Deliberation of Restricted Committee no. SAN-2023-009 of 15 June 2023 concerning [redacted]

The *Commission nationale de l'informatique et des libertés* (CNIL), meeting in its Restricted Committee composed of Mr Alexandre Linden, Chairman, Ms Christine Maugüé and Messrs Alain Dru and Bertrand du Marais, members;

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

Having regard to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on the processing of personal data and the protection of privacy in the electronic communications sector;

Having regard to amended French Data Protection Act No. 78-17 of 6 January 1978, in particular Articles 20 et seq.;

Having regard to Decree No. 2019-536 of 29 May 2019 implementing French Data Protection Act No. 78-17 of 6 January 1978;

Having regard to deliberation No. 2013-175 of 4 July 2013 concerning adoption of the CNIL's internal regulations;

Having regard to Decision No. 2020-005C of 27 December 2019 of CNIL's Chair to instruct the general secretary to carry out, or have a third party carry out, an assignment to verify the processing implemented by the company [redacted] or on its behalf, in any location that may be concerned by the implementation of said processing;

Having regard to the CNIL Chair's decision appointing a rapporteur before the Restricted Committee of 23 June 2021;

Having regard to the report of François Pellegrini, commissioner and rapporteur, notified to [redacted] on 03 August 2022;

Having regard to the written observations made by the counsel of [redacted] on 31 October 2022;

Having regard to the rapporteur's response to these comments notified to [redacted] on 7 December 2022;

Having regard to the new written observations made by the counsel of [redacted], received on 30 January 2023;

Having regard to the oral observations made during the Restricted Committee session;

Having regard to the other documents in the file;

The following were present during the Restricted Committee session on 16 March 2023:

- Mr François Pellegrini, commissioner, his report having been read;

In the capacity of representatives of [redacted]:

- [redacted]

- [redacted]

By videoconference: [redacted]

[redacted] having spoken last;

The Restricted Committee adopted the following decision:

I. Facts and proceedings

1. Founded in [redacted] in France, [redacted] (hereinafter the "Company") specialises in the display of targeted advertising on the web. In 2022, the [redacted] employed approximately [redacted] employees and had a total turnover of approximately [redacted] for a net profit of approximately [redacted]

2. The company implements so-called "advertising retargeting" data processing, which consists of tracking Internet users' browsing habits to display personalised advertising to them, using cookies placed in users' terminals.

3. On 8 November 2018, the *Commission nationale de l'informatique et des libertés* data protection authority (hereinafter "the CNIL" or "the Commission") received a complaint sent by the "Privacy International" association, which emphasised in particular that the company had not been processing the data of Internet users in accordance with the principles set out in Article 5(1) of 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, and repealing Directive 95/46/EC (hereinafter "the GDPR").

4. On 4 December 2018, the CNIL received a complaint sent by the "None of Your Business" association (hereinafter "NOYB") commissioned by [redacted], criticising the formalities imposed by the company from which he had wished to withdraw his consent and object to the processing of his data (hereinafter "the complainant"). The complainant stated that, despite having sent an email to this effect to the company, it had redirected him to various online procedures devoted to the exercise of rights.

5. On 14 January 2019, in accordance with Article 56 of the GDPR, the CNIL informed all European supervisory authorities of its competence to act as lead supervisory authority regarding cross-border processing implemented by the company, a competence derived by CNIL from the fact that the company's main establishment is located in France.

6. After exchanges between data protection authorities, it turned out that all European authorities are covered within the meaning of Article 4(22) of the GDPR.

7. As part of the investigation of the complaint lodged by NOYB, CNIL questioned the company on the follow-up to the complainant's requests. This investigation led to an exchange of letters between CNIL and the company, dated 27 March, 29 April, 9 September, 9 October, 27 December 2019 and 17 February 2020. A meeting was also held on 17 January 2020.

8. Further to this instruction, and pursuant to Decision No. 2020-005C of 27 December 2019 of the Chair of the Commission, a CNIL delegation carried out several checks on the company in order to verify compliance with the provisions of Law No. 78-17 of 6 January 1978 as amended on data processing, files and freedoms (hereinafter "the French Data Protection Act" or "Law of 6 January 1978") and the GDPR.

9. On 29 January 2020, the delegation sent a questionnaire to the Company, to which the company replied on 27 March 2020, concerning its organisation, the personal data processing that it implements, its qualification as a data controller, its relations with its customers and partners, and its management of requests to exercise rights.

10. On 16 and 17 September 2020, the delegation conducted an on-site investigation at the company's premises, during which it carried out audits on the website of two partners of the company. The delegation also checked the follow-up to the complainant's request to exercise his rights and obtained information on how to implement the right to withdraw consent and the right to erasure. The onsite investigation led to the production of two reports, no. 2020-005/1 and no. 2020-005/2, supplied to the company on 30 September 2020.

11. On 13 October 2020, using a list provided by the company of the hundred websites from which it collects the most data, the delegation conducted an online audit on several of these sites to verify such aspects as the procedures for placing the [redacted] cookie on user devices and the mechanism implemented to obtain their consent. The online inspection led to the production of report no. 2020-005/3, supplied to the company on 14 October 2020.

12. On 23 June 2021, on the basis of Article 22 of the Act of 6 January 1978, the Chair of the Commission appointed Mr François Pellegrini as rapporteur for the purpose of investigating these elements.

13. On 9 June 2022, the rapporteur sent an additional request to the company, requesting in particular the latest versions of the general terms and conditions of use of the [redacted] services, as well as a recent sample of contracts entered into by the company with its partners. The company responded on 17 June 2022.

14. On 3 August 2022, at the end of his investigation, the rapporteur notified the company of a report detailing the breaches of Articles 7, 12, 13, 15, 17 and 26 of the GDPR, which he considered established in this case.

15. This report made a recommendation to the Restricted Committee of the Commission to impose an administrative fine against the company of an amount of no less than sixty million euros. It also proposed that this decision be made public and that the company no longer be identifiable by name upon expiry of a period of two years following its publication.

