Decision of the Restricted Committee No. SAN-2023-006 of 11 May 2023 concerning [redacted]

The *Commission Nationale de l'Informatique et des Libertés* (CNIL - the French Data Protection Authority), met in its Restricted Committee consisting of Mr Philippe-Pierre Cabourdin, Vice Chairman, Ms Anne Debet, Ms Christine Maugüé, Mr Alain Dru and Mr Bertrand du Marais, members;

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 amended Decree No. 2019-536 of 29 May 2019 implementing French Data Protection Act No. 78-17 of 6 January 1978;

Having regard to Decision No. 2013-175 of 4 July 2013 adopting the internal rules of procedure of the CNIL;

Having regard to referral no. [redacted]

Having regard to Decision No. 2020-123C of 14 August 2020 of the Chair of the *Commission Nationale de l'Informatique et des Libertés* (CNIL) to instruct the general secretary to carry out or have a third party carry out an assignment to verify the processing of personal data accessible from the domain name "[redacted].fr" and any related processing;

Having regard to the CNIL Chair's decision appointing a rapporteur before the Restricted Committee of 29 November 2021;

Having regard to the report of Ms Valérie Peugeot, commissioner rapporteur, notified to [redacted] on 19 July 2022;

Having regard to the written observations made by [redacted] on 5 October 2022;

Having regard to the rapporteur's response to the observations notified on 21 November 2022 to the company's counsel;

Having regard to the written observations made by [redacted] on 5 January 2023;

Having regard to the other exhibits;

The following were present at the Restricted Committee session on 9 February 2023:

- Ms Valérie Peugeot, Commissioner, heard in her report;

In the capacity of representatives of [redacted]:

- […]

[redacted] having spoken last;

The Restricted Committee adopted the following decision:

I. Facts and proceedings

1. [redacted] (hereinafter "the company"), whose registered office is located at 1[redacted], is a subsidiary wholly owned by [redacted]. It was registered with the Trade and Companies Register on 17 November 1994 and the delegation was informed that it was founded in May 2000. In 2020, it employed around 30 employees. In 2020, it generated revenue of around €[redacted], with a net profit of around €[redacted], then in 2021 revenue of around €[redacted], with a net loss of €[redacted].

2. [redacted] was directly owned by the [redacted] until 28 June 2022, when the [redacted] sold to the [redacted] *"the media assets and digital activities of the Publishers division of [the company]* [redacted]", to which [redacted] belongs.

3. [redacted] publishes the French-speaking website www.[redacted] (hereinafter "the website"), which mainly provides articles, tests, quizzes and discussion forums related to health and well-being. The company's website is only available in French but can be accessed in all countries of the European Union and also outside Europe. [redacted] claimed around [redacted] unique visitors to the website between May 2021 and April 2022 and around [redacted] registered users with a user account created from the [redacted].fr website, on 8 April 2022. Users, whether registered or visitors, are mainly located in France and Belgium. Lastly, the company has around [redacted] users who answered at least one question from a questionnaire with a health theme between February 2020 and January 2021. The delegation was informed that of these users, [redacted] are located in France and [redacted] are located in Belgium.

4. On 26 June 2020, the Commission Nationale de l'Informatique et des Libertés (hereinafter "the CNIL" or "the Commission") received a complaint [redacted] association concerning all of the processing of personal data of users implemented by [redacted] on its website and, in particular, the methods of placing cookies on users' devices when they visit the website; the legal basis for processing users' personal data likely to be collected on the website when a user takes health-related tests; the obligation of transparency and the provision of information to users of the website, as well as the security of users' data.

5. Since [redacted] [redacted] publicly communicated regarding its complaint, [redacted] provided clarifications to the CNIL in a letter dated 7 July 2020 indicating, in particular, that it does not store any cookies or other trackers before the user has consented and is working on setting up consent for accessing tests likely to reveal the special categories of data.

6. Four audit engagements took place pursuant to Decision No. 2020-123C of 14 August 2020 by the Chair of the CNIL. On 9 September 2020, the CNIL first carried out an online audit from the domain www.[redacted].fr. On 1 October 2020, the CNIL then carried out an on-site audit of [redacted], on its premises located at [redacted] before carrying out, on 1 December 2020, a new on-line audit from the domain [redacted].fr. Lastly, on 8 February 2021, a documentary audit was carried out by sending a questionnaire addressed to the company.

7. These engagements gave rise to the preparation of minutes no. 2020-123/1, 2020-123/2 and 123/3 and letters and information communicated by the company on 13 and 21 October 2020, 19 November 2020, 8 December 2020, 18 January 2021 and 24 February 2021.

