertising which turns out to be incomplete. To complete the information relating to the data processed within the framework of this purpose, the user must also consult in its entirety the section offering personalized services contained in the document Confidentiality rules, itself accessible from the general document Confidentiality rules and terms of use. Similarly, with regard to the processing of

geolocation data, the Restricted Committee notes that the same path devoid of any intuitive character is required of the user with regard to information relating to geolocation data. He will have to complete the following steps: Consult the Privacy Policy and Terms of Use , click on More options then on the Find out more link to display the Position History page and read the text displayed . However, this text only constitutes a short description of the processing, the user must, to access the rest of the information, return to the Privacy Policy document and consult the Information relating to your geographical position section. The information will still not be complete since this section contains several clickable links relating to the different sources used to geolocate it. In the two cases described, five actions are necessary for the user to access information relating to personalization announcements and six with regard to geolocation. The Restricted Committee also notes that if the user wishes to have information on the retention periods of his personal data, he must first consult the Rules of confidentiality which can be found in the main document, then go to the section entitled Export and delete your information and finally click on the hypertext link click here contained in a general paragraph on retention periods. It is therefore only after four clicks that the user accesses this information. The Restricted Committee notes moreover that the title chosen by the company to Export and delete your information does not easily allow the user to understand that it is a section allowing access to information relating to retention periods. . Therefore, the Restricted Committee considers in this case that the multiplication of necessary actions, combined with a choice of non-explicit titles does not meet the requirements of transparency and accessibility of information. All of these elements result in an overall lack of accessibility of the information provided by the company in the context of the processing in question. Secondly, the Restricted Committee considers that the clear and understandable nature of the information provided, required by the 12 of the GDPR, must be assessed taking into account the nature of each processing operation in question and its concrete impact on the persons concerned. Beforehand, it is essential to emphasize that the data processing operations implemented by the controller processing are particularly massive and intrusive. The data collected by x come from extremely varied sources. This data is collected both from the use of the telephone, the use of company services, such as the messaging service x or the platform of x, but also from the data generated by the activity users when they visit third-party sites using the services x thanks in particular to the cookies x deposited on these sites. As such, the Privacy Rules reveal that at least twenty services offered by the company are likely to be involved in the processing, which may concern data such as web browsing history, application usage history, data stored locally on the equipment (such as address books), geolocation of the equipment, etc Therefore, a large amount of data is processed within the framework of these services via or

in connection with the x operating system. It appears from the investigation of the file that in addition to data from external sources, the company processes at least three categories of data: data produced by the person (for example, name, password, telephone number, email address, means of payment, content created, imported or received, such as writings, photos or videos); data generated by its activity (for example, IP address, unique identifiers of the user, mobile network data, data related to wireless networks and Bluetooth devices, timestamp of actions performed, geolocation data, technical data of devices used including data relating to sensors (accelerometer, etc.), videos viewed, searches performed, browsing history, purchases, applications used , e c.t. data derived or inferred from data provided by that person or their activity. Regarding this category, the Privacy Rules list a number of purposes that can only be accomplished by generating data from the other two categories of data. Thus, the personalization of the advertisements that the company carries out requires inferring the centers of interest of the users from their activity in order to be able to propose these to the advertisers. Similarly, the purposes of providing personalized content, research and recommendations require inferring new information from that declared, produced or generated by the person's activity. of data processed makes it possible to characterize in itself the massive and intrusive nature of the processing carried out, the very nature of some of the data described, such as geolocation data or the content consulted, reinforces this observation. Considered in isolation, the collection of each of these data is likely to reveal with a high degree of precision many of the most intimate aspects of people's lives, including their lifestyle, their tastes, their contacts, their opinions or even their displacements. The result of the combination of these data considerably reinforces the massive and intrusive nature of the processing in question. Consequently, it is in the light of the particular characteristics of this processing of personal data which have just been recalled that the clear and understandable nature, within the meaning of Article 12 of the GDPR, of the information provided for in Article 13 of the Regulation, must be assessed. The Restricted Committee considers that these requirements have not been met in this case. In concrete terms, the Restricted Committee notes that the information provided by the company does not allow users to sufficiently understand the specific consequences of processing for them. , the purposes announced in the various documents are thus described: to offer personalized services in terms of content and advertisements, to ensure the security of products and services, to provide and develop services, etc. . They are too generic with regard to the scope of the processing implemented and their consequences. This is also the case when users are told too vaguely: The information we collect is used to improve the services offered to all our users. […] The information we collect and how we use it depends on how you use our services and how you manage your privacy settings. The Restricted Committee

