Decision n°430810 of the Council of State

GOOGLE LLC

Session of 12 June 2020

Reading of 19 June 2020

This document is a courtesy translation by the CNIL of the original official decision of the Council of State.

In the event of any inconsistencies between the French version and this English courtesy translation, please note that the French version shall prevail.

The Council of State ruling as a Court of Law (Litigation Section, 10th and 9th Chambers assembled)

On the report of the 10th Chamber of the Litigation Section

Having regard to the following proceeding:

By a summary petition, a supplementary brief, two reply briefs, complementary observations and a new brief, registered on 16 May, 1 August and 19 December 2019 and 11 February, 18 May and 10 June 2020 at the Council of State Litigation Secretariat, Google LLC requests the Council of State:

1°) to annul Deliberation no. SAN-2019-001 of 21 January 2019 by which the Restricted Committee of the *Commission nationale de l'informatique et des libertés* (CNIL – French Data Protection Commission) imposed a monetary sanction against it to a total of 50,000,000 euros and decided to make its deliberation public, to be anonymised after two years as from its publication ;

2°) in the alternative, to put the following preliminary questions to the European Union Court of Justice and postpone its ruling while awaiting the Court's response to these questions:

"1 – Can a data controller established in a country outside the European Union but with several establishments in the European Union and a designated head office on the territory of a Member State have a "main establishment" within the meaning of Article 4(16) of the GDPR in such Member State assuming that decisions on the purposes and means of processing are taken in this third country?

2 – When a data controller envisages a processing operation with several purposes and seeks to obtain the data subject's consent pursuant to Article 6(1)(a) of the GDPR for all such purposes, do Article 7(2) and Recital 32 of the GDPR require the data controller to give the data subject the possibility of detailing their consent per purpose at the initial level of information, or can the data subject give their consent by a single clear affirmative action for all purposes at the initial level of information while having access, via a link or any other means, to the possibility of detailing their consent in a second level of information?".

It submits that the CNIL's Restricted Committee's Deliberation:

- is irregular, as Google's main establishment in Europe is located in Ireland and that, pursuant to the principle of lead authority enshrined by the General Data Protection Regulation (GDPR), it is the Irish regulatory authority that was competent to monitor its activities in the European Union;

- disregards the principle that offences and penalties must be defined by law and the principle of *non bis in idem* in deeming itself competent to examine the complaints;

- is irregular in that it has not correctly applied the procedures of cooperation and consistency provided for by Chapter VII of the GDPR;

- is irregular in that it followed the procedure provided for by the Decree of 20 October 2005 implementing the Act of 6 January 1978 bearing on information technology, data files and civil liberties, which does not ensure respect of the rights of the defence or the adversarial principle as protected by Article 16 of the Declaration of the Rights of Man and the Citizen of 1789 and the stipulations of Article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, as the time limits are too short to enable the data controller concerned to prepare its defence and no considerations of distance are provided for;

- is erroneous in law in that it found that the consent on which Google bases itself with regard to processing for the purposes of personalisation of advertising was not validly collected;

- is erroneous in law in that it found that there was a breach of the obligations of transparency and information as provided for by Articles 12 and 13 of the GDPR;

- in the alternative, is erroneous in law and lacks adequate grounds for its decision to impose a disproportionate monetary sanction of 50 million euros without having taken account of all the criteria provided for in Article 83 of GDPR.

By a defence brief and three reply briefs, registered on 23 October 2019 and 15 January, 26 February and 11 June 2020, the CNIL rejects the petition, submitting that there is no basis for any of the pleas.

By an intervention and a brief, registered on 6 April and 8 June 2020, the *Union fédérale des consommateurs* – "*Que Choisir*" (UFC – Federal Union of Consumers) stated that it would intervene on behalf of the defence.