8. The main purpose of these engagements was to investigate the complaint referred to the CNIL and to verify the compliance of the processing of personal data accessible from the domain name [redacted].fr", as well as any related processing, with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter "the GDPR") and Act No. 78-17 of 6 January 1978 on information technology, files and civil liberties as amended (hereinafter "the French Data Protection Act").

9. In accordance with article 56 of the GDPR, on 3 December 2020 the CNIL informed all European supervisory authorities of its competence to act as lead supervisory authority regarding cross-border processing implemented by the company, due to the fact that the company's main establishment is located in France. After dialogue between the CNIL and the European data protection authorities in the framework of the one-stop shop mechanism, they are all concerned by the processing, since the website has visitors from all European Union Member States.

10. On 8 April 2021, [redacted] submitted a request for advice and support to the CNIL. It responded on 30 April 2021 that the charter for the support of professionals stipulated that it was unable to support organisations in their efforts to comply with the law when an audit procedure was under way.

11. On 27 October 2021, [redacted] sent the CNIL a letter containing the actions relating to the processing of personal data accessible from the "[redacted].fr" domain and any related processing, carried out by [redacted] since July 2020.

12. In order to examine these items, the CNIL Chair appointed Ms Valérie Peugeot as rapporteur on 29 November 2021, pursuant to Article 22 of the amended French Data Protection Act of 6 January 1978.

13. At the end of her investigation, on 19 July 2022 the rapporteur notified the company of a report detailing the breaches of Articles 5-1-e), 9, 13, 26 and 32 of the GDPR and Article 82 of the French Data Protection Act, which she considered established in this case. This report proposed to the Restricted Committee to issue an administrative fine to the company, as well as an

injunction, plus a periodic penalty payment to bring the processing into conformity with the provisions of Articles 5-1-e) and 32 of the GDPR and Article 82 of the Act. This report also proposed that this decision be made public, but that the company no longer be identifiable by name upon expiry of a period of two years following its publication.

14. On 5 October 2022, the company submitted observations in response to the sanction report.

15. The rapporteur responded to the company's comments on 21 November 2022.

16. On 5 January 2023, the company submitted further observations in response to those of the rapporteur.

17. In a letter dated 19 January 2023, the rapporteur informed the company's counsel that the investigation was closed, pursuant to Article 40, III, amended decree no. 2019-536 of 29 May 2019.

18. In a letter dated 19 January 2023, the company was informed that the case file was on the agenda of the Restricted Committee of 9 February 2023.

19. The rapporteur and the company presented oral observations at the Restricted Committee meeting.

II. Reasons for the decision

A. On the European cooperation procedure

20. 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 30 March 2023.

21. As of 27 April 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 breach of the obligation to retain personal data only for a period not exceeding the time necessary for the purposes for which the data is being processed, pursuant to Article 5(1)e of the GDPR

22. According to Article 5(1)(e) of the GDPR, personal data must be *"kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject*

to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ("storage limitation")".

a. <u>On the retention periods for data relating to tests and quizzes taken by users of the [redacted].fr website</u>

23. **The rapporteur** noted that the delegation found during the audits of 9 September, 1 October and 1 December 2020 that tests and quizzes (hereinafter "questionnaires" or "tests") were available on the company's website. During the audit of 1 October 2020, the delegation was informed that these questionnaires were drawn up by the company but that they were implemented and hosted by a subcontractor, [redacted].

24. **Firstly, the rapporteur** notes that <u>until 11 October 2020,</u> [redacted] retained the responses from the tests carried out by all logged and non-logged users, as well as their IP address, for a period of 24 months from their completion. The rapporteur thus noted that a file contained the responses from the tests taken by users on the subject of colon cancer, associated with their IP address.

25. The rapporteur then notes that a notice below the questionnaires on health subjects states that taking a test allows the user to know the result and, if necessary, to share it with friends. This also allows [redacted] to produce aggregated statistics on the use of the tests.

26. With regard to the first two purposes, the rapporteur notes that it emerges from the findings made that the test result is immediately displayed after the questions have been asked. She therefore considers that the retention of the user's responses to the questionnaire and his/her IP address does not appear necessary after the communication of the result to the user and its possible sharing by the user with his/her friends. These purposes cannot in any case justify the retention of the personal data concerned for a period of 24 months.

27. With regard to the third purpose, the rapporteur observes that in this case, the aggregated statistics are produced independently of the responses to the questionnaires, using audience measurement tools, which involve in particular placing and/or reading cookies or other trackers on the user's device for the purpose of measuring audience and the use of the user's IP address. She therefore considers that the retention of responses to the questionnaires after the end of the test is not necessary to produce aggregated statistics on the use of tests, which is done on an ongoing basis by other means.