therefore notes that the description of the purposes pursued does not allow users to measure the extent of the processing and the degree of intrusion into their private life that they are likely to carry out. It considers, in particular, that such information is not provided in a clear manner, nor at the first level of information provided to users by means, in this case, of the document entitled Rules of confidentiality and conditions of use. , nor in the other levels of information offered by the company. The Restricted Committee also notes that the description of the data collected, which could be such as to clarify the scope of these purposes and to prevent the user from being caught later in the lacking as to how its data has been used and combined, is particularly imprecise and incomplete, both in the analysis of the first level of information and that of the other documents provided. Thus, the document Rules of confidentiality and conditions of use as well as the document entitled Privacy Policy specify: This may be more complex information (…), such as the advertisements you find most useful, the people that interest you the most on the web or YouTube videos that you are likely to like. In view of the foregoing, the Restricted Committee considers that the user is not in a position, in particular by reading the first level of information presented to him in the Rules of confidentiality and conditions of use, to measure the impact of the main processing operations on his private life. Although it notes that exhaustive information, from the first level, would be counterproductive and would not respect the requirement of transparency, it considers that this should contain terms such as to objectify the number and scope of processing implemented. It also considers that it would be possible, through other types of presentation methods adapted to data combination services, to provide, from the stage of the Confidentiality Rules, an overview of the characteristics of this combination according to the purposes pursued. The finding of the lack of clarity and comprehensibility must also be made with regard to the mention of the legal basis of the processing of personalization of advertising. Indeed, the company first states in the Privacy Policy: We ask your permission to process your information for specific purposes, and you are free to withdraw your consent at any time. For example, we ask your permission to provide you with personalized services, such as ads […]. The legal basis used here therefore appears to be consent. However, the company further adds that it is based on legitimate interest, in particular to carry out marketing actions with a view to making our services known to users and above all to use advertising in order to make a large number of our services available free of charge. for users. The Restricted Committee underlines that if before it, the company indicated that the only legal basis on which the processing relating to personalized advertising is based is consent, it appears from the instruction that this clarification is not brought to the attention of the users. The formulations recalled above do not allow the latter to clearly measure the distinction between properly

personalized advertising, from the combination of multiple data relating to the user, which is based, according to the company's statements, on the consent , other forms of targeting using e.g. browsing context, based on legitimate interest. The Restricted Committee underlines the particular importance of the requirement of clarity with regard to these processing operations, given their place in the processing operations carried out by society and their impact on people in the digital economy. With regard to information relating to retention periods, the Restricted Committee notes that the page How the information collected by x is retained comprises four categories: Information retained until you delete it; Information with an expiry date; Information retained until your account is deleted x; Information retained for long periods of time for specific reasons. However, it notes that with regard to the last category, only very general explanations on the purpose of this storage are provided and no precise duration or the criteria used to determine this duration are indicated. However, this information is among those that must be provided to persons pursuant to a) of 2°2 of Article 13 of the Regulation. Finally, if the company claims that multiple information tools are made available to users at the same time and after the creation of their account, the Restricted Committee notes that these methods do not make it possible to achieve the requirements of transparency and information resulting from Articles 12 and 13 of the GDPR. First of all, the Restricted Committee notes that the tools the company refers to do contribute, to some extent, to the objective of transparency throughout the life of the account and the use of x's services. However, the Restricted Committee considers that they do not participate sufficiently in the information provided for by Article 13, which must occur at the time the data in question is obtained . As recalled by the EDPS Transparency Guidelines, Article 13 indicates the information to be provided to data subjects from the start of the processing cycle . If data other than that strictly necessary for creating the account is collected throughout the life of the account, such as browsing history or purchases, the moment of its creation marks the user's entry into the ecosystem of services x, whose particularly massive and intrusive nature of the processing was recalled above. This step marks the beginning of a multitude of processing operations: collection, combination, analysis, etc. Consequently, insofar as the process of creating the account is essential in understanding the processing operations and their impact and where the proposed user experience itself invites the person concerned to focus their attention in particular at this stage, the information provided for in article 13 of the Regulation which occurs at this time must, by itself, be sufficient with regard to the requirements resulting from this provision as well as from article 12 of the same regulation. up arising at the time of the creation of the account that the electronic message sent upon creation of the account only contains summary or very targeted information on the processing implemented and cannot allow the prior information to be regarded as