16. On 31 October 2022, the company submitted observations in response to the rapporteur's report.

17. On 7 December 2022, the rapporteur replied to the company's observations.

18. On 30 January 2023, the company submitted further observations in response to those of the rapporteur.

19. In a letter dated 21 February 2023, the rapporteur informed the company's counsel that the investigation was closed, pursuant to Article 40, III, decree no. 2019-536 of 29 May 2019 implementing the French Data Protection Act.

20. The rapporteur and the company presented oral observations at the Restricted Committee session, which took place on 16 March 2023.

II. Reasons for the decision

A. On the European cooperation procedure

21. Pursuant to Article 60(3) of the GDPR, the draft decision adopted by the Restricted Committee was transmitted to the other competent European supervisory authorities on 16 May 2023.

22. As of 13 June 2023, none of the supervisory authorities concerned had raised a relevant, reasoned objection to this draft decision, so that, pursuant to Article 60(6) of the GDPR, they are deemed to have approved it.

B. On the processing in question, the qualification of personal data and the liability for processing.

1. On the processing in question for the purpose of displaying personalised advertising

23. Article 4(2) of the GDPR defines processing as "*any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, preservation, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, deletion or destruction*."

24. In this case, the **Restricted Committee** notes that the company implements data processing called "advertising retargeting" for the purposes of displaying personalised advertising (hereinafter the "processing in question").

25. In practical terms, the company collects browsing data from Internet users through cookies that are stored on their terminals when they visit one of their [redacted] partners' websites, including publishers and advertisers. When an Internet user visits a partner's website, the company stores a cookie on the device their browser is running on. This is assigned a unique identifier, called [redacted] ID, which will enable it to recognise him/her during future visits to the partner's other sites.

26. So when an Internet user visits a partner advertiser's website, the company records in its database the internet user's actions via the cookie (for example, visiting the home page, connecting to a user account, clicking on a "product" page, adding an item to the shopping basket).

27. Then, when the user visits the website of a partner publisher, the publisher sends a request to the company for information such as the size of the advertising insert, the nature of the publisher website and an identifier allowing the company to recognise the user.

28. The company then uses its data processing technologies to determine which advertising would be most relevant to display to the Internet user according to their browsing habits and the products or services that may be of interest to them. Based on this analysis, the company then engages in "real-time bidding" (RTB) for displaying an ad on the publisher's advertising space. If the company wins the bid, an advertiser's advertising banner is displayed in the insert available on the publisher's website.

29. In this way, acting as an intermediary between advertisers and website publishers, the company not only helps advertisers to reach their target audience with more relevant advertising, but also helps publishers to promote their advertising spaces.

30. The Restricted Committee notes that the company has acknowledged implementing the processing described in the preceding paragraphs.

2. <u>On the qualification of the data processed by [redacted] as personal data</u>

31. Article 4(1) GDPR defines personal data as "*any information relating to an identified or identifiable natural person ('data subject'); an 'identifiable natural person' is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*."

32. Recital 30 of the GDPR, which is part of well-established case law of the Court of Justice of the European Union (CJEU, 24 Nov. 2011, *Scarlet Extended SA C 70/10,* pt. 51 and 19 Oct. 2016, *Breyer*, C-582/14) provides that an online identifier associated with a natural person, such as an IP address or a login cookie, may "*leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them*."

33. In its aforementioned *Breyer* judgement, handed down under Directive 95/46/EC, the CJEU stressed the importance of a case-law approach to whether a data item was an "identifier" or not, rather than a general position based on principle. It stated that, in order to determine whether an individual is identifiable, account should be taken of all the means likely to be reasonably used, either by the data controller or by another individual, to identify that individual.

34. **The rapporteur** is of the view that the company processes personal data, taking into account that – in view of the number and diversity of the data collected and the fact that they are all linked to an identifier – it is possible, with reasonable means, to re-identify the natural persons to whom such data relates.

35. **The company** maintains that it processes *"browsing events*", which are pseudonymised technical data that do not enable it to directly identify the Internet users with which they are associated. It argues that it is only required to recognise the identity of an individual in the event of a request for a right of access where they can match the [redacted] cookie identifier ([redacted] ID) and the identity of the individual. Outside of such a hypothesis, it considers that the risk of re-identification is very low and produces simulations on this point carried out by service providers.

36. It concludes that since it only processes pseudonymised data, any possible breaches it may have committed have had a very limited impact on the data subjects, which the Restricted Committee should take into account in its assessment.

37. **The Restricted Committee** points out that only genuine anonymisation of the data processed, causing the data to lose their "personal" nature – i.e., without the possibility of re-identifying the natural person to which they relate – would exempt the processing from all the requirements of the GDPR.

38. In this specific case, the Restricted Committee notes that although the company maintains that it does not process anonymised data, it claims to process only pseudonymised data with a very low risk of re-identification.

39. The Restricted Committee also notes that the [redacted] ID cookie identifier, assigned by the company by means of the cookies it places, is intended to distinguish each individual whose data it collects, and that very many items of information intended to enrich the web user's advertising profile are associated with this identifier, including:
    - data related to the identification of the individual: geographical location from IP address, [redacted] user ID, device identifier, partner-provided identifiers, email address in hashed form provided by the partners;
    - data related to the individual's activity, which corresponds to the tracking of the web user's browsing history through the sites visited, the products viewed or added to the basket, and the act of purchasing. This also includes any interactions the user has with the advertisements presented to them (did the user click on the banner? did they make a purchase?);
    - data derived or inferred from the above information in order to be able to offer the user the most relevant products, taking into account their interests.

40. The Restricted Committee thus notes that although the company does not directly possess the identity of the natural persons to which the devices on which cookies are registered are linked, re-identification may be facilitated by the fact that, in certain cases, the company collects – in addition to data related to browsing events – other data facilitating re-identification, such as the e-mail addresses of the individuals whose browsing journeys have been from within an authenticated (or "logged") environment in hashed form, the identifiers corresponding to them generated by other players, the IP address in hashed form and the user agent of the device used.

41. Therefore, once the company is able to re-identify individuals by reasonable means, the processed data retain a personal character, within the meaning of Article 4.1 of the GDPR.

42. It follows that the GDPR is applicable and that, having regard to what has been indicated above, the company is a data controller for the processing in question.

C. On the failure to comply with the requirement of demonstrating that the data subject has given his/her consent;

43. Pursuant to Article 6(1) of the GDPR: "*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.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks."