Having regard to the other documents in the case file;

Having regard to:

- the Constitution, in particular its Preamble;

- the European Convention on the Protection of Human Rights and Fundamental Freedoms;

- Regulation (EU) 2016/679 of the European Parliament and Council of

27 April 2016;

- Act no. 78-17 of 6 January 1978;
- Decree no. 2005-1309 of 20 October 2005;European Union Court of Justice Ruling C-673/17 Bundesverband der Verbraucherzentralen un Verbraucherverbande – Verbraucherzentrale Bundesverband eV vs Planet49 GmbH of 1 October 2019;
- Administrative Justice Code and Ordinance no. 2020-305 of 25 March 2020 amended;

After having heard in Public Session:

- the report by Mr. Réda Wadjinny-Green, Auditor;
- the conclusions of Mr. Alexandre Lallet, Public Rapporteur;

The floor being given, before and after the conclusions, to Spinosi & Sureau, the law firm representing Google LLC;

Having regard to the post-hearing submission, registered on 13 June 2020, submitted by Google LLC;

Whereas:

1. The investigation showed that the *Commission nationale de l'informatique et des libertés* (CNIL – French Data Protection Commission) had two collective complaints referred to it on 25 and 28 May 2018, submitted pursuant to Article 80 of Regulation (EU) 2016/679 of 27 April 2016 bearing on protection of natural persons with regard to the processing of personal data and free movement of data, known as the General Data Protection Regulation (GDPR), and made by the *None of Your Business* and *La Quadrature du Net* associations. On 21 September of the same year, the CNIL conducted an online investigation in order to check whether the processing operations carried out by Google LLC on personal data of users of the Android operating system complied with the Act of 6 January 1978 bearing on information technology, data files and civil liberties, and with the GDPR. Following this investigation, the President of the CNIL initiated a sanction procedure. By a Deliberation of 21 January 2019, the annulment of which Google LLC requests, the CNIL's Restricted Committee imposed a monetary sanction of 50,000,000 euros on the company for breaches of 6, 12 and 13 of the GDPR and decided to make the sanction public for a period of two years as from its publication.

On the intervention by the UFC – *Que Choisir*:

2. Given the subject and nature of the litigation, the UFC – *Que Choisir* shows sufficient interest to intervene in this proceeding in support of the conclusions presented by the *Commission nationale de l'informatique et des libertés* (CNIL), which reject the petition. Consequently, its intervention is admissible.

On the CNIL's competence:

3. Article 55 of the GDPR provides that "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", while Article 56 of the Regulation provides, "1. 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 crossborder processing carried out by that controller or processor in accordance with the procedure provided in Article 60. (…) 6. The lead supervisory authority shall be the sole interlocutor of the controller or processor for the crossborder processing carried out by that controller or processor". Pursuant to 7) of Article 4 of the same Regulation, the notion of "data controller" refers to "the natural or legal person (…) which, alone or jointly with others, determines the purposes and means of the processing of personal data (…)", while 16) of the same Article provides that the notion of "main establishment" be taken to mean "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 (…)". Finally, the Regulation's 36th Recital specifies that "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 (…)".

4. The provisions quoted in the previous point make it clear that when crossborder processing of personal data carried out in the European Union is in question, the supervisory authority overseeing the controller's main establishment in the Union, as lead authority, is competent to monitor compliance with the requirements of the GDPR. For determination of the competent supervisory authority, the data controller's central administration, i.e. its real head office, must in principle be regarded as its main establishment. This is not the case if another of its establishments is competent to take decisions relating to the purposes and means of processing and has the power to see that they are applied at Union level. In the case of a data controller located outside the European Union implementing crossborder processing on Union territory but not having a central administration or establishment with decision-making powers as regards its purposes and means, the lead authority mechanism provided for in Article 56 of the GDPR cannot be implemented. In such a case, each national supervisory authority is competent to monitor compliance with the GDPR on the territory of the Member State it belongs to, in compliance with the abovementioned Article 55.

5. Google LLC submits that the CNIL was not competent to undertake the sanction procedure referred to in Point 1 and that it should have communicated the complaints it had received to the Irish data protection authority, as Google Ireland Limited should be regarded as its main establishment in the European Union. It confines itself to

stating that its Irish establishment constitutes its "head office" for its European operations, that it possesses major financial and human resources and is responsible for "numerous organisational functions" throughout Europe, without specifying what they consist of. It is undisputed that, on the date of the contested decision, the Android operating system was developed and operated exclusively by Google LLC, which is located in the United States and responsible for the processing under dispute. First of all, the investigation does not show that, on such date, Google Ireland exercised any powers of management or control of Google LLC's other European subsidiaries that might lead it to be regarded as a central administration within the meaning of the GDPR. Secondly, the investigation shows that this establishment, which at all events was not assigned new responsibilities with regard to processing carried out by Google in Europe until 22 January 2019, after the date of the contested sanction, did not possess any decision-making powers as to the purposes and means of the processing under dispute, no more in fact that any other of its European establishments.

