Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC.

The Commission Nationale de l'Informatique et des Libertés (French Data Protection Authority), meeting under its Restricted Committee, comprised of Mr. Jean-François CARREZ, Chairman, Mr. Alexandre LINDEN, Vice-Chairman, Ms. Dominique CASTERA, Ms. Marie-Hélène MITJAVILE et Ms. 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 automatic processing of personal data;

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data;

Having regard to amended Act no. 78-17 of 6 January 1978 on information technology, data files, and civil liberties, notably Articles 45 et seq.;

Having regard to Decree no. 2005-1309 of 20 October 2005, amended, implementing Act no. 78-17 of 6 January 1978 on information technology, data files and civil liberties;

Having regard to Deliberation no. 2013-175 of 4 July 2013 on the adoption of Commission Nationale de l'Informatique et des Libertés' internal regulations;

Having regard to Decision no. 2018-199C of 20 September 2018 of the Chair of the Commission Nationale de l'Informatique et des Libertés to entrust the secretary-general with carrying out a verification mission on all processing relating to the use of an Android operating system on multifunction mobiles including the creation of a Google account, or having such verification mission carried out;

Having regard to the Decision of the Chair of the Commission Nationale de l'Informatique et des Libertés designating a rapporteur before the Restricted Committee, dated 2 January 2018;

Having regard to the report of Mr. François PELLEGRINI, Rapporteur commissioner, of 22 October 2018;

Having regard to the written submissions from Google LLC. on 22 November 2018;

Having regard to the submissions in response from the Rapporteur commissioner of 7 December 2018;

Having regard to the submissions in response from Google LLC. on 4 January 2019 as well as the oral observations made during the Restricted Committee session;

Having regard to the other items in the case file;

The following were present during the Restricted Committee session of 15 January 2019:

- Mr François PELLEGRINI, commissioner, his report having been read;
- As representatives of Google LLC.:
  - […]

- As counsel to Google LLC.:
  - […]

Ms. Eve JULLIEN, Government Commissioner, having not made any submissions;

The company addressing the Committee last;

After having deliberated, adopted the following decision:

I. Facts and proceedings

1. Founded in 1998, Google LLC. (hereinafter referred to as "Google" or "the company") is a limited liability company under American law, whose registered office is located at Moutain View, in California (United States).

2. A fully-owned subsidiary of ALPHABET since 2015, the company achieved a turnover of 109.7 billion dollars (approximately 96 billion euros) in 2017. It has over 70 offices located in around fifty countries and has around 70,000 employees worldwide. In France, it has one establishment, Google France SARL, located at 8 rue de Londres in Paris (75009), which has approximately 600 employees and generated a turnover of around 325 million euros in 2017.

3. Since it came to exist, the company has developed many services targeting companies and private individuals (ex: the Gmail messaging service, the Google Search search engine, YouTube, etc.). It also designed the operating system for Android mobile terminals which includes app store Google Play. In addition, the company carries out advertising activities.

4. In 2016, this operating system totalled 27 million users in France.

5. On 25 and 28 May 2018, the Commission Nationale de l'Informatique et des Libertés (hereinafter referred to as "CNIL" or "the Commission") was seized for two collective complaints submitted in accordance with Article 80 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation, hereinafter referred to as "GDPR" or "the Regulation") by the association None Of Your Business (hereinafter "NOYB") and the association La Quadrature du Net (hereinafter "LQDN") respectively. In total, these complaints contained the claims of 9,974 people.

6. In its complaint, the association NOYB states in particular that the users of Android mobile terminals are required to accept the privacy policy and general conditions of use of Google services and that, failing such acceptance, they would not be able to use their terminal.

7. The association LQDN considers that, regardless of the terminal used, Google does not have valid legal bases for conducting personal data processing for the purposes of behavioural analyses and targeted advertising.

8. On 1 June 2018, the CNIL submitted the abovementioned complaints to its European counterparts via the European information exchange system with a view to designating

a possible leading authority in accordance with the provisions of Article 56 of the GDPR.

9. Pursuant to decision no. 2018-199C of 20 September 2018 of the Chair of the Commission, an online check was carried out on the following 21 September to check the compliance of any processing relating to the use of the Android operating system for mobile devices, including the creation of a Google account, with the Act of 6 January 1978 on information technology, data files and civil liberties (hereinafter "the Data Protection Act" or the "Act of 6 January 1978") and with the GDPR.

10. The online check report no. 2018-199/1 was sent to GOOGLE LLC. and Google France SARL on 24 and 25 September 2018.

11. Both companies also received the abovementioned complaints in letters from the CNIL on 28 September 2018.

12. In order to investigate these elements, on 2 October 2018, the Chair of the CNIL appointed Mr. François PELLEGRINI in the capacity of rapporteur on the basis of Article 47 of the Act of 6 January 1978.

13. Following his investigation, on 22 October 2018, the rapporteur sent Google LLC. and Google France SARL a report detailing the shortcomings relating to articles 6, 12 and 13 of the GDPR that he considered were established in this case.

14. This report suggested that the CNIL's Restricted Committee pronounce a financial sanction of 50 million euros against Google LLC., to be made public. It also suggested its inclusion in a publication, journal or any media designated by the Restricted Committee.

15. A summons to the Restricted Committee session of 10 January 2019 was also appended to the report. The body was given a period of one month to provide its written submissions.

16. By letter of 7 November 2018, the Company requested a hearing with the rapporteur, a request that was rejected by letter of 13 November 2018. On the same date, the Company also made a request for the session to be held behind closed doors and postponed, a request that was rejected by letter of 15 November 2018.

17. On 22 November 2018, the company produced its written observations relating to the report. These observations received a response from the rapporteur on 7 December 2018.
18. By letter of 11 December 2018, the company, which was given fifteen days as from receipt of the rapporteur's response, requested a postponement of the session as well as an extension to produce its new submissions from the Chair of the Restricted Committee. The request was accepted by the Chair of the Restricted Committee on 13 December 2018, who decided both to postpone the deadline for production of these submissions by two weeks - to the 7 January -, and to postpone the session to 15 January 2019.

19. On 4 January 2019, the Company produced new submissions in response to those of the rapporteur.

20. All of the submissions were reiterated orally by the Company and by the rapporteur during the Restricted Committee session of 15 January 2019.

II. Reasons for the decision

1. On the CNIL's competence

21. Article 55, Paragraph 1 of the GDPR provides: "*Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State*".

22. Article 56, Paragraph 1 of the GDPR provides: "*Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60"*.

23. First and foremost, the Company argues that the CNIL is not competent to carry out this procedure and that it should have transferred the complaints received to the Irish Data Protection Commission (hereinafter "DPC") whose responsibility it is, as Google's leading authority, to process such complaints relating to cross-border processing, in accordance with the cooperation procedure set out in Article 60 of the GDPR. Indeed, the Company considers that Google Ireland Limited must be considered its main establishment within the European Union for some of the cross-border processing that it carried out, and particularly that subject of the complaints received by the CNIL. As a consequence, the Data Protection Commission should, in its opinion, be considered as its lead supervisory authority and be responsible, as such, for processing the complaints received by the CNIL.