44. Article 4(11) of the GDPR defines consent as *"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*".

45. Article 7(1) of the GDPR relating to the conditions applicable to consent provides that: "*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*."

46. **The rapporteur** considers that the company has not put in place any measures to ensure that the personal data it processes are only data for which valid consent has been collected from the individual. It notes that of the websites audited by the CNIL, more than half of the websites published by its partners did not obtain valid consent and that the company had not implemented an audit mechanism for its partners.

47. **The company,** citing the *Fashion ID* judgement (CJEU, 29 July 2019, C 40/17), argues that its partners, who have the capacity of joint data controllers, remain the best placed to collect the consent of the data subjects in that the [redacted] cookie is placed on the devices of Internet users when browsing their website.

48. The company adds that in this respect, the various agreements entered into with its partners pursuant to Article 26 of the GDPR (in particular the aforementioned General Terms and Conditions of Service and its Data Protection Agreement) provide that this obligation lies with them. It considers that this contractual distribution is sufficient to ensure compliance with this obligation, which is binding on its partners under the principle of binding force of contracts.

49. It argues that there is no evidence that the practices observed on the twelve websites visited by the audit delegation are representative of the state of compliance of its [redacted] partners.

50. Although it claims that it has no obligation itself to ensure that its partners have validly obtained the consent of the data subjects, the company nevertheless points out that it does not hesitate to terminate contracts signed with parties who do not comply with their obligations in terms of obtaining the consent of Internet users.

51. It adds that it has implemented other auditing mechanisms, such as a strategy for auditing its partners which, as at 31 October 2022, has verified the state of compliance of nearly [redacted] of its partners, as well as a so-called *"Know Your Client*" process by which it checks the compliance of its future partners with several regulatory requirements (presence of a cookie banner and privacy policy) prior to entering into a service contract with them. Finally, it states that it has terminated a contract it had with one of its partners which had been audited by the CNIL delegation, and has sent a warning to another partner who did not comply with the regulations applicable to the collection of consent from Internet users.

52. **The Restricted Committee** points out that in the case of joint liability, Article 26 of the GDPR obliges joint data controllers to ensure, through an agreement, that they mutually comply with the GDPR and, in particular, that they work together to determine the best way to respond to the rights of data subjects, depending on the nature of the processing and their respective responsibility for such processing.

53. It points out that in points 167 and 168 of its guidelines 07/2020 on the concepts of data controller and data processor in the GDPR, the European Data Protection Board (EDPB) considers that in case of joint responsibility, *"both data controllers are always required to ensure that both have a legal basis for the processing*" and that they *"may have a certain degree of flexibility in the division and allocation of responsibilities between them, provided that they ensure full compliance with the requirements of the GDPR with regard to the specific processing*".

54. Firstly, with regard to the respective roles and obligations of [redacted] and the partner sites, the Restricted Committee notes that as part of its processing for the purpose of displaying personalised advertising, the company processes the personal data of Internet users visiting the websites of its partners which are collected in advance through the [redacted] cookie.

55. It also notes that the company and the websites of its partners from which the [redacted] cookie is deposited on the devices of Internet users are jointly responsible for the operations of depositing the [redacted] cookie and for the collection of data from Internet users carried out using this cookie.

56. With regard to the legal framework applicable to these various processing operations, the Restricted Committee recalls that if the storage of the [redacted] cookie on the device of the user visiting a partner's website, enabling the company to assign a unique identifier to that user, is subject to the provisions of Article 5(3) of Directive 2002/58/ EC of the European Parliament and of the Council of 12 July 2002 on the protection of privacy in the electronic communications sector (hereinafter the "'ePrivacy' Directive"), transposed into French law in Article 82 of the French Data Protection Act, the subsequent processing for advertising purposes, which is carried out from the personal data collected through this cookie, is subject to the provisions of the GDPR.

57. With regard to the legal basis applicable to these various processing operations, the Restricted Committee first points out that under the "ePrivacy" Directive, operations for reading or writing information in a user's device cannot be implemented without the user's prior consent.

58. It then notes, with regard to the processing in question, that the company stated to the auditing delegation in its response to the questionnaire of 29 January 2020 that: "*all processing that we carry out in connection with our advertising services in Europe is based on user consent*." Furthermore, the company's processing privacy policy also mentions consent as the legal grounds applicable for the purposes of displaying personalised advertising, whether targeted or contextual.

59. The Restricted Committee notes that, according to a consistent position of the CNIL, the overlap between the rules of the "ePrivacy" Directive and the GDPR allows the publisher of the website from which the cookie is saved to collect the consent necessary for saving the cookie at the same time necessary for the subsequent processing implemented from the data collected by this cookie.

60. Specifically, it notes, in this case, that the company has made an arrangement with its partners such that the general conditions of use of the [redacted] services, to which the partners of the company have subscribed, specify that it is the responsibility of the partner to obtain the consent of the data subject for the subsequent processing carried out on the basis of the data collected by this cookie.

61. However, the Restricted Committee considers that the mere fact that the collection of the consent of Internet users for the implementation of the processing in question is the responsibility of the partners does not exempt the company from its obligation, pursuant to Article 7 of the GDPR, to be able to demonstrate that the data subject has given his/her consent.

62. This dual-liability regime ensures that at all stages of the processing of data collected for a user's browsing on one of the company's partner sites, each joint data controller complies with the provisions incumbent upon it: for partners, those relating to the storage and reading of the [redacted] cookie on the user's device and, for the company, those provisions relating to subsequent processing carried out from the data collected by this cookie.

63. Specifically, the data subjects are required to benefit from the protection offered by the legislation in force to which they are entitled throughout their browsing and, in particular, that their data are processed by the company only if they have previously and validly consented to it.

64. In addition, the company's core activity is to transform raw browsing data into valuable information that it uses. The fact that the company plays a central role in the advertising ecosystem is all the more reason why it must be able to ensure that the processing in question complies with the regulations in force.

65. Finally, the Restricted Committee notes that the *Fashion ID* judgement, referred to by the company, deals with the question of whether it was the website manager (Fashion ID) or the publisher of the cookie (Facebook) who was responsible for obtaining the consent of the data subjects before filing the cookie published by Facebook and that it was handed down under Directive 95/46/EC on data protection.