sufficient. The text of the pop-up window does indeed say This account x is configured to include personalization features (such as recommendations and personalized ads) that are have based on the information registered in your account. The electronic message indicates the main functionalities of the account […] and the existence of control tools. With regard to tool x, this essentially allows the user to configure the information collected such as the browsing history or places visited. Finally, the x consists of an information panel grouping for each service […] an overview of the account holder's usage habits. electronic message mentioned above, only after the account creation stage, which is however essential for the information of the users as it has been said. In addition, although their existence and interest are brought to the attention of users, they presuppose an active approach and initiative on the part of them. For these reasons, these tools do not make it possible to consider that sufficient information has been provided for the application of Article 13 of the Regulation. With regard to all of these elements, the Restricted Committee considers that a breach of the obligations of transparency and information as provided for by Articles 12 and 13 of the Regulation is characterized.5. On the breach of the obligation to have a legal basis for the processing carried out Article 6 of the GDPR provides that: The processing is lawful only if, and insofar as, at least one of the following conditions is fulfilled: the data subject has consented to the processing of his or her personal data for one or more specific purposes; the processing is necessary for the performance of a contract to which the data subject is party or for the performance of pre-contractual measures taken at the request thereof; the processing is necessary for compliance with a legal obligation to which the controller is subject; the processing is necessary to safeguard the vital interests of the data subject or of another natural person; processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; the processing is necessary for the purposes of the ts pursued by the controller or by a third party, unless the interests or fundamental rights and freedoms of the data subject which require protection of personal data prevail, in particular where the data subject is a child. The company was criticized for not validly obtaining people's consent for advertising personalization processing. It was also considered that the company could not claim a legitimate interest for this same processing. In defence, the company specifies that it relies solely on consent for advertising personalization processing. Article 4 (11) of the aforementioned Regulation specifies what is meant by consent: any expression of will, free, specific, informed and unambiguous by which the person concerned accepts, by a declaration or by a clear positive act, that personal data concerning it are subject to processing. Article 7 of the same text provides the conditions applicable to it: 1. In cases where the processing is based on consent, the controller is able to demonstrate that the person