28. **Secondly, the rapporteur** notes that <u>since 11 October 2020,</u> [redacted] has asked [redacted] to anonymise the data relating to the tests and quizzes as soon as they are collected. [redacted] says that since that date, its subcontractor has hashed the IP addresses – regarding which the company says that these are the *"only identifying data to which information relating to participation is attached"* – using the HMAC-SHA256 algorithm and that all of the data relating to participation in tests dating back more than three months from their completion

have been deleted to meet the three purposes mentioned above. In view of the information provided by the company, the rapporteur noted that the hash algorithm used by [redacted] actually only corresponds to an SHA256 function, without a hash key. The rapporteur notes that the use of the SHA256 function alone, while ensuring the integrity of personal data, does not anonymise it.

29. **In its defence, the company** argued that the alleged breach was unintentional, as it resulted from poor contract performance by its data processor, which had not complied with its contractual obligations firstly relating to the deletion of test data once it had been displayed, and secondly stipulating the use of a random variable in the IP address anonymisation function. [redacted] adds that it terminated its contract with [redacted] on 16 March 2021. Secondly, the company argues that the rapporteur invokes a hypothetical possession of the information enabling re-identification and that the risk of attack in terms of probability and severity is not described. It considers that the likelihood of the risk of [redacted] attacking its own systems is negligible and that its severity would be very limited in the absence of sensitive data. Lastly, [redacted] concludes that as of 11 October 2020, the test data contained only non-identifying data and that this data could be retained for an unlimited period.

30. **Firstly, the Restricted Committee** recalls that the personal data retention period must be determined according to the purpose pursued by the processing and that when this purpose is achieved, the data must in principle be deleted or anonymised.

31. In this case, the Restricted Committee notes that it is not disputed by the company that before 11 October 2020, the subcontractor of [redacted] retained the responses from the tests taken by users and their IP address for 24 months from their completion. The Restricted Committee considers that the retention of the user's responses to the questionnaire, as well as his/her IP address, does not appear necessary after the communication of the result to the user and its possible sharing by the user with his/her friends. Similarly, the retention of responses to questionnaires after the end of the test and the IP address is not necessary for the production of aggregated statistics on the use of tests, insofar as they can be, and in this case are, produced on an ongoing basis using audience measurement tools. In this respect, the Restricted Committee notes that the company does not justify a need to retain this data.

32. The Restricted Committee notes that the subcontracting agreement stated that the participants' IP addresses should not be collected by [redacted] concerning *"so-called 'sensitive' anonymous quizzes"*. Nevertheless, the Restricted Committee notes that [redacted] had access to dashboards, drawn up by its subcontractor, including the participants' responses to the tests and quizzes, as well as their IP addresses in pseudonymised form. The Restricted Committee notes that it was only following the complaint by [redacted] that [redacted] queried its subcontractor to find out the measures it implemented, even though it was aware of the collection of IP addresses by the latter, via said dashboards. Subsequently, the Restricted Committee notes that although [redacted] asked its subcontractor to remove the results of the tests as soon as they were displayed, it did not object

to the alternative solution proposed by [redacted] consisting of merely anonymising the IP addresses from 11 October 2020.

33. Although the data controller can decide to use a specialised service provider, in particular by entrusting it with a personal data subcontracting assignment, within the meaning of the GDPR, it remains obliged to ensure, through reasonable diligence, that compliance with the protection of personal data is effectively ensured. The adequacy of this diligence depends in particular on the data controller's skills and resources. The Restricted Committee recalls that the data controller's liability may be invoked due to the failure by the latter to perform regular checks on the technical and organisational measures taken by its subcontractor (*EC, 10th chamber, 26 April 2022, Optical Center, no. 449284*). In particular, the Restricted Committee has invoked the liability of a data controller for not exercising sufficient control over the service provided by considering that a mere contractual commitment by its broker aimed at *"compliance with the GDPR and the rules applicable to sales canvassing"* is not a sufficient measure, in its deliberation SAN-2022-021 of 24 November 2022 against [redacted].

34. It follows from the foregoing that the Restricted Committee considers that [redacted], which constitutes a company that has skills in the field of digital technology, has not sufficiently monitored the execution of its contractual instructions by its subcontractor and has not exercised satisfactory control over the technical and organisational measures it implemented to ensure compliance with the GDPR and, in particular, to ensure the absence of collection of personal data or the anonymisation thereof. Furthermore, the Restricted Committee notes that the data in question and users' IP addresses were accessible to [redacted].