66. Insofar as the European legislator has intended to strengthen individual rights and stakeholder accountability by establishing, in particular, the obligation for the data controller to be able to demonstrate that the individual whose data it processes has actually given his/her consent, pursuant to Article 7(1) of the GDPR, the Restricted Committee considers that the reference to the Fashion ID judgement is not relevant in this case.

67. Secondly, the Restricted Committee notes that in connection with the online checks carried out during the on-site investigations of 16 September 2020 and during the online audit of 13 October 2020, the delegation found that on seven company partner websites, a [redacted] cookie had been placed on the device used on this occasion, at the time of its arrival on the home page without it having carried out the slightest action; whereas, at the time of these findings, the CNIL had already had been prompted to issue a reminder that such practices directly contradicted the provisions of the French Data Protection Act applicable to cookies.

68. The Restricted Committee also notes that in three cases, the website being visited did not allow the user to refuse cookies other than by configuring his/her browser, which does not constitute a mechanism for refusing valid consent, while in two cases, a [redacted] cookie was placed after the delegation had expressed its refusal to such storage.

69. In addition, as part of the on-site investigations of 16 September 2020, the delegation noted that the two websites visited did not contain any mechanism for obtaining consent to the deposit of cookies, such as a button or a box to be ticked. Several events related to the browsing of these two sites have been recorded in the company's database, such as visiting the pages of products sold by the company's partners.

70. It emerges from all these checks that the absence of valid consent was noted by the delegation on almost one in every two sites visited. Yet the Restricted Committee also notes that details of nine of the twelve sites visited by CNIL staff were provided by the company itself, as those generating the largest amount of data collected in its database.

71. While it is true that the audit procedure did not permit verification of all the sites of the company's [redacted] partners, the Restricted Committee considers that it can reasonably be inferred from the aforementioned findings that as of the date of the checks, the company processed a large volume of browsing data for which Internet users had not given valid consent.

72. Thirdly, the Restricted Committee notes that at the date of the initiation of the audit procedure, the company had not implemented any satisfactory measures to suggest that it was in compliance with the requirements of Article 7(1) of the GDPR.

73. Thus, the Restricted Committee notes that at the beginning of the audit procedure, in response to the delegation's question regarding the measures put in place by the company to ensure the validity of the consent, in the event that it had to delegate the collection of this consent to a third party, the company had simply reproduced a reference to its general terms and conditions of use, in their applicable version of May 2016, according to which the company required its partners, *"where the law so provides*", to ensure that the privacy policy of their website included *"information and choice mechanisms in accordance with applicable laws and regulations*".

74. It is the view of the Restricted Committee that such a clause did not, on its own, ensure the existence of valid consent and that, at the very least, a supplementary clause needed to be added to specify that the body collecting consent must make proof of consent available to the other party, so that all data controllers wishing to rely on it could actually refer to it.

75. In this case, the Restricted Committee notes that on the date of commencement of the audit procedure, this clause was not only not supplemented by a specific clause on proof of consent, but also that the company had additionally admitted that it had never terminated a contract due to a partner's failure to comply with its contractual obligations, nor implemented any other auditing measures on its partners.

76. In relation to this, the Restricted Committee notes that the various measures referred to by the company were progressively implemented only from 2020, after the initiation of the audit procedure initiated in January 2020.

77. The Restricted Committee thus takes note of the company's audit campaign with its partners since 2020 and the fact that the company has also terminated the contract it had with one such partner who did not comply with its obligations in terms of cookies.

78. It similarly notes that in subsequent versions of its general conditions of use, the company has inserted a clause relating to proof of consent that the partner undertakes to *"provide promptly to [redacted], upon request and at any time, proof that the consent of the data subject has been obtained by the partner*".

79. In light of this information, the Restricted Committee considers that the company has complied with the requirements of Article 7(1) of the GDPR.

80. It nevertheless points out that this late achievement of compliance does not alter the fact that the company has processed the personal data of Internet users without being able to demonstrate that they validly consented to the processing whose purpose is to display personalised advertising, in breach of Article 7(1) of the GDPR.

D. On the violation of information and transparency obligations

81. Article 12(1) of the GDPR states 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."*

82. According to Article 13 of the GDPR, the data controller must provide the data subject with the following information:
"a) the identity and the contact details of the data controller and, where applicable, of the data 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 grounds for the processing;
d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the data controller or by a third party;
e) the recipients or categories of recipients of the personal data, if any; and
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;".

83. **In this case**, **the rapporteur** maintains that the information provided by the company to the data subjects was not complete in that it did not contain all the purposes relating to the processing in question in the version of its confidentiality policy applicable on the date of the findings, including the purpose relating to the improvement of its technologies.

84. The rapporteur also criticises the company for a lack of clarity as to the legal grounds for consent applicable to the processing; the company specifies that this differs from country to country, and according to the purposes implemented on the basis of the legitimate interest.

85. **The company** responds that it has updated its privacy policy.

86. It contests this first complaint in any case, maintaining that it did not have to specify the purpose of improving its technologies since, in its view, this purpose includes technical elements that contribute to the same overall purpose as the display of personalised advertisements.

87. On the second objection, it argues that the possible ambiguities criticised by the rapporteur have never prevented the data subjects from exercising their rights.

88. In its second observations, the company argues that it cannot be accused of any breach of its obligations under Article 13 of the GDPR insofar as it only collects data indirectly.

89. **The Restricted Committee** points out, firstly, that the GDPR makes a distinction over the regime governing the obligation to inform which is imposed on the data controller according to the nature of the data collection: the data controller is subject to the provisions of Article 13 of the GDPR when the data are collected directly from the data subject, and to the provisions of Article 14 of the GDPR otherwise.

90. It adds that in point 26 of its guidelines of 29 November 2017 on transparency, in their revised version of 11 April 2018, the EDPB points out that Article 13 of the GDPR also applies when the data is collected by the data controller *"by observation*", i.e. when the data controller collects the data via the use of sensors of any kind.

91. The Restricted Committee notes that the French Conseil d'Etat adopted the same interpretation in a decision handed down before the entry into force of the GDPR, considering that the fact that the collection does not require any intervention on the part of the data subjects had no impact on the direct nature of this collection (Conseil d'Etat, 10th - 9th chambers combined, 8 February 2017, *JCDecaux,* No. 393714).