6. It results from what has been said in Points 4 and 5 that Google Ireland Limited could not be regarded as the central administration of the data controller responsible for the processing operations under dispute, and that, on the date of the contested sanction, Google LLC, which alone determined their purposes and means, did not have a main establishment in the European Union within the meaning and for application of the GDPR. As no lead authority could therefore be designated under the conditions provided for in Article 56 of the GDPR, the CNIL was competent to investigate the complaints made by the *None of Your Business* and *La Quadrature du Net* associations due to the processing of the personal data of French users of the Android operating system operated by Google LLC, and impose the contested sanction against the company. Recognition of such competence regarding controllers processing data on users located in France, the conditions for determination of which at all events do not disregard the principle that offences and penalties must be defined by law, could not result in a breach of the principle of *non bis in idem*.

On the regularity of the procedure:

7. Firstly, the European Data Protection Board (EDPB) issues opinions in the cases referred to in Paragraph 1 of Article 64 of the GDPR, which do not include sanction procedures, or when a supervisory authority, the Chair of the Board or the Commission refer to it in this respect pursuant to the second Paragraph of the same Article. The Board may also take binding decisions in the cases referred to in Article 65 of the Regulation, which provides that "*1. In* order *to ensure the correct and consistent application of this Regulation in individual cases, the Board shall adopt a binding decision in the following cases: a) where, in a case referred to in Article 60 (4), a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead supervisory authority and the lead supervisory authority has not followed the objection or has rejected such an objection as being not relevant or reasoned (...) b) where there are conflicting views on which of the supervisory authorities concerned is competent for the main establishment; / c) where a competent supervisory authority does not request the opinion of the Board in the cases referred to in Article 64 (1), or does not follow the opinion of the Board issued under Article 64".*

8. The investigation shows that, on 1 June 2018, the CNIL submitted two

complaints that had been referred to it to its European counterparts via the European information exchange system, with a view to designating a possible lead authority. None of the European supervisory authorities made the decision to refer the matter to the European Data Protection Board or gave voice to any assessments differing from the CNIL's as regards Google LLC having no main establishment in Europe. Furthermore, after that date, the Irish data protection authority publically stated, by a right of reply exercised on 27 August 2018 in the *Irish Times* newspaper, that it was not Google LLC's lead authority as the company's Irish establishment had no decision-making powers as to data processing operations that it carried out in Europe. As there were no divergent points of view and as investigation of the complaint in litigation noted no other cases provided for by Articles 64 and 65 of the GDPR, the plea that the procedure was irregular because the European Data Protection Board had not been referred to cannot but be dismissed.

9. Secondly, the mechanism provided for in Articles 60 to 62 of the GDPR, which aims to encourage cooperation between the various European data protection supervisory authorities and ensure consistent application of the Regulation throughout the Union, only applies in cases of designation of a lead authority or joint operations by supervisory authorities. As the litigation is not the result of either of these two cases, the allegation that the CNIL disregarded its duty of cooperation and mutual assistance, which at any event cannot be usefully cited in support of an appeal against a sanction imposed by the Commission, cannot but be dismissed.

On disregard of the rights of the defence:

10. Firstly, the petitioning company submits that the Decree of 20 October 2005 implementing Act no. 78-17 of 6 January 1978 bearing on information technology, data files and civil liberties, under which the litigation proceeding was conducted, disregards the rights of the defence and the right to a fair trial guaranteed by Article 16 of the Declaration of the Rights of Man and the Citizen of 1789 and Article 6 of the European Convention on the Protection of Human Rights and Fundamental Freedoms, as, on the one hand, the procedural deadlines it provides for are too short to enable the data controller to prepare their defence properly, and on the other, no adjustment of such deadlines is allowed for, in particular as regards data controllers located abroad.

11. Under the terms of Article 16 of the Declaration of the Rights of Man and the Citizen of 1789, "*Any society in which the respect of rights is not guaranteed, nor the separation of powers secured, has no Constitution at all"*. Among other things, this provision implies that no sanction with the character of a punishment can be imposed on a person without their being put in a position to present their observations on the charges against them. As regards measures of a punitive nature, respect of the general principle of the rights of the defence assumes that the data subject is informed, in adequate detail and within a reasonable time before the sanction is imposed, of the complaints made against it, and is able to have access to the documents served as the basis of the charges against it, at the very least when it so requests.