24. To attest to the fact that Google Ireland Limited is its main establishment within the European Union, it specifies that this company is Google's registered office for its European operations since 2003 and that it is the body in charge of several organisational functions necessary to the performance of these operations in Europe, the Middle-East and Africa (general secretariat, taxation, accounting, internal auditing, etc.). It also states that all advertising sales contracts with clients based in the European Union are signed by this company. Said company employs over 3,600 employees and has, among others, a team in charge of managing requests made within the European Union relating to confidentiality and a person responsible for privacy protection. Lastly, it specifies that an operational and organisational reshuffling is in progress with a view to making Google Ireland Limited the data controller for certain personal data processing operations concerning European citizens.

25. 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 in which decisions concerning processing are taken, this would be expressly stated.

26. Secondly, it considers that, given the cross-border nature of advertising personalisation processing operations, the high number of Android users in Europe and the questions raised in relation to such processing, the cooperation and consistency mechanisms as provided for in Articles 60, 64 and 65 of the GDPR should have applied. It also specifies that the European Data Protection Board (hereinafter "EDPB") should have been referred to in case of doubt on the determination of the lead authority.

27. Lastly, the company considers that the informal discussions which may have taken place between the other European supervisory authorities on this procedure have no legal effect, since they took place without its presence.

a) On Google Ireland Limited's status as main establishment

28. Article 4, Paragraph 16 of the GDPR defines the notion of main establishment as follows: "*(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment*".

29. Recital 36 of the GDPR states: "*The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements".*

30. The Restricted Committee considers that it follows from those provisions that, in order to qualify as a main establishment, the establishment in question must have decision-making power with regard to the processing of the personal data in question. The status of main establishment indeed requires that the effective and real exercise of "*management activities determining the main decisions as to the purposes and means of processing*".

31. Thus, the existence of a main establishment is determined *in concreto*, with respect to objective criteria, and the main establishment is not automatically the registered office of the data controller in Europe.

32. The Restricted Committee notes that this analysis is also that used by all European supervisory authorities, as attested to by the EDPB's guidelines of 5 April 2017 for identifying a controller or processor's lead supervisory authority (WP244). The latter indicate that: "*the central administration (...) is the place where decisions about the purposes and means of the processing of personal data are taken and this place has the power to have such decisions implemented*".

33. Furthermore, the Restricted Committee notes that these guidelines also state that: *"The GDPR does not permit 'forum shopping'(...). Conclusions cannot be based solely on statements by the organisation under review"*.

34. It is therefore necessary to assess the decision-making powers available to Google Ireland Limited to determine whether it qualifies as a main establishment.

35. In this respect, the Restricted Committee notes that Google Ireland Limited does possess many financial and human resources enabling Google to effectively provide services in Europe, particularly through the sale of advertising services.

36. However, although these elements attest to such participation, the Restricted Committee considers that they do not qualify Google Ireland Limited as a main establishment. The elements provided alone do not demonstrate that Google Ireland Limited had, at the time when proceedings were initiated, any decision-making powers as regards the purposes and the means of processing governed by the privacy policy presented to the user on creating an account, when configuring their mobile phone under Android. These elements only reveal this entity's involvement in the company's different activities (financial and accounting activities, sale of advertising spaces, conclusion of contracts, etc.).

37. Moreover, the Restricted Committee notes that Google Ireland Limited is not referred to in the company's "*Privacy Policy*" dated 25 May 2018 as being the entity where main decisions are taken as regards the purposes and the means of processing governed by the privacy policy presented to the user on creating an account, when configuring their mobile phone under Android.

38. It also highlights that Google Ireland Limited has not appointed a Data Protection Officer in charge of the personal data processing that it may carry out within the European Union. Furthermore, it notes that the Android operating system is only developed by Google LLC.

39. Lastly, the Restricted Committee notes that the company itself stated, by letter of 3 December 2018 sent to the DPC, that the "transfer of responsibility" from Google LLC. to Google Ireland Limited for certain personal data processing operations relating to European citizens would be complete on 31 January 2019. It later specified that it would update its Privacy Policy, which will come into effect on 22 January 2019.

40. **In light of all these elements, the Restricted Committee considers that Google Ireland Limited cannot be considered as Google LLC.'s main establishment in Europe within the meaning of Article 4 (16) of the GDPR, where it has not been established that it has decision-making power over the processing covered by the privacy policy presented to the user on creation of their account when setting up their mobile phone with Android.**

41. **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 procedures

42. Firstly, the company argues that the CNIL should have referred to the EDPB because of the uncertainty over the identification of the supervisory authority to act as lead authority.

43. The Restricted Committee firstly considers that the absence of a main establishment for a data controller in the European Union does not in itself create uncertainty about the identification of a supervisory authority acting as lead authority. It follows only from this absence of a main establishment that the identification of a lead authority is not appropriate, and that the one-stop mechanism is not intended to apply.

44. 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.

45. The Restricted Committee notes that, within this procedure, no supervisory authority, nor the Chair of the Committee, considered it necessary to refer the matter to the EDPB because of uncertainties about the identification of the lead authority or the competence of the CNIL.

46. It further notes that the analysis concluding that there is no main establishment for Google LLC. in Europe for the processing referred to by the complaints, and the resulting lack of lead authority, was shared by the DPC.

47. It notes that the DPC publicly stated on 27 August 2018 - in an Irish Times press article - that it was not the lead authority for the processing that could be implemented by the company: "*The Data Protection Commission is not the "main regulator" of Google (nor, in terms of data protection, its "lead supervisory authority") [...] Google LLC., an American company, is the data controller and Google can absolutely not invoke the one-stop mechanism. [...]. The current position is that Google is subject to the supervision of all European supervisory authorities […]".*

48. Therefore, it does not follow from the investigation that there were doubts or divergent points of view within the supervisory authorities that would require a referral to the EDPB, in accordance with Article 65 of the GDPR. Furthermore, in view of the guidelines already adopted at European level to guide the national authorities in identifying the possible lead authority, there was no new issue justifying referral to the EDPB by the CNIL in application of Article 64.

49. **Considering all of these elements, the Restricted Committee considers that the CNIL was not required to refer the matter to the EDPB for the purpose of identifying a lead authority.**

50. Secondly, although the company claims that the CNIL should have cooperated on investigation of the complaints and the follow-up they should be given, the Restricted Committee notes, as mentioned above, that the CNIL communicated, upon receipt, the 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.