35. **Consequently**, the Restricted Committee considers that the abovementioned circumstances constitute a breach of Article 5(1)(e) of the GDPR since, until 11 October 2020, the responses to the tests and quizzes and the IP addresses, which could be associated with user account information, were retained for a period of twenty four months from the time they were taken, which exceeded the purposes for which the data was processed.

36. **Secondly**, the Restricted Committee notes that, since 11 October 2020, [redacted] has hashed IP addresses with the SHA256 function without a hash key, and that all of the data relating to participation in tests dating back more than three months from their completion has been deleted.

37. The Restricted Committee notes that the Commission publicly communicated on its website on the use of the SHA256 function. As such, the Commission considered that while it ensures the integrity of personal data, the use of the SHA256 function without an associated hash key does not make it possible to ensure their anonymisation. The Restricted Committee therefore considers that the hash function used by [redacted]'s subcontractor cannot constitute an anonymisation solution, merely a solution to pseudonymise users' personal data, in that [redacted], which knew the hash parameters, and given the fact that the number of IP addresses is known and limited, could find, by brute force and within a reasonable time, the IP address of the persons who responded to the tests.

38. Since the data relating to users' participation in the tests and quizzes are not anonymised, the Restricted Committee considers, as it has previously expanded on, that their retention does not appear necessary after the communication of the result to the user and its possible sharing, since the result of the test is displayed immediately after the questions have been answered. Similarly, the Restricted Committee considers that their retention is not necessary for the production of aggregated statistics on the use of the tests. The Restricted Committee therefore considers that the company does not justify any need to retain this data for a period of three months.

39. **Consequently**, the Restricted Committee considers that the aforementioned facts constitute a breach of Article 5-1-e) of the GDPR for the facts identified as of 11 October 2020, since the responses to the tests and quizzes are retained for a period of three months from their completion due to ineffective anonymisation of the IP addresses, which exceeds the period necessary for the purposes for which they are processed.

40. The Restricted Committee notes that during the procedure, [redacted] stated that it complied with the requirements of Article 5-1-e), as since 16 March 2021 its subcontractor no longer collects the IP addresses of users, such that there is no need to send an injunction to the company on this point. The Restricted Committee nevertheless considers the breach established for past events.

b. <u>On the retention periods for accounts created by users of the [redacted].fr website</u>

41. **The rapporteur** notes that it emerges from the baseline relating to the company's retention periods that it anonymises *"data relating to the member account after three years of inactivity"*. The rapporteur also notes that during the on-site audit of 1 October 2020, the delegation was informed that after three years of inactivity, the *"information directly identifying accounts is deleted or replaced with random data for anonymisation purposes"*. However, the rapporteur notes that the anonymisation procedure put in place by the company does not meet the criterion of impossibility of individualisation due to the retention of the user's unique identifier, "id_user", and his/her pseudonymised username, which allows indirect re-identification of the latter.

42. The rapporteur considers that the procedure put in place by the company does not constitute an anonymisation solution, merely a pseudonymisation of the user's data.

43. **In its defence,** the company does not dispute that the user's unique identifier, "id_user", is retained. Nevertheless, the company believes that it does not allow account holders to be re-identified since it is not linked to any other data and that users' pseudonyms are anonymised after three years of inactivity, when they are replaced by a random sequence of numbers and letters. [redacted] therefore argues that the possibility and risk of persons being re-identified is not demonstrated. Lastly, the company stated that it is implementing a new procedure to anonymise all accounts of users who have been inactive for more than three years

from the end of October 2022. In this regard, it specifies that the unique identifiers of users who have been inactive for more than three years and the pseudonyms will be deleted, including those present on the forums and those in posts by other forum members.

44. **The Restricted Committee** recalls that the pseudonymisation of personal data is a reversible operation and that it is possible to find a person's identity by having additional information.

45. The Restricted Committee notes in this case that the company does not dispute that its data anonymisation policy included, concerning accounts inactive for more than three years, the retention of users' unique identifier, "id_user", as well as their pseudonymised username. However, the Restricted Committee considers that the retention of the unique identifier, "id_user", of the user, associated with his/her pseudonymised username, did not prevent the data associated with the accounts from being linked. As such, the Restricted Committee states that the company's procedure allowed for the retention of non-identifying data associated with accounts, such as posts on forums; the committee considers that it is common for users to communicate with each other using their usernames. The Restricted Committee considers that it was therefore possible in this case to find a person's identity by having additional information.