12. Article 74 of the Decree of 20 October 2005, then in force, provides that: "When a sanction is likely to be imposed, the President of the Commission shall appoint a

rapporteur who does not belong to the Restricted Committee and shall inform the data controller or processor in question. / The rapporteur shall take all necessary steps with the assistance of the Commission's departments. The controller or processor may be heard if the rapporteur considers it useful (…)". Under the terms of Article 75 of the same Decree, "The report provided for by Article 47 of the aforementioned Act of 6 January 1978 shall be notified to the data controller or processor by any means enabling the Commission to provide proof of the date of such notification. It shall also be communicated to the Restricted Committee. / The data controller or processor shall have one month to communicate their written observations to the rapporteur and Restricted Committee. Notification of the report shall refer to this deadline and specify that the data controller may consult and copy the documents in the file at the Commission's departments, and be assisted or represented by a counsel of its choice. / The rapporteur may reply to the data controller or processor within the fifteen days following reception of their observations. If necessary, the data controller or processor shall have a further fifteen day in which to communicate its written observations. (…) The data controller or processor shall be informed that, after the deadline referred to in the previous paragraphs has elapsed, unless closure of the investigation is postponed, the investigation will be closed and its written observations declared inadmissible by the Restricted Committee. / The rapporteur may decide to modify their report at any time; in particular in the light of factors brought to their attention by the data controller or processor. The procedure provided for in the previous paragraphs shall then be applied. If such modification is made after the investigation is closed, the investigation shall be reopened". Finally, Article 76 of the Decree provides that "The data controller or processor shall be informed of the date of the Restricted Committee's meeting during which its case is to be considered, and of its right to be heard, either personally or through its representative, by any means enabling proof of the date of its notification to be provided. Such information must reach it at least one month before the date of the meeting in which the case is to be examined. In the event of re-examination or postponement of the case at a later meeting, the minimum deadline may be reduced to seven days".

13. First of all, it results from these provisions that a data controller notified of a report proposing a sanction against it has a month to communicate its observations to the Restricted Committee and the rapporteur, and then another fifteen days to reply to the rapporteur's new observations, if any. At the end of this second period, the examination is in principle closed. A date is also set for the hearing, during which the data controller may present its observations orally. The controller is informed of this date at least a month before the hearing is held. It follows from the provisions of the aforementioned Articles 75 and 76 that, depending on the circumstances of the case, the Chair of the Restricted Committee may postpone the date of closure of the investigation and/or the date of the hearing in order to enable the data controller to prepare its defence. Moreover, with regard to administrative sanction proceedings, no rule or principle requires that time limits be extended on account of distance, for petitioners domiciled outside Metropolitan France. This being so, the plea of illegality of Articles 75 and 76 of the Decree of 20 October 2005 must be dismissed.

14. Secondly, it is submitted that, in this case, the procedure followed disregarded the rights of the defence, as Google was not put in a position where it was able to make good use of its observations. The investigation showed that the petitioning company had an initial month to reply to the rapporteur's report and then had a second month to react to the rapporteur's response as the Chair of the Restricted Committee had granted it an extension of fifteen days, meaning that the investigation was closed two months and fifteen days after

communication of the aforementioned report. Although the petitioning company requested organisation of hearings twice during the proceeding, firstly with the Commission and then with the rapporteur, on the basis of Article 74 of the Decree of 20 October 2005, and these requests were rejected on 11 October and 13 November 2018, the investigation showed that the Restricted Committee's meeting, initially set for 10 January 2019, was postponed to 15 January at the petitioner's request and that it was able to submit it oral observations on that date. This being so, the company was able to prepare and present its defence properly. The plea that the rights of the defence were disregarded must therefore be dismissed, without the facts that most of the documents in the proceeding were in French and that no prior formal notice was given having any influence on this point.

On the breaches of the obligations of information and transparency:

15. 1 of Article 12 of the GDPR provides that "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 means (…)". Article 13 of the same Regulation specifies the information that must obligatorily be provided to users. It is clear from these provisions that the information provided to users must enable them to determine the scope and consequences of the processing operation in advance in order to avoid being caught off guard as to the way that their personal data are to be used. Although the requirements of conciseness, intelligibility, clarity and simplicity of information imposed by the GDPR justify its not being excessively detailed so as not to discourage users from taking note of it, all relevant information on the various purposes and scope of the processing operation must be easily accessible to them.