51. The Restricted Committee thus notes that a procedure for cooperation was initiated with the supervisory authorities, in accordance with the provisions of Article 56 of the GDPR, initially on the sole question of identifying the respective powers of these authorities.

52. The Restricted Committee observes that this step of disseminating information and determining a potential lead authority is a prerequisite for the potential application of the one-stop mechanism provided for in Article 60 of the GDPR.

53. The Committee then notes that since this approach and the resulting exchanges did not lead to the identification of a main establishment or, subsequently, a lead authority, no further obligation of cooperation was imposed on the CNIL, including under Article 60 of the GDPR.

54. The Restricted Committee finally recalls that, for the sake of consistency, in accordance with the guidelines referred to in Article 63 of the GDPR, the CNIL has informed and consulted its European counterparts on several occasions about the investigations it has carried out, and taken utmost account of the guidelines adopted by the EDPB to ensure uniform application of the Regulation.

55. **In view of these elements, the Restricted Committee considers that the procedures for cooperation and consistency have not been ignored.**

56. Moreover, the Restricted Committee notes that, except in the case of express provisions, which is not the case here with regard to the determination of the lead authority, the supervisory authorities are not obliged to inform data controllers during the implementation of cooperation actions nor to put them in a position to participate in exchanges between authorities.

2. On the proceedings

57. Firstly, the company argues that the admissibility of complaints filed by None Of Your Business and La Quadrature du Net has not been established.

58. The Restricted Committee considers that the question of the admissibility of the abovementioned complaints does not in any case affect the legality of the present proceedings, the referral to the Committee not being necessarily subordinated to receipt of a complaint, and being able to result from a self-referral from the Commission on the basis of the findings made by the latter's departments. It recalls that the CNIL's mission is to supervise the application of the Regulation and to ensure compliance with it and that it has, for this purpose, the power to carry out investigations, in accordance with Article 57 1.a) and h) of the GDPR.

59. Moreover, the Restricted Committee notes that Article 80 of the GDPR provides that individuals have the right to mandate "*a not-for-profit [...] association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data*" to lodge a complaint on their behalf.

60. With regard to LQDN, the Restricted Committee notes that it is a French association created on 3 January 2013. It is apparent from its statutes that the purpose of this association is to take action to "*ensure the defence of fundamental rights and freedoms in the digital space* [...]".

61. As regards NOYB, the Committee notes that this is a not-for-profit association properly constituted on the Austrian territory since 12 June 2017. It appears from its statutes that its purpose is "*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 recourse)"*.

62. The Committee also notes that these two associations received, from the people referring to them, a mandate of representation under Article 80 of the GDPR.

63. Secondly, the company claims that the proceedings against it have breached 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.

64. On this point, it submits, firstly, that the report proposing a sanction and the responses given by the Rapporteur to its comments were addressed to it in French only, and, secondly that the refusal to extend the deadline set to submit its first comments limited the time available to prepare its defence. It also considers that the adjournment of the session, as well as the additional time it was ultimately granted to submit its second comments, were still not sufficient.

65. The Restricted Committee firstly states that providing notification of a sanction report in French meets 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 with the provisions of Act no. 94-665 of 4 August 1994 relating to the use of the French language*".

66. In addition, no legal or supranational provision requires the CNIL to translate the documents it produces.

67. Moreover, the company has a place of business on French territory, Google France SARL. This company has several hundred employees and has been notified of all documents related to the proceedings. It also notes that the main documents supporting the proceedings ("*Privacy Policy*", "*Terms of Service*", etc.) were the company's own documents, also available in English on other media.

68. In view of these elements, the Restricted Committee considers that the company had, in any event, sufficient material and human resources enabling it to ensure a translation of the documents into English in sufficient time to become acquainted with it and make its comments by the deadline set.

69. The Restricted Committee further recalls that Article 75 of amended Decree no. 2005-1309 of 20 October 2005 provides that the data controller has one month to make comments in response to the report it is sent, and a further period of 15 days following the deadline for the Rapporteur to respond.

70. The Restricted Committee stresses that the Company's requests of 11 December 2018 for an extension of the deadline to file comments in response to the Rapporteur's

evidence, and a postponement of the session, were granted. This postponement allowed it to benefit from an additional period of fifteen days to produce its second comments, compared to the time initially envisaged, and thus to prepare its defence for the Restricted Committee session. It was also able to present its oral comments on the day of the Restricted Committee session, in addition to its written submissions.

71. The Restricted Committee finally notes that the findings in the case made in the context of the present proceedings focused on institutional documents drafted by the company itself.

72. **In view of these elements, the Restricted Committee considers that Google LLC's rights of defence have been ensured.**

3. On the scope of the investigations

73. In defence, the company argues, firstly, that the Rapporteur has confused the Android operating system and the Google account, when they are separate services that implement different processing activities.

74. In particular, it states that when setting up an Android mobile device, users have a clear choice whether to create a Google Account or not, and that the "*Privacy Policy*" tell them how Google services can be used with or without a Google Account (e.g. watching YouTube videos without creating an account, etc.).

75. It then argues that the scope of investigation chosen by the CNIL - namely the creation of a Google account when setting up a new device using the Android operating system - is limited in that it represents a situation that only affects 7% of users.

76. Finally, it states that the findings were made on an older version of the Android operating system.

77. First, the Restricted Committee indicates that it does not call into question the existence of separate services, respectively linked to the Android operating system and to the Google account, implementing different processing activities.

78. It observes, however, that the facts covered by the investigations correspond to the scenario chosen to carry out the online test, namely a user's journey and the documents to which they could have access during the initial configuration of their mobile equipment using the Android operating system. This journey included the creation of an account. These facts therefore relate to the processing covered by the privacy policy presented to the user on creation of their account, when setting up their mobile phone under Android.

79. Next, although it is true that the user actually has the choice to create an account and has the opportunity to use some of the company's services without having to create an account, the Committee notes however that when setting up an Android device, the ability to create a Google account or connect to an existing account naturally appears at the beginning of the setup process, without specific action by the user.

80. Moreover, the latter is invited to create or to connect to a Google account given that when the user clicks on the links "*learn more*" or "*ignore*" that are available at this stage in the device's set-up, they are provided with the following information: "*Your device works best with a Google account*", "*If you don't have a Google account, you will not be able to perform the following actions [...] Activate the device's safety features*".

81. The Restricted Committee thus considers that this journey, when creating an account, creates a continuum of use between the processing carried out by the operating system and that carried out through the Google account, and justifies the scenario chosen for the online test. This succession of information and choices presented to the user does not, however, preclude a differentiated analysis, with regard to the legal framework, of the different processing activities in question, on the basis of all the facts found in the context of this test scenario.