46. **Consequently**, the Restricted Committee considers that the aforementioned facts constitute a breach of Article 5-1-e) of the GDPR, since the measures taken by the company to properly anonymise the user's personal data at the end of a period of three years did not correspond to anonymisation but to a mere pseudonymisation of the data. The Restricted Committee notes that the company complied during the procedure with the implementation of a new anonymisation procedure, such that there is no need to send an injunction to the company on this point, but it nevertheless recalls that this cannot exempt the company from its liability for past events.

C. <u>On the failure to comply with the obligation to obtain the consent of data subjects to process special categories of personal data under Article 9 of the GDPR</u>

47. According to Article 9 of the GDPR, the processing of personal data revealing data concerning the health of a natural person is prohibited unless it falls within one of the conditions provided for in Article 9-2-a) to j) of the GDPR.

48. According to Article 4-15 of the GDPR, *"Health data" are "personal data relating to the physical or mental health of a natural person […]"*.

49. **The rapporteur** notes that it emerges from the observations made during the inspections of 9 September, 1 October and 1 December 2020 that the company processes health data when people answer the various health-related questionnaires offered to them on the [redacted].fr website.

50. The rapporteur then notes that the delegation found during its online audit of 9 September 2020 that the company did not obtain the web user's agreement on the use of his/her "sensitive" data to process his/her health data, since only a text containing a link to the personal data protection policy appeared below the test.

51. The rapporteur nevertheless notes that the delegation was informed, in a letter dated 19 November 2020, that the tests likely to lead to the collection of health data were removed from the site on 12 September 2020. These tests were once again accessible since 15 October 2020 and their participation is conditional on web users consenting, by means of a tick box, to the processing of their information. The rapporteur notes that it emerges from the findings of 1 December 2020 that the tick box is accompanied by the following notice: *"I accept that any sensitive data I enter through my responses to the test is used as described below and detailed in the Personal Data Protection Policy"*.

52. **In its defence**, the company argues firstly that the material scope of the notion of health data is not defined by the GDPR and that its vagueness is what led the company to seek CNIL's advice, in vain, more than six months before the appointment of the rapporteur, on 8 April 2021. Secondly, the company argues that the rapporteur has not provided evidence of systematic processing of health data by [redacted] in breach of Article 6 of the ECHR. The company argues that since it only has access to users' hashed IP addresses, it cannot identify the data subjects. Lastly, only a very small proportion of the tests offered on the [redacted] website, around 5%, would be likely to allow the collection of health data, assuming that this legal qualification is actually applicable.

53. **Firstly, the Restricted Committee** considers that the file demonstrating the collection of users' responses to a test entitled *"Colon Cancer: What are your risks*?*"* associated with their IP addresses makes it possible to observe the collection of information about the medical history (breast or endometrial cancer) or the physiological state of the data subjects (body mass index). The Restricted Committee notes that the company offered other tests accessible on its website on the theme of health, such as tests entitled *"How is your relationship with alcohol?"*, *"Are you lacking iron?"*, *"Are you eating too much sugar?"*, *"Could it be asthma?"*, *"Varicose veins: are you at risk?"*, *"Could it be Alzheimer's?"*, *"Stroke: what are your risks?"*, *"Hypertensive patients: are you exercising enough?"* and *"Do you have good hearing?"*.

54. The Restricted Committee notes that it was demonstrated that the IP address hashing system used did not prevent re-identification of the website's users and that [redacted] was able to associate test responses and IP addresses with account holders' data on the [redacted].fr website.

55. The Restricted Committee therefore considers that by having such information on the persons who responded to the tests, the company processes health data within the meaning of Article 4-15 of the GDPR.

56. **Secondly**, in the absence of other conditions that can be invoked to allow such processing in the present case under Article 9-2-b) to j) of the GDPR, the Restricted Committee considers that such processing can only be implemented based on the data subject's explicit consent to the processing of his/her personal data for one or more specific purposes, pursuant to Article 9-2-a) of the GDPR. The Restricted Committee recalls that the explicit nature of consent is analysed on a case-by-case basis and depends on the context of the processing of the health data. Where the service requested by the user necessarily involves the processing of health data, it is however necessary for the user to be fully aware that his/her health data will be processed and sometimes retained by the data controller, which in principle implies explicit information on this point when collecting consent.

57. The Restricted Committee notes that until the tests likely to lead to the collection of health data were removed from the website on 12 September 2020, no particular warning or mechanism for obtaining consent was included in the questionnaires to ensure that the person was aware of and consented to the processing of their health data.

58. The Restricted Committee recalls that it has already adopted corrective measures against data controllers not collecting individuals' express consent to the collection and processing of their sensitive data, notably in its deliberations no. 2016-405 of 15 December 2016 and no. 2016-406 of 15 December 2016.