concerned has given his consent to the processing of data of a personal nature concerning her.2. If the consent of the data subject is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a form which clearly distinguishes it from these other matters, in a comprehensible and easily accessible form. , and formulated in clear and simple terms. No part of this statement that violates these rules is binding.3. The data subject has the right to withdraw consent at any time. Withdrawal of consent does not affect the lawfulness of processing based on consent made prior to such withdrawal. The person concerned is informed of this before giving his consent. Withdrawing is as easy as giving consent.4. When determining whether consent is freely given, utmost account should be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional . First, the company claims that users' consent is informed. It believes that simple and clear information is presented to the user when creating an account and allows him to be aware of how the company uses the data for advertising personalization purposes. The company refers in particular to the summary entitled Privacy Policy and Terms of Use, to the sections dedicated to the personalization of advertisements contained in the Privacy Policy as well as to the additional information message entitled Personalization of advertising appearing in the options of account creation settings. Secondly, the company claims that users' consent is specific and unambiguous. In particular, it argues that when setting up the account, the user has the possibility of making a choice regarding personalization of advertising. She considers that this possibility allows her to express her consent to the use of her data independently of the other choices that she may express with regard to other purposes relating to the processing associated with account x. She also considers that the terms of collection of consent for the purpose of personalizing the ads it sets up comply with the recommendations of the CNIL of December 5, 2013 regarding cookies. In particular, it specifies that succinct information is available on the personalization of ads followed by an "I accept" button (the Privacy Policy and the Terms of Use), preceded by a "more options" button which gives users the possibility of deactivating several processing operations, including for the purpose of personalizing advertisements. to all purposes via an accept all button. Finally, it considers that explicit consent for the processing of data for the purposes of personalizing advertising, within the meaning of a) of 2 of Article 9 of the GDPR, could not be required since it is not does not act on sensitive data.As regards the enlightened nature Beforehand, the Restricted Committee specifies that this enlightened nature must be examined in the light of the previous developments concerning the lack of transparency and information of users when creating their account . It considers that the breaches previously identified necessarily have an impact on the information provided to users to ensure the informed

nature of the consent. The restricted committee indicates that the EDPS guidelines of 10 April 2018 on consent within the meaning of the 2016 /679 (WP250) specify: the controller must ensure that consent is provided on the basis of information that allows data subjects to easily identify who is the data controller and to understand what they are consenting to. [It] must clearly describe the purpose of the data processing for which consent is sought. These guidelines also specify that: For consent to be informed, it is necessary to inform the person concerned of certain crucial elements in order to make a choice. [..] At least the following information is necessary in order to obtain valid consent: the identity of the data controller, the purpose of each of the processing operations for which consent is sought, the (types of) data collected and used, the existence of the right to withdraw consent, information about the use of data for automated decision-making [..] and information about possible risks related to the transmission of data due to the lack of decision suitability and appropriate safeguards […] . As it was able to note with respect to the breach of the obligations of transparency and information, the Restricted Committee considers that the information on the processing of personalization of advertising is excessively disseminated in separate documents and that it is not, as such, not easily accessible. In this respect, the restricted training refers to the previous developments on the multiple actions that must be taken by a user who wishes to be aware of the information available on the processing related to the personalization of advertising. In addition, as was also noted in As a result of the breach of the transparency obligations, the information provided is not sufficiently clear and understandable in that it is difficult for a user to have an overall understanding of the processing operations to which he may be subject and their scope. By way of illustration, the information disseminated in the Personalization of advertisements section, accessible from the Privacy policy and terms of use document via the More options button, contains the following statement: x can present you with advertisements depending on of your activity within x services (in search or on x for example, as well as on websites and applications pa x) . The Restricted Committee notes that it is not possible to learn, for example through clickable links, of the services, sites and application of x to which the company refers. Therefore, the user is not able to understand the advertising personalization processing to which they are subject, as well as their scope, even though this processing involves a plurality of services (for example: […]) and the processing of a large number of personal data. Users are not able to have a fair perception of the nature and volume of the data collected. In view of these elements, the Restricted Committee considers that the consent of users for advertising personalization processing does not is not sufficiently informed.As regards the specific and unequivocal nature of consentRecital 32 of the Regulation provides that: Consent must be given by a clear positive act by which the data subject manifests in a free, specific,