82. In addition, with respect to the comments made by the company that this case concerns only 7% of users - mostly users of a device running Android and connecting to a pre-existing account - the Restricted Committee notes that under Article 11.1.2 of the Data Protection Act, the CNIL has substantial discretion as to the scope of the checks it may undertake. A specific test scenario, such as that used in this case, may make it possible to obtain findings reflecting a more comprehensive privacy policy.

83. Moreover, the Restricted Committee notes that the Company states in its comments dated 7 December 2018 that : "*the scope of the personal data processing carried out for Google Account holders when they use a device under Android is largely similar to the processing that occurs for Google Account holders when they use Google services on a computer or on a device that does not work under Android*" and that *[...]* "*Presenting the same Privacy Policy and Terms of Service ensures consistency and users' knowledge and, more importantly, serves as a reminder to holders of existing accounts of the nature of the data collection and the purposes of said collection*". Therefore, users who configure their Android mobile by associating it with a pre-existing account are, as regards the information communicated to them, in a situation similar to the users who proceed to create an account.

84. Finally, as regards the version of the Android operating system 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 a user's journey is similar in a more recent version of the operating system.

85. In addition, the Restricted Committee notes that the distribution statistics of the use of successive versions of the Android operating system, made available on the official website for Android developers (https://developer.android.com/about/dashboards/), demonstrate that the version used during the check is one of the most used versions (statistics covering a period of one week in October 2018 based on the connection data of devices connecting to the Google Play Store).

4. On failure to comply with transparency and information obligations

86. Paragraph 1 of Article 12 of the General Data Protection Regulation provides that: "1. *The controller shall take appropriate measures to provide any information referred to*

in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic communication. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means".

87. Article 13, paragraph 1, of the same text provides that: "*Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:*

    a) *the identity and the contact details of the controller and, where applicable, of the controller's representative;*
    b) *the contact details of the data protection officer, where applicable;*
    c) *the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;*
    d) *where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;*
    e) *the recipients or categories of recipients of the personal data, if any;*
    f) *where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available; [...]".*

88. The Rapporteur considers that the information provided to users by the company does not meet the objectives of accessibility, clarity and intelligibility laid down in Article 12, and that certain information made mandatory by Article 13 is not provided to users.

89. In defence, the company considers that the information it disseminates to its users meets the requirements of Articles 12 and 13 of the GDPR.

90. Firstly, it considers that the document entitled "*Privacy Policy and Terms of Service*", accessible when creating an account, constitutes first-level information in accordance with the EDPB guidelines on transparency under Regulation EU 2016/679 (WP260) of 25 May 2018. It states that this document offers "*a good overview of the processing implemented*" and that the mention of the legal basis of this processing does not have to be included in this first level of information. The information concerning the data retention period is in the section "*Exporting & deleting your information*" in the "*Privacy Policy*".

91. The company goes on to argue that individuals' information must, in the light of Articles 12 and 13 of the Regulation, be assessed overall. In this respect, it states that the information it issues also operates through several other modes, in addition to the documents entitled "*Privacy Policy and Terms of Service*", "*Privacy Policy*" and "*Terms of Service*". It explains that additional information messages may appear when creating an account under each of the privacy settings. Furthermore, an email is sent to

the user on creation of their account which states, in particular, that: "*At any time, you may change the privacy and security settings for your Google account, create reminders to remember to check your privacy settings or check your security settings*". This email contains clickable links redirecting to various setting tools.

92. These other control tools, which are made available to the user after the creation of their account from the management interface of their account, include, for example, a tool called "*Privacy Check-Up*" that allows users to choose the privacy settings that suit them, including personalised advertisements, location history, web-based activity and applications.

93. The company also presents a "Dashboard" tool that allows users to have an overview of their use of Google services such as Gmail or YouTube.

94. Finally, the company notes that when a user clicks on "*Create an account*" without having disabled the settings related to personalised advertisements, an account creation confirmation pop-up window appears, to remind them that the account is configured to include personalisation features. The company indicates that the user journey is thus configured to slow down the progression of users who would not naturally have chosen higher privacy settings.

95. Firstly, the Restricted Committee takes note of the progress made in recent years by the company in its policy of informing users, towards 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 respected.

96. Firstly, the Restricted Committee recalls that, in accordance with the provisions of Article 12 of the Regulation, information must be provided in an "*easily accessible*" form. This accessibility requirement is clarified in the guidelines on transparency, in which the EDPB considers that "*A central consideration of the principle of transparency outlined in these provisions is that the data subject should be able to determine in advance what the scope and consequences of the processing entails and that they should not be taken by surprise at a later point about the ways in which their personal data has been used. [...] In particular for complex, technical or unexpected data processing, the WP29 position is that controllers should [...] separately spell out in unambiguous language what the most important consequences of the processing will be: in other words what kind of effect will the specific processing described in a privacy statement/notice actually have on a data subject?*". The Restricted Committee also recalls that the accessibility requirement set out in Article 12 is based in part on the ergonomic choices made by the data controller.

97. In this case, the Restricted Committee finds that the general architecture of the information chosen by the company does not meet the requirements of the Regulation. Indeed, the information that should be communicated to individuals in accordance with Article 13 is excessively spread out across several documents: *"Privacy Policy and Terms of Service",* displayed during the creation of an account, and then the "*Terms of Service*" and "*Privacy Policy*" which are accessible subsequently through

clickable links on the first document. These different documents include buttons and links that must be activated to learn additional information. Such an ergonomic choice leads to a fragmentation of information, thus forcing the user to greatly increase the number of clicks necessary to access the different documents. They must then attentively read a large amount of information before they can identify the relevant paragraph or paragraphs. However, the user's work does not end there, since they will still have to cross-check and compare the collected information in order to understand which data is collected according to the various settings they may have chosen.

98. The Restricted Committee notes that, given this architecture, some information is difficult to find.

99. For example, with regard to advertisement personalisation processing, in order to find out the information collected from them for this purpose, a user must perform many actions and combine several document resources. As a first step, they must read the general "*Privacy Policy and Terms of Service*" document, before clicking on the "*More options*" button and then on the "*Learn more*" link to display the page "*Personalized advertising*". They will thus have access to a first description of the processing relating to personalised advertising, which proves to be incomplete. To complete the information relating to the data processed for this purpose, the user will still have to consult, in its entirety, the section "*Provide personalised services*" contained in the "*Privacy Policy*" document, itself accessible from the general document "*Privacy policy and Terms of Service*".

100. Similarly, as regards geolocation data processing, the Restricted Committee notes that the same route, devoid of any intuitive character, is required of the user with regard to information relating to geolocation data. Indeed, the latter must take the following steps: Read the "*Privacy Policy and Terms of Service*", click on the "*More options*" button and then on the "*Learn more*" link to display the page "*Location History*" and read the text displayed. However, this text is only a short description of the processing; to access the rest of the information, the user will have to return to the document "*Privacy Policy*" and consult the heading "*Your location information*". The information will still not be complete, since this section contains several clickable links relating to the different sources used to geolocate them.