92. In this case, the Restricted Committee notes that the data is indeed collected by the company directly from the Internet user, as when that user browses the website of a partner of the company, the requests of the [redacted] cookie enabling the partner to identify that an Internet user is visiting home page, log into an account or click on a "product" page, are sent directly to its servers, without transiting via another data controller.

93. As the data is collected from individuals, the Restricted Committee concludes that Article 13 of the GDPR applies to the company.

94. Secondly, the Restricted Committee notes that the general terms and conditions of use of the [redacted] services provide that the company's partners must incorporate a personal data protection policy, containing a link to [redacted]'s privacy policy, into their website.

95. It notes that the "*Legal grounds for data processing*" section of the company's privacy policy, in its version applicable on the date of the findings, stated that: "[redacted] *'s processing operations comply with the regulations in force, in countries requiring the consent of users for the use of cookies or any other similar technology. This consent is collected on the Advertisers' and Publishers' websites and mobile applications*."

96. Furthermore, it was also stated in the same section that: *"[redacted] believes that it has a legitimate interest in processing your data for the purposes expressed in this privacy policy, in particular to:*
- *adhere to the commercial agreements made with our clients and partners;*
- *enable our Advertisers to promote their products and services;*
- *enable our Publishers to fund their activities."*

97. The Restricted Committee considers, firstly, that the first wording creates uncertainty as to the legal basis for processing, in that it does not make it clear to Internet users located within the European Union that the processing of their data is based on their consent.

98. Next, it states its belief that the purposes announced by the company are expressed in vague and broad terms that do not give users a clear understanding of which personal data are being used for what purposes. Furthermore, the Restricted Committee considers it contradictory to state that the purposes relating to the promotion of advertisers' products and the financing of publishers' activities are based on the legal basis of legitimate interest, when in fact these purposes are directly linked to the processing of displayed personalised advertising, which, as the company itself acknowledges, is based on the legal grounds of the consent of Internet users. The Restricted Committee adds that such a vague and contradictory description of the purposes pursued on the basis of legitimate interest is likely to hamper the exercise by data subjects of their right to object, which is intrinsically linked to the quality of the information provided.

99. The Restricted Committee notes that the company has responded to these shortcomings in the new version of its privacy policy; it now specifies that consent applies to individuals residing in the European Economic Area and includes a table summarising all the purposes of its processing, including those based on the legal grounds of legitimate interest, which includes a detailed description of these purposes and the categories of data concerned. The Restricted Committee notes that the company has also removed the contradiction noted above.

100. Thirdly, the Restricted Committee notes that the *"Purpose of the processing of personal data*" section of the company's privacy policy, in its version applicable on the date of the findings, contained only the following line: "[redacted]*processes your personal data to display personalised ads*".

101. However, during the on-site investigations of 16 and 17 September 2020, the company specified to the delegation that the processing also allowed it "*to optimise the responses to be given to auctions and the selection of items to be presented in an advertisement, and to suggest the best layout for this banner*".

102. While the Restricted Committee admits that certain technical operations described by the company directly contribute to the main purpose of displaying personalised advertising, it is of the opinion that by contrast, others serve a separate purpose.

103. Indeed, the company uses the data collected through cookies in order to improve its own technologies (purpose called "machine learning", mobilising the data collected by the company to auto-configure algorithm-driven targeting processing operations). Thus, the main objective of this subsequent processing is to improve the overall effectiveness of the advertising targeting carried out by [redacted]. This is therefore a separate purpose, which must be brought to the attention of the data subjects.

104. The Restricted Committee also notes that the new version of its privacy policy, posted online on 4 November 2022, clearly distinguishes, within the *"Use of your data*" section, (a) the purpose of *"display of personalised advertising"* and (b) the purpose of *"training models"*, defined as making it possible to *"improve the performance of [redacted]'s advertising operations*".

105. The result of the above is that by not providing data subjects with all the information required, by using insufficiently clear and precise terms, and by presenting erroneous legal grounds for the processing operations, the company has failed to fulfil its transparency and information obligations under Articles 12 and 13 of the GDPR. However, the Restricted Committee takes note of the fact that the company was compliant during these proceedings.

E. On the violation of the obligation to uphold the right of access of data subjects to their personal data

106. Article 12(1) of the GDPR states 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*".

107. Article 15(1) of the GDPR states that: "*The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data […]*".

108. **In this case**, as part of the investigations carried out by the CNIL, the company provided the delegation with three examples of responses sent to data subjects who made access requests.

109. It emerges from this that when an individual exercised his right of access with the company, it sent that individual the data extracted from the following three tables:
- the "*Advertiser_advent*" table, which stores all data related to the advertiser's events;
- the "*Banner_display*" table, which stores all the data necessary to enable an advertisement to be displayed to the user (e.g.: the user's country, advertiser-related data or the version of the operating system of the user's device);
- the "*Click_cas*" table, which stores all the data related to a user's interactions with the advertising banners.

110. **The rapporteur** is of the view that the company only partially responded to requests for access rights made to it, since it did not supply the data contained in three other tables:
- the "*Usermatching*" table, which contains the information enabling [redacted] identifiers to be reconciled (in the event that the same user uses several devices) in a "deterministic" manner (the company relies on information provided by its partners, such as a loyalty card number, an Apple or Android identifier, and/or an e-mail address in hashed form to create a link between two [redacted] identifiers);
- the "*bc_tcp_timestamp*" table, which contains information enabling the reconciliation of identifiers in a "probabilistic" way (the company applies a prediction model from the data linked to two identifiers that it believes correspond to the same user);
- the "*Bid_request*" table, which contains information related to events related to the online auction protocol.

111. It is also of the view that the provided information was not intelligible to the user, as the company merely provided a summary description of the goal of each table, yet did not provide explanations on the goal of each of the columns in these tables, nor on their content.

112. **The company** argues that its procedures in the event of requests made under the right of access comply with the requirements of Article 15 of the GDPR. More specifically, it returns to each of the three tables listed by the rapporteur and explains why, in the event of a request for access, it did not communicate the data they contained.