informed and unequivocal manner his or her agreement to the processing of personal data concerning him […]. There can therefore be no consent in the event of silence, boxes checked by default or inactivity. Recital 43 of the GDPR specifies that: Consent is presumed not to have been freely given if separate consent cannot be given to different personal data processing operations although this is appropriate in the particular case. The EDPS Guidelines on consent mentioned above specify that: In order to comply with the specific nature of consent, the controller must ensure: […] (ii) the detailed nature of requests for consent […] This means that a A controller that seeks consent for various specific purposes should provide separate consent for each purpose so that users can provide specific consent for specific purposes. In the present case, the Restricted Committee notes that when the user creates an account, he has the possibility of modifying some of the parameters associated with the account. To access these settings, the user must click on the more options button, present before the Create an account button. The Restricted Committee also notes that the personalization settings of the account, which contain the choice regarding the display of personalized ads, are pre-ticked by default, which translates, unless otherwise specified, the user's agreement to the processing of its data for the purposes mentioned (e.g. search history x, display of personalized ads, etc.). The user has the possibility of unchecking these parameters if he does not want these processing operations to be implemented. The Restricted Committee observes that, when the account is created, if the user does not click on the more button options in order to set up their account, they must check the boxes I accept the terms of use of x and I accept that my information will be used as described above and detailed in the confidentiality rules. Subsequently, he must press the Create an account button. A pop-up window appears titled Simple Confirmation which contains the following text This account x is configured to include personalization features (such as recommendations and personalized ads), which are based on information stored in your account. To change your personalization settings and the information saved in your account, select More options. If he does not click on More options , the user must then select the Confirm button to finalize the creation of the account. In view of the above, the Restricted Committee notes that if the user has the possibility of modifying the configuration of the parameters of his account prior to its creation, a positive action on his part is necessary to access the possibilities of setting up the account. Thus, the user can completely create his account, and accept the processing linked to it, in particular the processing of personalization of advertising, without clicking on More options . Consequently, the user's consent is not, in this case, validly collected insofar as it is not given through a positive act by which the person specifically and distinctly consents to the processing. of its data for the purpose of personalizing advertising in relation to other processing purposes.

The restricted formation further considers that the actions by which the user proceeds to create his account - by checking the boxes I accept the conditions of use of x and I accept that my information will be used as described below above and detailed in the privacy policy, then selecting Create an account - cannot be considered as an expression of valid consent. The specific character of the consent is not respected since the user, by these actions, accepts all the processing of personal data implemented by the company, including those of personalization of advertising. Moreover, the Restricted Committee notes that when he clicks on More options to access the configuration of his account settings, these, and in particular the one relating to the display of personalized ads, are all pre-checked by default . Also, the possibility left to users to configure their account does not translate either, in this case, into a positive act aimed at obtaining consent, but into an action aimed at allowing opposition to processing. The Restricted Committee finally notes that this analysis is corroborated by the G29 guidelines on consent which specify that: A data controller must also be aware that consent cannot be obtained by means of the same action as when a data subject accepts a contract or the terms and conditions of a service. [...] The GDPR does not allow controllers to offer default checked boxes or opt-out options that require action by the data subject to signal opt-out (e.g. opt-out boxes). The Restricted Committee observes in this respect that, while certain user paths may include a functionality allowing the user to consent in a shared manner to the processing of his data for various similar purposes, this facility can only be considered as compliant if the various purposes of processing were presented to him separately beforehand and that he was able to give specific consent for each purpose, by a clear positive act, the boxes not being pre-ticked. For this type of user journey to be considered compliant, the possibility of giving specific consent for each purpose must be offered to people before the possibility of accepting everything, or refusing everything, without them having to do anything. particular action to access it, such as clicking on more options. In view of the foregoing, the restricted training considers that this type of user journey offers guarantees different from those proposed in this case, this journey allowing the user to consent specifically and distinctly to the processing of his data for a specific purpose. , by a clear positive act, and this possibility being offered to him immediately and prior to the functionality to accept everything . Therefore, in this case, being authorized and masked by default, advertising personalization processing cannot be considered as having been accepted by the user by a specific and unequivocal positive act. Secondly, if the company maintains that the procedures for obtaining consent for the purpose of personalizing the ads that it puts in place comply with the recommendations of the CNIL of December 5, 2013 in terms of cookies, the Restricted Committee recalls that the rules specifically applicable in terms of cookies related to operations relating to targeted advertising