101. In the two cases described, five actions are necessary for the user to access the information relating to personalised advertising and six for geolocation.

102. The Restricted Committee further notes that if the user wishes to have information on the retention periods for their personal data, they must first consult the "*Privacy Policy*" found in the main document, then go to the heading "*Exporting & deleting your information*", and finally click on the hyperlink "Click here" contained in a general paragraph on retention periods. It is therefore only after four clicks that the user can access this information. The Restricted Committee notes that the title chosen by the company for "*Exporting & deleting your information*" does not make it easy for the user to understand that this is a section providing access to information concerning 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 satisfy the requirements of transparency and accessibility of information.

103. **As a result of all these factors, there is an overall lack of accessibility to the information provided by the company in the context of the processing in question.**

104. Secondly, the Restricted Committee considers that the "clear" and "intelligible" nature of the information provided, as required by Article 12 of the GDPR, must be assessed by taking into account the nature of each type of processing in question and its concrete impact on the people concerned.

105. First, it is essential to emphasise that the data processing implemented by the data controller is particularly extensive and intrusive.

106. The data Google collects comes from a wide variety of sources. This data is collected both from the use of the phone, the use of the company's services, such as the Gmail email service or the YouTube video platform, but also from the data generated by users' activity when they visit third-party sites that use Google services, including Google Analytics cookies on these sites.

107. As such, the "*Privacy Policy*" reveals that at least twenty services provided by the company are likely to be involved in the processing, which may concern data such as web browsing history, application use history, data stored locally on the device (such as address books), geolocation of devices, etc. Therefore, a large amount of data is processed as part of these services via or in connection with the Android operating system.

108. It arises from the investigation of the case that, in addition to data from external sources, the company processes at least three categories of data:

- data "produced" by the person (for example, their name, their password, their telephone number, their email address, a means of payment, content created, imported or received, such as writings, photos or videos);

- data generated by their activity (for example, the IP address, unique user identifiers, mobile network data, data related to wireless networks and Bluetooth devices, timestamping of actions performed, geolocation data, the technical data of the devices used including data relating to the sensors (accelerometer, etc.), the videos viewed, the searches carried out, the browsing history, the purchases, the applications used, etc.);

- data derived or inferred from the data provided by that person or their activity. In this category, the "*Privacy Policy*" lists a number of purposes that can only be accomplished by generating data from the other two categories of data. Thus, the personalised advertising that the company performs requires that it infers users' interests from their activity, in order to offer them to advertisers. In the same way, the purposes of providing content, research and personalised recommendations require inferring new

information from those stated, produced or generated by the person's activity.

109. Moreover, if the very large amount of processed data can characterise alone the extensive and intrusive nature of the processing performed, the very nature of some of the data described, such as geolocation data or content consulted, reinforces this finding. Considered in isolation, the collection of each of these pieces of 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 their trips. The result of the combination of this data as a whole greatly reinforces the extensive and intrusive nature of the processing in question.

110. Consequently, it is in the light of the particular characteristics of this processing of personal data, as recalled above, that the "clear" and "intelligible" characteristics, within the meaning of Article 12 of the GDPR, of the information referred to in Article 13 of the Regulation, must be appreciated. The Restricted Committee considers that these requirements are not respected in this case.

111. In practical terms, the Restricted Committee states that the information provided by the company does not allow users to sufficiently understand the particular consequences of the processing for them.

112. In fact, the purposes indicated in the various documents are described as follows: "*provide personalised services in terms of content and advertising, ensuring the safety of products and services, providing and developing services, etc.*". They are too generic in light of the scope of the processing implemented and its consequences. This is also the case when users are told, in too vague a manner: "*The information we collect is used to improve the services offered to all our users. [...] The information that we collect and how we use them depends on how you use our services and how you manage your privacy settings*".

113. 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 lives that they may experience. It considers, in particular, that such information is not provided in a clear manner, nor at the first level of information provided to users through, in this case, the document entitled "*Privacy Policy and Terms of Service*", nor in the other levels of information offered by the company.

114. The Restricted Committee further notes that the description of the data collected, which could be of such a nature as to clarify the scope of these purposes and prevent the user from being subsequently caught off guard as to the way in which their data is 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.

115. Thus, the document "*Privacy policy and Terms of Service*" and the document entitled "*Privacy Policy*" specify that: "*We collect [...] more complex things like which ads*

you'll find most useful, the people who matter most to you online, or which YouTube videos you might like."

116. In view of the foregoing, the Restricted Committee considers that the user is unable, in particular by being aware of the first level of information presented to them in the "*Privacy Policy and Terms of Service*", to measure the impact of the main processing on their privacy. While it notes that exhaustive information, from the first level, would be counterproductive and does not respect the requirement of transparency, it considers that this should contain terms that would objectify the number and scope of the processes implemented. It also considers that it would be possible, through other types of presentation methods adapted to data combining services, to provide at the "*Privacy Policy*" stage an overview of the characteristics of this combination, according to the purposes pursued.

117. The finding of the lack of "clarity" and of an "intelligible" character must also be made with regard to the mention of the legal basis of the personalised advertising processing. In fact, the company first states in its "*Privacy Policy*": *"We ask for your agreement to process your information for specific purposes and you have the right to withdraw your consent at any time. For example, we ask for your consent to provide you with personalized services like ads […]"*. The legal basis chosen here therefore appears to be consent. However, the company adds further along that it bases itself on legitimate interest, including to conduct "*marketing to inform users about our services*" and above all to provide "*advertising to make many of our services freely available for users.*"

118. The Restricted Committee stresses that if before it, the company indicated that the only legal basis for the processing relating to personalised advertising is consent, the investigation shows that this clarification is not brought to the attention of users. The formulations recalled above do not allow the latter to clearly measure the distinction between properly personalised advertising, based on the combination of multiple pieces of user data, which is based on the company's consent statement, and other forms of targeting, using for example the context of navigation, based on the legitimate interest. The Restricted Committee emphasises the particular importance of the need for clarity in this processing, given its place in the processing implemented by the company, and its impact on people in the digital economy.

119. With respect to information on retention periods, the Restricted Committee notes that the "*How Google Retains Data We Collect*" contains four categories:

(i) "Information retained until you remove it";
(ii) "Data that expires after a specific period of time";
(iii) "Information retained until your Google Account is deleted";
(iv) "Information retained for extended time periods for limited purposes".

120. It notes, however, that as regards the latter category, only very general explanations of the purpose of this retention are provided, and no precise duration or the criteria used to determine that duration are indicated. Yet, this information is among that which must be issued to people pursuant to Article 13, Paragraph 2 (a) of the Regulation.

121. Lastly, although the company claims that multiple information tools are made available to users concomitantly and after the creation of their account, the Restricted Committee notes that these methods do not make it possible to reach the requirements of transparency and information in Articles 12 and 13 of the GDPR.