59. **Thirdly,** the Restricted Committee notes that the CNIL's refusal to provide support, evidenced by the letter from the Commission's legal support department of 30 April 2021 in response to the company's request of 8 April 2021, falls within the framework provided for by the CNIL charter for the support of professionals, which includes the inability to support organisations in their compliance when an inspection procedure is in progress. The Restricted Committee notes that although the CNIL can respond to a request for advice after the audit if the criminal phase is not initiated, this is not the case here since a sanction procedure was subsequently initiated.

60. **Fourthly**, the Restricted Committee notes that according to the company, the portion of the tests proposed on [redacted]s website concerned by the collection of health data is around 5%. The Restricted Committee therefore notes that the processing of sensitive data concerns around [redacted] responses.

61. **Consequently**, the Restricted Committee considers that the aforementioned facts constitute a breach of the obligations of Article 9 of the GDPR since, until 12 September 2020, the data were processed in breach of the conditions defined by this article.

62. Lastly, the Restricted Committee notes that the tests likely to lead to the collection of health data have been accessible again since 15 October 2020 and that participation in these tests is conditional on web users consenting, by means of a tick box, to the processing of their information. It notes that the company came into compliance during the audit procedure, which nevertheless does not call into question the existence of the breach for past facts.

D. <u>On the breach of the obligation to inform data subjects pursuant to Article 13 of the GDPR</u>

63. According to Article 13 of the GDPR, the data controller must provide the data subject with several pieces of information at the time the data is obtained.

64. **In her initial report**, the rapporteur noted that the information provided by the company on the website www[redacted].fr did not specify the legal basis for the processing carried out. The rapporteur also noted that there was no mention of whether the provision of information was mandatory in that it was of a regulatory or contractual nature or whether it required the conclusion of a contract and whether the data subject was required to provide the personal data.

65. **In its defence,** the company communicates its "Data Protection Policy" and says that this contains references to the applicable legal bases.

66. **During the session**, taking into account the information provided by the company as part of the investigation, the rapporteur proposed to the Restricted Committee to not uphold the breach in connection with the information provided by the company on the website, considering that the "Data Protection Policy" accessible from the website www.[redacted].fr contains information on the legal basis applied for the processing carried out and the fact that certain information determines the creation of a user account or is regulatory in nature.

67. **The Restricted Committee** considers that the breach of Article 13 of the GDPR is not established.

E. <u>On the failure to provide a formal legal framework for the processing operations carried out jointly with another data controller pursuant to Article 26 of the GDPR</u>

68. Under Article 26 GDPR: *"1. Where two or more data controllers jointly determine the purposes and means of processing, they are joint controllers. They shall in a transparent manner determine their respective responsibilities 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 unless, and in so far as, the respective responsibilities of the data controllers are determined by Union or Member State law to which the data controllers are subject. The arrangement may designate a contact point for data subjects.*
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. The essence of the arrangement shall be made available to the data subject.
3. Irrespective of the terms of the arrangement referred to in paragraph 1, the data subject may exercise his or her rights under this Regulation in respect of and against each of the controllers."

69. **The rapporteur** notes that it emerges from the information provided by [redacted] that it considers itself jointly liable for [redacted] and [redacted]. However, the rapporteur notes that no contract concluded between the company and these two entities contains a provision concerning the definition of the parties' respective obligations pursuant to Article 26 of the GDPR. The rapporteur notes, however, that on 24 February 2021, the company sent amendments to the existing contracts that define the parties' respective obligations.

70. **In its defence**, the company did not question the reality of the alleged breach but argued that no data subjects had complained that they had not received the necessary information or that their rights had not been respected and that the exercise of the persons' rights was guaranteed. The company consequently submits that this breach should be set aside.

71. **The Restricted Committee** notes that it emerges from the information communicated by [redacted] that the latter is jointly liable with [redacted], firstly, with regard to processing related to the marketing of advertising spaces on the website www.[redacted].fr, and [redacted], secondly, for the processing of data using the technical tools and functional structures made available by the latter.

72. Although the information communicated by [redacted] certifies that amendments relating to the protection of personal data, defining the parties' respective obligations, have been concluded since 24 February 2021, in accordance with the requirements of Article 26 of the GDPR, the Restricted Committee notes that the joint liability relationship was not governed at the time of the CNIL's audits.

73. **Therefore,** in view of the foregoing, the Restricted Committee considers that the aforementioned facts constitute a breach of Article 26 of the GDPR, since the absence of a complaint or prejudice for users is inoperative. The Restricted Committee notes the compliance measures carried out during the procedure, which cannot exempt the company from its liability for the breach found.