113. With regard to the "*Usermatching*" table, the company argues that it only contains data enabling the reconciliation of the [redacted] identifier with other identifiers, but that it nevertheless undertook to provide these data as part of its responses to access requests from November 2022.

114. With regard to the "*bc_tcp_timestamp*" table, the company argues that this table, which is based on a probabilistic method, may potentially reconcile two distinct individuals, so that the communication of data could potentially harm the rights and interests of third parties in the event that the data relating to another individual are communicated to the originator of the access request. For this reason, it excluded this table from its responses to access requests.

115. With regard to the "*bid_request*" table, the company argues that it contains approximately 400 fields relating to auction requests, so that these are essentially technical data and that the remaining data are identical to those appearing in the "*Banner_display*" table already provided by the Company. However, it specifies that it had committed to providing all of these data as part of its responses to access requests by March 2023, the time required to implement an action plan that will allow it to extract these data by profile.

116. With regard to the intelligibility of the information provided to data subjects, it states that it has supplemented the explanations with a table that, for each table, lists the nature of the data processed, and provides a description and examples of data, which it sends in its response to access requests.

117. **The Restricted Committee** takes note of the explanations given by the company for the *"bc_tcp_timestamp* " table and in fact considers that the company was not required to provide the data of this table, insofar as they may concern several individuals without the company being able to identify with certainty which data concerns exclusively the individual making the request.

118. With regard to the "*Usermatching*" and "*bid_request*" tables, it is of the opinion that the information presented and produced by the company now enable users to better understand the information sent to them.

119. The Restricted Committee notes, however, that the explanations provided by the company do not, on the date of the findings, justify the non-communication of the data contained in these two tables, whereas it is not disputed that these tables contain personal data which may be combined with other data recorded by the company and, in particular, with the identifier assigned to each Internet user.

120. It adds that it emerges from these same findings that, in its response to requests for access rights, the company explained the objective of each table in a brief sentence, and invited users to send an email for more information. By not automatically providing information on the purpose and

content of each of the columns in these tables, the company left users uncertain as to the nature of the processed data concerning them.

121. The result of the above is that, by not communicating all the personal data of the individuals exercising their right of access to it and by not officially providing them with documentation enabling them to understand the data supplied to them, the company failed to fulfil its obligations under Articles 12 and 15 of the GDPR.

F. On the violation of the obligation to uphold the right to withdraw consent and to erasure of data

122. Article 7(3) of the GDPR states that: "*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 simple to withdraw as to give consent*."

123. Under Article 17(1) of the GDPR, *"The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:*
[…]
b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing
[…]
d) the personal data have been unlawfully processed
[…]".

124. **In this case**, exchanges took place between the CNIL and the company following the receipt of [redacted]' complaint concerning his individual situation but also, more generally, the procedures implemented by the company to respond to requests to exercise the rights of individuals. The company stated that it had improved the measures put in place, in particular to make effective the right to withdraw consent and the right to erasure of data.

125. The outcome of investigations subsequent to these exchanges and the introduction of the measures announced by the company is that data subjects who wished to withdraw their consent to the processing of their data by the company, or who exercised their right of erasure, could do so by clicking the "*Disable* [redacted] *services*" button accessible in the company's privacy policy found at "[redacted].com". The company specified that when an individual clicks on this button, an "opt-out cookie" is placed in the individual's browser, thus preventing the subsequent placement of [redacted] cookies and the display of personalised advertisements.

126. The company stated that the deactivation of the [redacted] services, i.e. the act of no longer displaying personalised advertising to the individual, could also be effected by using the platforms made available by professional associations representing the sector, such as the *"YourOnlineChoices*" platform.

127. During the on-site investigations of 17 September 2020, the delegation noted that the company was no longer tracking the user ID assigned to [redacted] in its databases. During the same audit,

the company stated that the opt-out procedure for its services no longer enabled it "*to link the user ID in question to the user's browser, so that no advertising will be offered to this identifier*", without having the effect of removing from its tables the user ID originating the objection or erasure request. The company added that: "*in the event that a user identifier has been disabled, it will no longer be possible to match events related to that identifier with any other identifiers related to that user*". Lastly, the company stated that it could re-use the [redacted] user ID, and the events related to the request for deactivation, for the purpose of improving its technologies.

128. **The rapporteur** is of the view that the company has not met the requirements of Article 17 of the GDPR since it is not removing the individual's identifier or deleting the linked browsing events, despite the fact that the processing of [redacted]' complaint demonstrates that it is indeed able to effectively erase the data it processes.

129. **The company** argues that it is not required to make such a deletion if it has a legitimate interest in retaining and processing the data of individuals who have made a request for erasure for the following six purposes: reconciliation of sales/allocation, prevention of fraud / fight against fraud, training of models, invoicing, reporting and incident resolution.

130. For this reason, it considers itself justified in not effectively deleting this data as long as the pursuit of these other purposes based on the legitimate interest justifies their retention. For each of these six purposes, the company has produced a study demonstrating the relevance of using this legal basis.

131. Specifically with regard to the purpose of training models, the company is of the view that this allows data subjects to receive even more personalised advertisements, which is also in their interest. It adds that the CNIL has already recognised, in sanction deliberation no. 2013-420 of 3 January 2014 and in a decision MED-2017-075 of 27 November 2017, that *"the improvement of services*" could be considered as a legitimate interest for a data controller.

132. **The Restricted Committee** notes that when it responds to a request for erasure, the company does no more than halt the display of personalised advertisements on the device of the individual making the request, without effectively deleting the data relating to that individual.

133. The Restricted Committee notes that the company claims that it cannot perform such erasure on the grounds that it requires the data collected during its advertising targeting processing, based on consent, to carry out six other purposes which, according to the latter, are based on the legal grounds of legitimate interest.

134. However, without it being necessary to rule on the suitability of the legitimate interest as legal grounds for each of the six purposes put forward by the company, the Restricted Committee considers that, in cases where the company was in any event unable to ensure that the individual originating the request had validly consented to the processing of his/her data by the company, the company could not continue to process the data of this individual for subsequent purposes based on legitimate interest. However, as has been demonstrated above, the company did not retain any proof of the valid consent of the individuals, in breach of Article 7 of the GDPR. The company could not therefore restrict itself to halting the display of personalised advertising and effectively had to delete the data processed.