122. First, the Restricted Committee notes that the tools to which the company refers do contribute, to a certain extent, to the goal of transparency throughout the lifetime of the account and the use of Google's services. However, the Restricted Committee considers that they do not play a significant enough role in the information provided by Article 13, which must intervene "*at the time when personal data are obtained*". As reminded in the EDPB transparency guidelines, Article 13 specifies the information to be provided to data subjects "*at the start of the data processing cycle*".

123. If any data other than that strictly necessary to create the account is collected throughout the lifetime of the account, such as browsing history or purchases, the time of its creation marks the user's entry into the ecosystem of Google services, whose particularly extensive and intrusive nature of processing has already been mentioned. This step marks the beginning of a multitude of processing operations: collection, combination, analysis, etc. Therefore, since the process of creating the account is essential in the apprehension of the processing and its impact, and where the proposed user journey itself invites the data subject to particularly focus their attention at this stage, the information provided for in Article 13 of the Regulation which appears at that time must, by itself, be sufficient in light of the requirements of that provision and of Article 12 of the same regulation.

124. Moreover, both the pop-up window appearing at the time of creating the account and the email sent as soon as the account is created contain only summary or very specific information on the processing implemented, and do not allow the prior information to be regarded as sufficient.

125. Indeed, the pop-up text states "*This Google account is configured to include personalisation features (such as recommendations and personalised advertising) based on the information stored in your account*". For its part, the e-mail indicates the main features of the Google account and the existence of control tools.

126. With regard to the "*privacy check-up*" tool, it essentially allows the user to configure which information is collected, such as browsing history or places visited. Finally, the "Dashboard" consists of an information panel for each Google service providing an overview of the account holder's use.

127. Nevertheless, these "Privacy check-up" and "Dashboard" tools are only mobilised, just like the email mentioned above, after the step of creating the account, which is however essential for user information, as has been said. In addition, although their existence and interest are brought to users' attention, they presuppose the latter's active approach and initiative. For these reasons, these tools do not show that sufficient information is provided for the application of Article 13 of the Regulation.

128. **In light of all these elements, the Restricted Committee considers that there has been a breach of the transparency and information obligations as provided for in Articles 12 and 13 of the Regulation.**

5. On the breach of the obligation to have a legal basis for the processing implemented

129. Article 6 of the GDPR states that: *"Processing shall be lawful only if and to the extent that at least one of the following applies*:

a) *the data subject has given consent to the processing of his or her personal data for one or more specific purposes;*
b) *processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*
c) *processing is necessary for compliance with a legal obligation to which the controller is subject;*
d) *processing is necessary in order to protect the vital interests of the data subject or of another natural person;*
e) *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;*
f) *processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."*

130. The company was criticised for failing to validly collect the consent of individuals for personalised advertising processing. It was also considered that the company could not avail itself of a legitimate interest in this same processing.

131. In defence, the company specifies that it relies solely on consent for personalised advertising processing.

132. Article 4 (11) of the above-mentioned Regulation specifies what is meant by consent: "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*".

133. Article 7 of the same text provides the conditions for consent:

"1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent

before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."

134. Firstly, the company states that the users' consent is informed.

135. It believes that simple and clear information is presented to the user when creating an account, allowing them to know how the company uses the data for personalised advertising purposes. In particular, the company refers to the summary entitled "*Privacy Policy and Terms of Service*", the sections dedicated to advertising personalisation contained in the "Privacy Policy", and the additional information message entitled "Personalised advertising" which appears in the account creation settings options.

136. Secondly, the company claims that user consent is specific and unambiguous.

137. In particular, it states that when setting up the account, the user has the option of making a choice regarding the display of personalised advertising. It considers that this possibility enables the user to express their consent to the use of their data independently of the other choices they may express with regard to the other purposes for processing associated with the Google account (e.g. YouTube search history).

138. It also considers that the procedures for obtaining consent for the purposes of personalised advertising it sets up are in line with the CNIL's recommendations of 5 December 2013 regarding cookies. In particular, it specifies that there is brief information on the personalisation of advertisements, followed by an "Accept" button (*Privacy Policy* and *Terms of Service*), preceded by a "*More options*" button that gives users the option to disable several processing operations, including for personalised advertising purposes.

139. It also argues that the solution accepted in the Chair of the CNIL's public notice no. MED-2018-023 of 29 November 2018 allows the user to consent to all purposes via an "*Accept all*" button.

140. Finally, it considers that explicit consent for the processing of data for the purposes of personalised advertising, within the meaning of Article 9, Paragraph 2, (a) of the GDPR, could not be required if it is not sensitive data.

141. With regard to the "informed" nature of consent

142. Firstly, the Restricted Committee specifies that this informed nature must be examined in light of the preceding developments concerning the lack of transparency and information for users during the creation of their account. It considers that the

previously identified deficiencies necessarily have an impact on the information delivered to users to ensure the informed nature of the consent.

143. The Restricted Committee states that the EDPB guidelines of 10 April 2018 on consent under Regulation 2016/679 (WP250) specify that: *"A controller must ensure that consent is provided on the basis of information that allows the data subjects to easily identify who the controller is and to understand what they are agreeing to. The controller must clearly describe the purpose for data processing for which consent is requested."*

144. The guidelines also state that: "*For consent to be informed, it is necessary to inform the data subject of certain elements that are crucial to make a choice. [...] at least the following information is required for obtaining valid consent:*

- *(i) the controller's identity,*
- *(ii) the purpose of each of the processing operations for which consent is sought,*
- *(iii) what (type of) data will be collected and used,*
- *(iv) the existence of the right to withdraw consent,*
- *(v) information about the use of the data for automated decision-making [...] and*
- *(vi) on the possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards [...]".*

145. As it was able to identify under the breach of the transparency and information requirements, the Restricted Committee considers that the information on personalised advertising processing is excessively disseminated in separate documents and is not, as such, easily accessible. In this respect, the Restricted Committee refers to the preceding developments on the multiple actions that a user must perform to take cognisance of the information available on processing related to personalised advertising.

146. Furthermore, as was also noted under the breach of the transparency and information requirements, the information provided is not sufficiently clear and intelligible in that it is difficult for a user to have an overall understanding of the processing to which it may be subject and their scope.

147. By way of illustration, the information provided in the "*Personalised advertising*" section, accessible from the "*Privacy Policy and Terms of Service*" document via the "*More options*" button, includes the following indication: "*Google can show you ads based on your activity on Google services (ex: Search, YouTube, and on websites and apps that partner with Google)*". The Restricted Committee notes that it is not possible to find, for example through clickable links, the Google services, sites and applications to which the company refers. Thus, the user is not able to understand the personalised advertising processing that they are subject to, including their scope, when such processing involves a multitude of services (e.g. Google search, YouTube, Google home, Google maps, Playstore, Google photo, Google play, Google analytics, Google translation, Play books) and the processing of a large amount of personal data. Users are not able to have a proper perception of the nature and volume of data collected.