F. <u>On the breach of the obligation to ensure the security of personal data pursuant to Article 32 of the GDPR</u>

74. Under Article 32 GDPR: *"1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*
a) the pseudonymisation and encryption of personal data;
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services."

<u>a. On the lack of security relating to user navigation on the website</u>

75. **The rapporteur** noted that during the on-site audit on 1 October 2020, the company told the delegation that before October 2019, the pages relating to the tests implemented on the www[redacted].fr website by [redacted] had been using the "HTTP" communication protocol by default. The rapporteur therefore notes that this communication protocol was present on the test pages from which personal data – including health data – was entered by users.

76. The rapporteur nevertheless notes that the delegation found on 9 September 2020 that said pages now used the "HTTPS" communication protocol.

77. **In its defence,** the company also argues that the GDPR stipulates no obligation to implement the HTTPS protocol and that the CNIL cannot therefore impose a sanction for using the "HTTPS" protocol on the grounds of a mere recommendation, as there has been no data breach. The company also states that the absence of the "HTTPS" protocol before October 2019 was the prevailing market practice and in line with the "state of the art" in this area. Lastly, the company argued that the CNIL delegation had not been able to establish the facts, since the breach was based solely on statements made by the company's employees, which could not be used as a basis for a sanction, unless [redacted]'s right not to incriminate itself was disregarded.

78. **Firstly, the Restricted Committee** recalls that, pursuant to article 32 of the GDPR, it is incumbent on the data controller to take *"appropriate technical and organisational measures to ensure a level of security appropriate to the risk"*.

79. The Restricted Committee considers first of all that the occurrence of a data breach is not necessary for the characterisation of a breach and that it has repeatedly adopted financial penalties in which the establishment of a breach of Article 32 GDPR is based on the absence of sufficient measures to guarantee the security of personal data, in particular in deliberations No. SAN-2019-006 of 13 June 2019 and No. SAN-2021-021 of 28 December 2021 against [redacted].

80. In this case, the Restricted Committee notes that the "HTTP" protocol is a communication protocol that does not allow authentication of the website, nor encryption of data when sent to [redacted]'s servers, which does not guarantee the authenticity of the website viewed, nor the integrity and confidentiality of the data exchanged, exposing the personal data processed through these pages to the risks of listening, interception or modification without the user's knowledge, which may lead to a breach of the data subjects' privacy.

81. The Restricted Committee notes by way of clarification that the need to ensure the confidentiality of the channels for the transmission of personal data has been highlighted by the French National Agency for Information Security (ANSSI) since 2013, notably in its *"Recommendations for the implementation of a website: achieving proficiency in the standards of browser security"*, which states that *"The implementation of HTTPS on a website*

or a web application is a security guarantee based on TLS to ensure the confidentiality and integrity of the information exchanged, as well as the authenticity of the server contacted. The absence of this guarantee can lead to many abuses without malicious intent."

82. The Restricted Committee also notes that since the publication of its *"Personal Data Security*" guide in 2018, the Commission has consistently recommended that the "TLS" protocol be implemented as a basic precaution, using only the most recent versions and verifying its proper implementation.

83. The Restricted Committee considers that while the ANSSI's recommendations and the CNIL guide are not imperative, they are referred to for clarification purposes and nevertheless set out the basic safety precautions corresponding to the state of the art. The Restricted Committee therefore considers that the use of the "HTTPS" protocol fell within the scope of the state of the art before October 2019, contrary to what the company argues.

84. The Restricted Committee also notes that the personal data in question are sensitive data, since they are users' responses to tests involving the collection of health data associated with their IP address. Therefore, taking into account the risks to the protection of personal data and privacy leads the Restricted Committee to consider that the measures deployed to guarantee data security in this case were inadequate, given that personal data were transmitted to [redacted]'s servers.

85. Consequently, the Restricted Committee considers, with regard to the personal data subject to the processing, that the failure to implement the basic security measure that constitutes the use of the "HTTPS" protocol or another equivalent security measure characterises a breach of Article 32 of the GDPR. However, the Restricted Committee found that during its 9 September 2020 audit, the pages relating to the tests implemented on the website www.[redacted].fr used the "HTTPS" communication protocol. It nevertheless reiterates that the compliance measures taken cannot absolve the company from responsibility for the failure observed.