16. Google LLC submits that the architecture it selected aims to inform users clearly and intelligibly, based on a multi-level approach, in compliance with the recommendations of the European Data Protection Board. The first level, comprising "Confidentiality Rules and Conditions of Use", presents the scope and main purposes of processing, while several hypertext links – "conditions of use"; "confidentiality rules"; "more options"; "regulations"; and "find out more" – enable users to access more exhaustive information. Finally, and after an account has been created, other tools are made available to the user for management of their confidentiality parameters, including the "confidentiality check-up" and "dashboard" tool.

17. Firstly, the first level of information provided to users appears too general in view of the scope of the processing operations carried out by the company, the degree of intrusion of privacy that they involve, and the volume and nature of data collected.

18. Secondly, the investigation showed that essential information on certain processing operations is only accessible following a lengthy series of actions, or that it is only available via hypertext links which are themselves difficult to access. In order to obtain all relevant information on personalised processing of advertisements, a user must first of all carry out three actions starting from the first level of information before returning to the initial

document and carrying out two more actions, a total of five actions altogether, while six actions are required to obtain exhaustive information on geolocation. Information on data retention periods, which must be provided pursuant to a) of 2° of Article 13 of the GDPR, is only accessible via a hypertext link available on the sixty-eighth page of the "Confidentiality Rules" document.

19. Thirdly and finally, the information communicated is itself sometimes incomplete or not detailed enough, including in the final levels of information. For example; the investigation showed that the document on data retention published by Google states that certain data may be retained "*for long periods for specific reasons"*, without stating the intended purposes or which data are concerned.

20. This being so, due to the way in which it fragments the information it organises, the tree structure adopted by Google would seem to impair its accessibility and clarity for users, despite the processing operations in question being particularly intrusive in view of the quantity and nature of data collected. It follows that the CNIL's Restricted Committee, which, contrary to what is submitted, did not require exhaustive information to be delivered at the first level of information, was right in characterising a breach of the obligations of information and transparency defined by the aforementioned Articles 12 and 13 of the GDPR. Furthermore, the CNIL's Restricted Committee was not bound to indicate what measures should be taken in order to meet the GDPR's requirements.

On the breaches of the rules on consent for processing for the purposes of personalisation of advertising:

21. Firstly, Article 6 du GDPR provides 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". 11 of Article 4 of the same Regulation specifies 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". Under the terms of Article 7 of the same Regulation, "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 (…)". It results from these provisions as interpreted by the European Union Court of Justice in its Ruling C-673/17 of 1 October 2019 that freely given, specific, informed and unambiguous consent can only be a user's express consent, given in full knowledge of the facts and after provision of adequate information on the use to be made of their personal data. Consent given in default via a ticked box does not involve any active behaviour on the user's part and cannot therefore be regarded as having resulted from a clear affirmative action enabling valid collection of consent. Moreover, consent collected in the context of overall acceptance of a service's general conditions of use does not have a specific character within the meaning of the GDPR. Finally, independently of the method by which it is collected, consent is only valid if it is preceded by clear and distinct presentation of all intended purposes of the processing concerned.

22. The investigation showed that, for creation of the Google account required for use of the Android operating system, the user is first of all presented with the "Confidentiality Rules and Conditions of Use", which inform him or her succinctly and very generally on the nature of data processed and the aims of processing operations carried out by Google. The user can then click on the "more options" link or tick the "I accept Google's conditions of use" and "I agree to my information being used as described above and detailed in the confidentiality rules" boxes in order to create their account. If the user clicks on the "more options" link, a page proposes that he or she configure their account. As regards personalisation of advertising, a pre-ticked box, which can be deselected, indicates that he or she consents to display of personalised advertisements The user can then obtain more information by clicking on the "find out more" link, which specifies the methods by which personalised advertisements are displayed, without such information being exhaustive, however. If the user decides not to click on the "more options" link on the first page presented to him or her, a "simple confirmation" window appears, reminding the user that the account is configured to include personalisation functionalities "such as personalised recommendations and advertisements". This page tells the user how to modify these parameters. He or she can then access the "more options" page again or confirm creation of their account definitively.