148. In view of these elements, the Restricted Committee considers that users' consent for personalised advertising processing is not sufficiently informed.

149. With regard to the specific and unequivocal nature of the consent

150. Recital 32 of the Regulation provides: *"Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her [...]. Silence, pre-ticked boxes or inactivity should not therefore constitute consent.*"

151. Recital 43 of the GDPR states: *"Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case"*.

152. The abovementioned EDPB guidelines on consent specify that: *"To comply with the element of 'specific' the controller must apply: [...] (ii) Granularity in consent requests [...] This means, a controller that seeks consent for various different purposes should provide a separate opt-in for each purpose, to allow users to give specific consent for specific purposes".*

153. In this case, the Restricted Committee notes that when the user creates an account, they have the possibility to modify some of the settings associated with the account. To access these settings, the user must click on the "*More options*" button, found before the "*Create an account*" button. The Restricted Committee also notes that the personalisation settings for the account, which contain the choice for the display of personalised advertising, are pre-checked by default, which means, unless otherwise indicated, the user's agreement to processing of their data for the purposes mentioned (e.g. YouTube search history, display of personalised advertising, etc.). The user has the option to uncheck these settings if they do not want this processing to be implemented.

154. The Restricted Committee observes that, at the time of creating the account, if the user does not click on the "*More options*" button in order to change their account settings, they must tick the boxes "*I accept Google's Terms of Service*" and "*I accept that my information is used as described above and detailed in the Privacy Policy*". They must then press the "*Create an account*" button. A pop-up window appears, entitled "*Simple confirmation*", which contains the following text: "*This Google account is set up to include personalisation features (such as recommendations and custom ads that are based on information stored in your account. To change your personalisation settings and information stored in your account, select "More options"*."

155. If they do not click on "*More options*", then the user must select the "*Confirm*" button to finalise the creation of the account.

156. In view of the foregoing, the Restricted Committee notes that although the user has the possibility of changing the configuration of their account settings prior to its creation, a positive action on their part is necessary to access the account settings options. Thus, the user can fully create their account, and accept the related processing, including personalised advertising processing, without clicking on "*More options*". Therefore, the user's consent is not, in this case, validly collected as it is not given through a positive act by which the person consents specifically and separately to the processing of their data for purposes of personalised advertising, as opposed to other purposes of processing.

157. The Restricted Committee observes that the actions by which the user creates their account - by ticking the "*I accept Google's Terms of Service*" and "*I accept that my information is used as described above and detailed in the Privacy Policy*" boxes, then by clicking on "*Create an account*" - cannot be considered as the expression of valid consent. The specific nature of the consent is not respected because the user, through these actions, accepts all of the processing of personal data implemented by the company as a block, including personalised advertising.

158. In addition, the Restricted Committee notes that when they click on "*More options*" to access the configuration of their account settings, these, and in particular the display of personalised advertising, are all checked by default. Also, the possibility users are given to configure their account settings does not translate either, in this case, into a positive action for the purpose of obtaining consent, but by an action intended to allow opposition to the processing.

159. Lastly, the Restricted Committee notes that this analysis is corroborated by the WP29 guidelines on consent which specify that: *"A controller must also beware that consent cannot be obtained through the same motion as agreeing to a contract or accepting general terms and conditions of a service. [...] The GDPR does not allow controllers to offer pre-ticked boxes or opt-out constructions that require an intervention from the data subject to prevent agreement (for example 'opt-out boxes')"*.

160. The Restricted Committee observes that, while certain user journeys may include a feature allowing the user to consent in a mutual way to the processing of their data for different purposes, this facility can only be considered as compliant if the different purposes of processing were presented to them in a distinct way beforehand, and they were able to give specific consent for each purpose, by a clear positive act, without boxes being pre-checked. In order for this type of user journey to be considered compliant, the option of giving specific consent for each purpose must be offered to people before the option "*Accept all*", or "*Refuse all*", and this must be without them having to perform any particular action to access it, like clicking on "*More options*". In view of the foregoing, the Restricted Committee considers that this type of user journey offers different guarantees from those proposed in this case, with this journey allowing the user to consent specifically and separately to the processing of their data for a specific purpose by a clear positive action, and this option being offered to them immediately and prior to the "*Accept all*" feature.

161. Therefore, in this case, by being authorised and masked "*by default*", the personalised advertising processing cannot be considered as having been accepted by the user by a specific and unequivocal positive action.

162. Secondly, although the company claims that the procedures for obtaining consent for the purposes of the personalised advertising it implements are in line with the CNIL recommendations of 5 December 2013 on cookies, the Restricted Committee notes that the specific rules applicable to cookies relating to targeted advertising operations are set out in the separate provisions of Article 32-II of the Data Protection Act, resulting from the transposition of the ePrivacy Directive of 12 July 2002 (as amended by Directive 2009/136/EC). The invocation of the recommendation of 5 December 2013 is therefore, and in any event, ineffective.

163. Thirdly, contrary to Google's argument, the requirements for consent are not intended to provide a consent system that is more protective than the one imposed by GDPR, and "wrongly" defined by criteria imposed for collecting consent applicable to the processing of so-called "sensitive" personal data.

164. The Restricted Committee notes that the terms of expressing consent were clarified and defined by Article 4 (11) of the Regulation, which states that consent means: "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*".

165. These same terms of expressing consent apply in the same way, whether consent is obtained under Article 6 of the GDPR, for the implementation of processing for a specific purpose, or collected, pursuant to Article 9 of the GDPR, to lift the prohibition in principle on the processing of so-called "sensitive" personal data.

166. Therefore, in order to be considered valid, the consent obtained must be a specific, informed and unambiguous manifestation of intent, which, as the Restricted Committee has previously noted, is not the case here.

167. **In view of all these elements, the Restricted Committee considers that the consent on which the company bases personalised advertising processing is not validly obtained.**

III. On the sanction and publicity

168. Article 45, Paragraph III, sub-paragraph 7) of the Act of 6 January 1978 provides that: "*Where the data controller or their data processor does not comply with the obligations resulting from abovementioned Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 or from this Act, the Chair of the Commission Nationale de l'Informatique et des Libertés may also, where necessary and after having sent the warning provided for in Paragraph I of this Article or, where necessary in addition to the notice provided for in Paragraph II, refer to the*

Commission's Restricted Committee to pronounce, following an adversarial procedure, one or several of the following measures [...]: 7) Save for cases in which the processing is carried out by the State, an administrative fine that cannot exceed 10 million euros or, where it is carried out by a company, 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher. In the cases mentioned in paragraphs 5 and 6 of Article 83 of abovementioned Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, these ceilings shall be increased respectively to 20 million euros and 4% of turnover. The Restricted Committee shall take into account, to determine the amount of the fine, the criteria specified in the same Article 83."