are set by the separate provisions of Article 32-II of the Data Protection Act, resulting from the transposition of the ePrivacy Directive of July 12, 2002 (amended by Directive 2009/136/EC). The invocation of the recommendation of December 5, 2013 is therefore, and in any event, ineffective. of consent which would be more protective than that imposed by the GDPR and which would be, wrongly, defined with regard to the criteria imposed for the collection of consent applicable to the processing of so-called sensitive personal data. The Restricted Committee notes that the terms and conditions for expressing consent have been specified and defined by Article 4 (11) of the Rules, which indicates that consent is understood to mean: any expression of will, free, specific, informed and unequivocal by which the data subject accepts, by a declaration or by a clear affirmative act, that personal data relating to him or her may be processed. These same methods of expressing consent apply in the same way, whether the consent is obtained, under Article 6 of the GDPR, for the implementation of processing for a specific purpose, or whether it be collected, pursuant to Article 9 of the GDPR, to lift the prohibition in principle imposed on the processing of so-called sensitive personal data. Consequently, in order to be considered valid, the consent obtained must be a specific, informed and unequivocal expression of will which, as the Restricted Committee has previously noted, is not the case in this case. all of these elements, the Restricted Committee considers that the consent on which the company relies for advertising personalization processing is not validly obtained.III.On penalties and advertisingArticle 45-III 7° of the law of January 6, 1978 provides: When the data controller or its subcontractor does not comply with the obligations resulting from regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 mentioned above 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. In the cases mentioned in 5 and 6 of Article 83 of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 mentioned above, 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. The company considers that an administrative fine of 50 million euros is disproportionate. It notes that a formal notice would have allowed it to take steps to bring it into compliance and that it does not appear that the direct imposition of an

administrative fine constitutes the most appropriate corrective measure. It also considers that the criteria set out in Article 83 of the GDPR have not all been taken into account in the assessment of the proposed fine. On this point, it refers in particular to the impossibility of taking corrective measures due to the absence of prior formal notice. people who configure a device under the operating system x per day, only 5,000 people create an account. First of all, the Restricted Committee notes that under the aforementioned Article 45 from Law No. 493 of June 20, 2018, the President of the CNIL has the opportunity to prosecute and can therefore choose, depending on the circumstances of the case, the follow-up to be taken to the investigations by closing a file, by issuing a formal notice or by contacting the restricted committee with a view to issuing one or more corrective measures, without it being for the latter to decide on the direction chosen by the President. The Restricted Committee, thus seized, is then fully competent to rule on the materiality and qualification of the facts, then to assess whether the shortcomings that it would have characterized justify, in its very principle, the pronouncement of one of the corrective measures. mentioned in III of article 45 of the law of January 6, 1978 and, finally, to rule on the amount of a possible fine. taken with regard to a set of criteria provided for by a text, must take into account all of these criteria, it is not required in the reasons for its decision to rule on each of them but may be limited to mention those that it deems relevant and the corresponding factual elements. ity for the following reasons. Firstly, the Restricted Committee wishes to underline the particular nature of the breaches noted with regard to the lawfulness of the processing and the obligations of transparency and information. Indeed, Article 6 of the GDPR - which exhaustively defines the cases of lawfulness of processing - is a central provision for the protection of personal data in that it only allows the implementation of processing if the one of the six listed conditions is met. The obligations of transparency and information are also essential in that they condition the exercise of the rights of individuals and therefore allow them to maintain control over their data. In this respect, both Article 6 and Articles 12 and 13 are among the provisions whose disregard is the most severely sanctioned in 5. of Article 83 of the GDPR. The Restricted Committee thus considers that the obligations provided for in terms of transparency and legal bases are fundamental guarantees allowing people to keep control of their data. The lack of knowledge of these essential obligations therefore appears particularly serious, because of their very nature. Secondly, the Restricted Committee notes that the shortcomings retained persist to this day and are continuous violations of the Rules. This is neither a one-off disregard of the company's obligations, nor a habitual violation to which the data controller would have put an end spontaneously since the referral to the restricted committee.Thirdly, the seriousness of the violations must be assessed with regard in particular to the purpose of the processing, its scope and the number of people