135. This conclusion is all the more necessary since it emerges from the investigations that the company processes a large volume of data which is established as having originated from cookies placed

before any expression of intention by the Internet user and even, in certain cases, when the user has expressly expressed his/her refusal.

136. It follows from the foregoing that in limiting itself to halting the display of personalised advertising and not deleting personal data in the event of exercise of users' right to erasure, for individuals for whom the company could not show meaningful consent, the company breached its obligations under Articles 7 and 17 of the GDPR.

G. On the violation of the obligation to provide for an agreement between joint controllers

137. Article 26 of the GDPR states that: "*1. [The joint controllers] shall in a transparent manner determine their respective liabilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them.* 2. *The arrangement referred to in paragraph 1 shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects."*

138. **The rapporteur** notes that on the date of the findings, the company had entered, with its joint controller partners (advertisers, publishers and online auction platforms), into a contract that contained a description of the processing that is the subject of joint responsibility and the role of each manager with regard to such processing.

139. It nevertheless emphasises that this agreement was not sufficient to lead to the conclusion that the company complies with Article 26 of the GDPR.

140. **The company** argues that, as drafted, the agreement with its partners did not harm data subjects, who have benefited from the full protection of the GDPR, since the general terms and conditions of use of its services specify that partners must provide a link to [redacted]'s privacy policy and allow data subjects to express their consent to targeted advertising.

141. Yet it explains that it has adopted a new agreement, which entered into force on 5 July 2022.

142. **The Restricted Committee** considers that the drafting of Article 35 of the GDPR shows that the deed of distribution of the obligations of joint controllers must cover all the obligations provided for by the GDPR in order to determine, for each of these obligations, which joint controllers will be responsible for them.

143. In this case, the Restricted Committee notes that on the date of the findings, the agreement entered into by the company with its partners did not specify some of the respective obligations of the data controllers with regard to the requirements contained in the GDPR, such as the exercise by the data subjects of their rights, the obligation to notify a data breach to the supervisory authority and to the data subjects or, where applicable, carrying out an impact assessment under Article 35 of the GDPR.

144. It points out that the obligation to enter into an agreement in the event of joint liability is a specific obligation imposed on joint controllers under Article 26 of the GDPR.

145. Although, in its version of 5 July 2022, the agreement entered into by the company with its partners now includes the information expected under this provision, the Restricted Committee notes that this late achievement of compliance does not alter the fact that a breach was committed in the past.

146. It follows from the above that the company breached its obligation under Article 26 of the GDPR.

III. On the issue of corrective measures and publicity

147. Article 20 of amended Act No. 78-17 of 6 January 1978 provides that: *"When the data controller or its processor does not comply with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or from this Act, the chair of the Commission nationale de l'informatique et des libertés (French Data Protection Authority) may […] refer the matter to the Restricted Committee of the Commission with a view to imposing, after an adversarial proceeding, any one or more of the following measures: […]*
7. With the exception of cases where the processing is implemented by the State, an administrative fine may not exceed 10 million euros or, in the case of a company, 2% of the total annual global turnover of the previous financial year, whichever is the greater. In the cases mentioned in 5 and 6 of Article 83 of Regulation (EU) 2016/679 of 27 April 2016, these upper limits shall be increased, respectively, to 20 million euros and 4% of the said turnover. In determining the amount of the fine, the Restricted Committee shall take into account the criteria specified in the same Article 83".

148. Article 83 of the GDPR, as referred to in Article 20, paragraph III of the French Data Protection Act, states: "*Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive",* before specifying the information to be taken into account when deciding whether to impose an administrative fine and when deciding on the value of such fine.

A. On the issue of an administrative fine and its amount

149. **The company** first argues that the CNIL infringed the principle of non-discrimination by bringing proceedings solely against it, despite having established that the websites of its partners did not comply with the regulations applicable to cookies.

150. It then argues that it should not be sanctioned for not ensuring that its partners obtain valid consent other than by contractual means, since such verifications should in fact be returned to the CNIL, which was thus engaging in a "privatisation" of its functions.

151. The company maintains that better consideration of the criteria laid down in Article 83(2) of the GDPR, in particular with regard to the absence of proof of damage, the non-intentional nature of the breaches, the measures taken to mitigate the damage, the cooperation it claims to have demonstrated with the supervisory authority, and the categories of personal data concerned, which are not particularly intrusive, would – should the Restricted Committee decide to impose a fine – justify a significant reduction of the 60 million euros amount proposed by the rapporteur.

152. It argues that the rapporteur's proposed fine represents 50% of its profit and almost 3% of its worldwide turnover, which is close to the legal maximum under Article 83 of the GDPR. By comparison, it highlights the previous decisions handed down by the CNIL against Google (CNIL, FR, 31 December 2021, sanction deliberation no. SAN-2021-023) and Facebook (CNIL, FR, 31

December 2021, sanction deliberation no. SAN-2021-024) on cookies, the amount of which amounted to 0.07% and 0.06% of their overall turnover respectively.

153. **The Restricted Committee** recalls, as a preliminary point, that it is not the Restricted Committee's responsibility to assess the decision of the Chair of the CNIL to take legal action against the company alone.

154. The Restricted Committee notes that, in order to assess the appropriateness of imposing an administrative fine and establishing its value, it must take into account the criteria specified in Article 83 of the GDPR, such as the nature, gravity and duration of the infringement, the number of data subjects, the measures taken by the controller to mitigate the damage suffered by the data subjects, the degree of cooperation with the supervisory authority, the categories of personal data concerned by the infringement and the financial benefits from the infringement.

155. Firstly, with regard to the imposition of an administrative fine, the Restricted Committee deems that it is in the first place appropriate to apply the criterion provided for in Article 83(2)(a) of the GDPR relating to the gravity of the infringement taking into account the nature, scope of the processing as well as the number of data subjects affected.

156. It points out, first of all, that it has been established that the company was unable to demonstrate that the data subjects had given their consent to the processing of personal data concerning them, and that the findings of the audit delegation revealed that the company used browsing data partially obtained from cookies placed before the Internet user had been able to exercise consent.