169. The company considers that an administrative fine of 50 million euros is disproportionate.

170. It points out that formal notice would have enabled it to undertake a compliance procedure, and that it does not appear that direct pronouncement of an administrative fine is the most appropriate corrective measure.

171. It further considers that the criteria set out in Article 83 of the GDPR were not all taken into account in the assessment of the proposed fine. On this point, it refers in particular to the impossibility of taking corrective measures because of the absence of prior notice.

172. The company then invokes the low number of users affected by the breaches and indicates that, out of […] people who set up a device with the Android operating system per day, only […] people create an account.

173. Firstly, the Restricted Committee notes that under the aforementioned Article 45 of Act no. 2018-493 of 20 June 2018, the Chair of the CNIL has the opportunity to prosecute and can thus choose, depending on the circumstances of the case, how to follow-up on investigations when closing a file, by issuing a formal notice or referring to the Restricted Committee for the purpose of one or more corrective measures, without it being for the latter to decide on the direction chosen by the Chair. The Restricted Committee, thus referred to, is then fully competent to decide on the substance and characterisation of the facts, and then to assess whether the breaches established would justify, by its very principle, pronouncement of one of the corrective measures mentioned in Article 45, Paragraph III of the Act of 6 January 1978 and, finally, to decide on the amount of any fine.

174. In addition, the Restricted Committee notes that while an administration, in the case where a decision is taken in respect of a set of criteria provided by a text, must take into account all of these criteria, it is not required, in the statement of reasons for its decision, to rule on each of them, but may limit itself to mentioning those it considers relevant and the corresponding facts.

175. In this case, the Restricted Committee considers that the above facts and breaches justify the pronouncement of an administrative fine on the company for the following reasons.

176. Firstly, the Restricted Committee emphasises the particular nature of the breaches noted relating 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 of the protection of personal data, in that it allows processing to be implemented only if one of the six conditions listed is fulfilled. Transparency and information obligations are also essential in that they condition the exercise of people's rights and thus enable them to maintain control over their data. In this respect, Article 6 and Articles 12 and 13 are among the provisions which, when disregarded, are most severely punishable under Article 83, Paragraph 5 of the GDPR.

177. The Restricted Committee thus considers that the obligations laid down in terms of transparency and legal bases constitute fundamental guarantees enabling people to maintain control of their data. The disregard for these essential obligations therefore appears particularly serious, because of their nature alone.

178. Secondly, the Restricted Committee notes that the breaches found continue to this day and are ongoing violations of the Regulation. It is neither a short-term disregard for the company's obligations, nor a customary violation which the data controller has willingly terminated since referral to the Restricted Committee.

179. Thirdly, the gravity of the violations is to be assessed with particular regard to the purpose of the processing, its scope and the number of people concerned.

180. In this respect, the Restricted Committee notes that although, according to the company, the scenario for online investigations by the CNIL directly corresponds to only 7% of its users, the number of people thus affected is, in itself, particularly significant. It also notes that users who configure their Android mobile phone by associating it with a pre-existing account are, in the case of the documents communicated to them and therefore of the noted breaches of the Regulation, in a situation similar to those creating an account for the first time, which the company did not dispute in its letter of 7 December 2018.

181. In addition, the Restricted Committee notes that the company carries out data processing on a considerable scale, given the prominent place occupied by the Android operating system on the French market for mobile operating systems, and the proportion of use of smartphones by phone users in France. Thus, the data of millions of users is processed by the company in this context.

182. The processing covered by the privacy policy presented to the user when creating their account - when setting up their mobile phone under Android - also appear to be considerable in terms of the number of services involved - at least twenty - and the variety of data processed via or in connection with the Android operating system. In addition to the data provided by the user themselves during creation of the account and use of the operating system, the Restricted Committee notes that a vast quantity of data is also generated from their activity, such as web browsing history, application usage

history, geolocation of devices, purchases etc. Likewise, data is derived from information provided by the data subject or their activity, in particular as part of personalised advertising. It is therefore a large amount of information, which is particularly enlightening on people's lifestyles and habits, their opinions and social interactions. As a result, the data processed by the company closely involves their identity and their privacy.

183. In addition, the Restricted Committee notes that the company uses multiple technology processes to combine and analyse data from different external services, applications or sources. They undeniably have a multiplying effect on the precise knowledge the company has of its users.

184. As a result, the Restricted Committee deems that the company has operations involving combinations with almost unlimited potential, allowing extensive and intrusive processing of users' data.

185. Given the scope of the data processing - in particular that for personalised advertising - and the number of data subjects, the Restricted Committee stresses that the breaches previously found are of a particular gravity. A lack of transparency regarding this wide-ranging processing, as well as a lack of valid user consent to the personalised advertising processing, constitute substantial breaches as regards the protection of their privacy, and are contrary to people's legitimate wish to maintain control of their data.

186. In this respect, strengthening individuals' rights is one of the main focuses of the Regulation. The European legislator notes that "*Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities (...) Technology has transformed both the economy and social life*" (Recital 6). It thus emphasises that "*Those developments require a strong and more coherent data protection framework (...) backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data.*" (Recital 7). Finally, the European legislator regrets that Directive 95/46/EC has not prevented the "*widespread public perception that there are significant risks to the protection of natural persons, in particular with regard to online activity.*" (Recital 9).

187. The Restricted Committee thus considers, in view of the scale of the processing performed and the compelling 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, rather than deprive them of basic trust in the digital ecosystem.

188. Fourthly, the Restricted Committee stresses that the breaches need to be put into perspective with regard to the company's business model, in particular the role of processing users' data for advertising purposes via the Android operating system. In view of the benefits it derives from this processing, the company must pay particular attention, in its implementation, to its responsibility under the GDPR.

189. It follows from all the foregoing, and the criteria which have been duly taken into account by the Restricted Committee, in view of the maximum amount established on the basis of 4% of the turnover indicated in point 2 of this Decision, that a financial penalty of 50 million euros is justified, as well as a complementary penalty of publicity for the same reasons.

190. The Committee has also taken into account the company's prominent position in the operating systems market, the seriousness of the breaches and the interest this decision represents for public information, in determining the duration of its publication.

FOR THESE REASONS

The Restricted Committee of the CNIL, after having deliberated, decides:

- **to issue against Google LLC. a financial penalty of 50 (fifty) million euros;**

- **to notify this decision to Google France SARL for the execution of this decision;**

- **to make its decision public on the CNIL website and on the Légifrance website, which will be anonymised upon expiry of a period of two years from its publication.**

The Chairman

Jean-François CARREZ

This decision may be appealed to the French Conseil d'État within two months of its notification.