23. Although the architecture described in the preceding point ensures that the user is always asked to signal that he or she agrees to their information being processed in compliance with their account's default configuration, i.e. including advertisement personalisation functions, the information provided on this purpose is general and included in the midst of purposes that do not necessarily require consent as their legal basis, both at the first level of information and in the "simple confirmation" window. Hence, in view of the aforementioned requirements of clarity and accessibility, it would appear that information on the scope of processing for "advertisement targeting" provided at the first level is insufficient. In the absence of adequate prior information, the consent collected in all-inclusive fashion for all purposes, including this one, cannot be regarded as informed, and consequently and in any event, must be deemed invalid. Although further information on the advertisement targeting purpose is provided at the second level (by clicking on "more options") and separate consent is collected for this purpose, it would appear that such information is itself inadequate given the scope of the processing. Finally, there is the fact that consent is collected by means of a pre-ticked box. Under these circumstances, the CNIL's Restricted Committee was right in considering that the methods used for collecting consent do not meet the GDPR's provisions, which require a clear affirmative action, without the allegation that the Regulation does not impose separate collection of consent for the advertisement targeting purpose having any influence on this point. Furthermore, and contrary to what is submitted, the Restricted Committee was not bound to provide any specific definition of the obligations incumbent upon the petitioning company as regards consent, which are a direct result of the GDPR.

24. Secondly, although the petitioning company submits that the CNIL interpreted the requirement of consent in a manner inconsistent with its previous position statements, it cannot usefully cite the fact that the methods for collection of consent described in Point 22 were in compliance with the recommendations made by the CNIL in Deliberation no. 2013-378 of December 2013 bearing on cookies, which was based on Directive 95/46, which was no longer in force at the date of the contested sanction, or cite Deliberation no. 2019-093 of 4 July 2019, which gives operators six months to adapt with regard to cookies

and trackers, during which the Commission stated that continuation of browsing as an expression of consent would not result in implementation of its repressive powers. Nor can the petitioner usefully cite the fact that "explicit" consent is required to authorise the processing of the so-called sensitive data referred to in Article 9 of GDPR in order to infer that such consent is not required for data not referred to in the said Article, as Article 4 of the Regulation defines consent in the same way whatever the nature of the data concerned.

On the grounds for the sanction imposed by the CNIL:

25. First of all, 2 of Article 83 of the GDPR provides that "Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:/ a)the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them; / b) the intentional or negligent character of the infringement; / c) any action taken by the controller or processor to mitigate the damage suffered by data subjects; / d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32; / e) any relevant previous infringements by the controller or processor; / f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement; / g) the categories of personal data affected by the infringement; / h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement; / i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures; / j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and / k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement".

26. Secondly, Article L. 211-2 of the Code of Relations between the Public and the Administration provides that "*grounds must be given for decisions that*: (…) *2° Impose a sanction",* while, under the terms of Article L. 211-5 of the same Code, "*The grounds required by this chapter must be in writing and include a statement of the legal and factual considerations forming the basis of the decision"*. It results from these provisions that, in cases where the legality of an administrative decision is based on a number of considerations being taken into account, the compliance with the requirement to state grounds that they provide for results in its authors only having to state those on which they have based their decision. Nor is there any provision requiring the CNIL's Restricted Committee to provide an explanation of the amount of the sanctions it imposes. It follows that the plea that there are insufficient grounds for the contested decision, as it did not pronounce on all the criteria provided for in the aforementioned Article 83 of the GDPR or make mention of the figures used in determining the amount of the sanction to be imposed and the error of law revealed by such inadequate statement of grounds, must be dismissed.

On the amount of the sanction imposed:

27. It results from the forgoing that, in view of the particular seriousness of the breaches committed, which is due to the nature of the requirements that were disregarded and their effects on users, the ongoing character of such breaches and the length of the period during which they lasted, the ceilings provided for by 4 of Article 83 of the GDPR, and the company's financial situation, the monetary sanction of 50,000,000 euros imposed on Google is not disproportionate.

28. It results from the foregoing, without it being necessary to put preliminary questions to the European Union Court of Justice, that the Google LLC's petition must be rejected.

DECIDES:

Article 1: The intervention by the UFC – *Que Choisir* is permitted.

Article 2: Google LLC's petition is rejected.

Article 3: This decision will be notified to Google LLC and the *Commission nationale de l'informatique et des libertés*.