157. Next, with regard to the scope of the processing, the Restricted Committee stresses that the violation is all the more serious because the processing in question, which is aimed at displaying personalised advertisements, is carried out on a very large scale and is by nature widespread and intrusive.

158. It points out that in order for the displayed advertisements to be relevant, it is necessary for the company to collect large quantities of data relating to the browsing habits of Internet users in order to establish a precise picture of their consumption habits, preferences or concerns at the time.

159. This means that each visit to an advertiser's or publisher's site, each click on a product or each purchase made by an Internet user is recorded by the company and analysed for advertising purposes. As such, the company claims on its website that it collects 35 billion events per day from browsing and purchases worldwide. In addition, the company shares and receives data from its partners; for example, to enable it to better identify each Internet user or to establish a link between the various devices and browsers used by a single Internet user.

160. The Restricted Committee notes that, although when taken in isolation, each of the data items collected by the company has a low identifying value, when combined with each other, they could reveal with a significant degree of precision many aspects of people's private lives, including their gender, age and consumption habits, i.e. their tastes, thus giving the processing in question a widespread and intrusive nature.

161. Consequently, the result of the combination of this data considerably reinforces the widespread and intrusive nature of the processing in question and makes it even more necessary for it to be implemented in strict compliance with the rules in force, in particular those rules surrounding the choice of individuals as to the use of their data.

162. Similarly, the Restricted Committee points out that the transformation of raw browsing data into usable information constitutes the core activity of the company. The company must therefore be able to ensure that the personal data it processes complies with the regulations in force.

163. With regard to the number of individuals concerned by the processing in question, the Restricted Committee notes that the company publicly states that it has data relating to approximately 370 million user identifiers across the European Union, including approximately 50 million identifiers on French territory alone. Although a single individual may correspond to several identifiers, these figures reveal the substantial amount of data collected by the company.

164. As regards the violation related to informing individuals, the Restricted Committee emphasises that it has resulted in a loss of control by Internet users over their data insofar as the company has not provided them with complete and comprehensible information.

165. As regards the violations relating to the exercise of the rights of access, withdrawal of consent, and erasure, the Restricted Committee emphasises that these are structural in nature and are severe in that the measures introduced by the company lead not only to individuals' requests being incorrectly processed, but also to individuals legitimately believing that their request has been complied with.

166. It thus recalls that on the date of the findings, data subjects making access requests did not receive the data contained in two tables of the company's database.

167. The Restricted Committee also points out that the company's consideration of a request for erasure has no effect other than to stop the display of personalised advertisements, with the company also continuing to retain the data of the individual requesting the request and even using it for other purposes.

168. With regard to the breach of the obligation to provide for an agreement between joint controllers, the Restricted Committee considers that the fact of not having more precise supervision of the processing carried out jointly with other stakeholders has deprived the data subjects of the full protection of their personal data afforded by the GDPR.

169. Secondly, the Restricted Committee considers that it is appropriate to apply the criterion set out in Article 83(2)(k) of the GDPR related to the financial benefits gained from the infringement.

170. It points out that the company's business model is based exclusively on its ability to display the most relevant advertising to Internet users to promote the products of its advertising customers, and therefore on its ability to collect and process a huge amount of personal data.

171. However, it emerges from this procedure that this collection and the processing in question are in breach of the requirements of the GDPR and the rights of data subjects, since the company is accused of not being able to demonstrate that these data subjects have given their consent to the processing of their data and that it has been established, in certain cases, that the company processed data for which the data subjects had not consented or had not given valid consent.

172. This means that the personal data collected and processed without valid consent of the individuals have enabled the company to unduly increase the number of individuals concerned by its processing, and therefore its financial income.

173. The Restricted Committee adds that the company also gained a financial advantage because it did not erase data by continuing to use data that had not been erased for the purpose of improving its technologies, which contributes to its competitiveness in the targeted advertising market.

174. Consequently, the Restricted Committee considers that an administrative fine should be imposed in view of the breaches of Articles 7, 12, 13, 15, 17 and 26 of the GDPR.

175. Secondly, with regard to the determination of the amount of the fine, the Restricted Committee points out that pursuant to the provisions of Article 20(III) of the French Data Protection Act and Article 83 of the GDPR, the company is incurring, in respect of the established breaches mentioned above, a financial penalty of a maximum amount of 20 million euros or 4% of its total worldwide turnover of the previous financial year, [redacted], whichever figure is the higher.

176. Therefore, in view of the company's liability, its financial capacities and the relevant criteria of Article 83(2) of the Regulation, referred to above, the Restricted Committee considers that a fine of forty million euros appears to be justified.

177. It notes that although the amount of the proposed penalty actually constitutes [redacted] of the company's worldwide turnover, it nevertheless remains below the legal ceiling of 4% provided for in Article 83(5) of the GDPR and Article 20(III, (7)) of the French Data Protection Act.

178. Furthermore, the Restricted Committee points out that the value of the fine may be higher than the profit generated by the data controller, insofar as this would be necessary to ensure the deterrent nature of the penalty (in this respect, see: EC, 1 March 2021, *Futura Internationale company*, no. 437808, pt. 6).

B. On publication of the decision

179. The company asks the Restricted Committee to not make its decision public.

180. However, the Restricted Committee considers that publication of this decision is justified in the light of the severity of the breach in question, the scope of the processing and the number of data subjects concerned.

181. It also notes that this measure will enable the data subjects to be informed of the existence of the processing carried out by the company and of the fact that it was able to process their data without their knowledge, or even despite their lack of consent. By being informed in this way, they will, where applicable, be able to assert their data protection rights vis-à-vis the company.

182. Finally, it considers that this measure is proportionate since the decision will no longer identify the company by name upon expiry of a two-year period following its publication.

FOR THESE REASONS

The CNIL's Restricted Committee after having deliberated, decided to:

- **impose an administrative fine against [redacted] SA in the amount of forty million euros (€40,000,000) with regard to the established breaches of Articles 7, 12, 13, 15, 17 and 26 of the GDPR**;

- **make its deliberation public, on CNIL's website and on the Légifrance website,** the deliberation no longer identifying the company by name upon expiry of a period of two years following its publication.

The Chair

Alexandre Linden

This decision may be appealed before the Conseil d'Etat within two months of its notification.