concerned. directly to only 7% of its users, the number of people thus concerned is, in itself, particularly important. It also recalls that users who configure their mobile under x by associating an already existing account with it find themselves, with regard to the documents communicated to them and therefore the breaches of the Regulations, in a situation similar to those creating for the first an account, which the company did not dispute in its letter of December 7, 2018. In addition, the Restricted Committee recalls that the company implements data processing on a considerable scale given the preponderance that is operating system x on the French market for mobile operating systems and the proportion of use of smartphones by telephone users in France. Thus, the data of millions of users are processed by the company in this context. The processing covered by the privacy policy presented to the user when creating his account - when configuring his mobile phone under x - also appear to be of considerable scope in view of the number of services involved - at least twenty - and the variety of data processed via or in connection with the x operating system. In addition to the data provided by the user himself during the creation of the account and the use of the operating system, the restricted training recalls that a multitude of data resulting from his activity is also generated such as the history web browsing, application usage history, geolocation of equipment, purchases, etc. Similarly, data is deduced from information provided by the person concerned or his activity, in particular in the context of the personalization of advertisements. It is therefore a lot of information that is particularly enlightening on the lifestyle of people, their opinions and social interactions. Consequently, the data processed by the company closely affects their identity and their privacy. In addition, the Restricted Committee notes that multiple technological processes are used by the company to combine and analyze data from different services, applications or sources. external. They undeniably have a multiplier effect as to the precise knowledge that the company has of its users. Consequently, the Restricted Committee considers that the company has operations of combinations with almost unlimited potential allowing a massive and intrusive processing of user data. Given the scope of data processing - in particular that of personalization of advertising - and the number of people concerned, the Restricted Committee emphasizes that the shortcomings previously identified are particularly serious. A lack of transparency concerning this extensive processing, as well as the absence of valid consent from users to the processing of personalization of advertising constitute substantial breaches of the protection of their privacy and go against the current of legitimate aspirations. people wishing to retain control of their data. In this respect, the strengthening of people's rights is one of the major focuses of the Regulation. The European legislator recalls that the rapid evolution of technologies and globalization have created new challenges for the protection of personal data. The scale of the collection and sharing of

personal data has increased significantly. Technologies allow both private companies and public authorities to use personal data as never before in the course of their activities (…) Technologies have transformed both the economy and social relations (recital 6) . It thus stresses that these developments require a solid data protection framework (…) accompanied by rigorous application of the rules, because it is important to create the confidence which will allow the digital economy to develop throughout the internal market. . Individuals should have control over their personal data. (recital 7). Finally, the European legislator regrets that Directive 95/46/EC has not made it possible to avoid the feeling, widespread among the public, that significant risks for the protection of natural persons remain, in particular with regard to the online environment. (recital 9). The Restricted Committee considers, therefore, in view of the extent of the processing deployed and the imperative need for users to maintain control of their data, that they must be put in a position to be sufficiently informed of the scope of the processing implemented and to validly consent to it, except to deprive basic trust in the digital ecosystem. , in particular the place of the processing of user data for advertising purposes via the operating system x. Given the benefits it derives from this processing, the company must pay particular attention to the responsibility incumbent upon it under the GDPR in their implementation. duly taken into account by the Restricted Committee, in view of the maximum amount incurred established on the basis of 4% of the turnover indicated in point 2 of this decision, that a financial penalty is justified in the amount of 50 million euros , as well as an additional sanction of publicity for the same reasons. Account is also taken of the preponderant place occupied by the company on the operating systems market, the seriousness of the breaches and the interest represented by this decision for the information of the public, in the determination of the duration of its publication. on pecuniary in the amount of 50 (fifty) million euros; to address this decision to company x with a view to the execution of this decision; to make its deliberation public, on the CNIL website and on the Légifrance site, which will be anonymized at the end of a period of two years from its publication.The PresidentJean-François CARREZThis decision may be appealed to the Council of State within four months from its notification.