86. **Secondly,** the Restricted Committee recalls that although a person's right not to participate in his/her own incrimination implies that the prosecution cannot establish its argument by using evidence obtained by coercion or pressure, it considers that all of the information collected by the CNIL has been collected within the framework of the audit procedure based on Article 19 of the French Data Protection Act. The Restricted Committee notes that the company was able to make observations at the end of the drafting of the minutes, as well as to challenge the analysis made of these statements. However, the Restricted Committee notes that the company does not dispute having used the "HTTPS" protocol until October 2019. Lastly, the Restricted Committee notes that the company's counsel, [redacted], was present during the on-site audit carried out on 1 October 2020 by the CNIL. The Restricted Committee considers that there has been no constraint contrary to Article 6 of the European Convention on Human Rights when the employees of [redacted] voluntarily made statements concerning the use of the "HTTP" protocol during the audit procedure.

87. **Consequently**, since [redacted] disregarded a basic security measure and incurred risks to the security of its users' personal data until October 2019, the Restricted Committee considers that the aforementioned facts constitute a breach of the obligations of Article 32 of the GDPR for past events.

b. On the lack of security in storing website users' passwords

88. **The rapporteur** notes that the delegation found that the company retains the passwords of the website's users in a format obtained via a three-step process: passwords are initially converted using the MD5 hash algorithm, then the result obtained is converted a second time via the "password_hash" function of the PHP programming language used by default with the Bcrypt algorithm and, lastly, the result obtained is stored in the company's database. The rapporteur considers that these methods of storing passwords are insufficient to ensure the security of the personal data to which they allow access (personal space containing in particular the last name, first name, date of birth, email address and gender of the data subject).

89. **In its defence**, the company acknowledges that the MD5 algorithm does not provide sufficient guarantees for keeping secure password hashes, which is why it decided to combine it with the Bcrypt function. The company says that this technique makes it possible to create longer, and therefore stronger, passwords. It argues that this technique is still widely used by websites and was considered a valid security technique until very recently, as researchers have been reporting the limitations of this method only since 2020. Furthermore, the company states that no attack has been documented and therefore that the high risk mentioned by the rapporteur is hypothetical and does not justify the imposition of a sanction. Lastly, the company said that it had deleted the pre-hashing since 7 September 2022, as well as all user passwords, and they would have to change their passwords the next time they logged on. The company added that the new passwords are stored using the processes under this new method, which represents a *"non-reversible and secure"* encryption function.

90. **Firstly, the Restricted Committee** recalls that securely storing passwords constitutes a basic precaution in the protection of personal data.

91. The Restricted Committee also recalls by way of clarification that since 2013, the ANSSI has specified best practices with regard to the storage of passwords, indicating that they must *"be stored in a form converted by a one-way cryptographic function (hashing function) that is slow to calculate, such that PBKDF2"* and that *"the conversion of passwords must involve a random salt to prevent an attack by pre-calculated tables"*.

92. The Restricted Committee also notes that the Commission recommends in its deliberation adopting a password recommendation, no. 2017-012 of 19 January 2017, *"that it should be converted by means of a non-reversible and secure cryptographic function (i.e. using a public algorithm deemed to be strong, the implementation of which is free of known vulnerability), integrating the use of a salt or a key."*

93. The Restricted Committee considers that the recommendations of the ANSSI and the CNIL are referred to for clarification purposes and set out the basic security precautions corresponding to the state of the art.

94. The Restricted Committee recalls that combining encryption algorithms to store personal data, while technically possible, is not recommended.

95. The Restricted Committee notes, in this case, that the MD5 algorithm is no longer considered as state of the art since 2004 and that its use in cryptography or security is prohibited. It recalls that the ANSSI subsequently withdrew it from the general security standards in 2014, recalling that the MD5 algorithm was considered "permanently broken".

96. The Restricted Committee also considers that the process of first converting the password using the MD5 function then introduces a vulnerability in the Bcrypt function. It recalls that the Open Web Application Security Project (OWASP) discourages this practice, as it introduces a risk of a particular form of attack by credential stuffing, since the Bcrypt function is combined with another function, such as the MD5 function. The Restricted Committee notes that such a configuration exposes the data to the risk of an attack based on the reuse of the MD5 and password pairs from leaked databases.

97. **Therefore**, the Restricted Committee considers that the company's password management policy does not utilise satisfactory measures to ensure the security of the personal data to which they allow access.

98. **Secondly,** the Restricted Committee recalls that the occurrence of an attack or a data breach is not necessary for the characterisation of a breach of Article 32 of the GDPR.

99. **Consequently**, the Restricted Committee considers that the above facts constitute a breach of article 32 of the GDPR. It nevertheless notes that [redacted] indicated that it had implemented a new method of storing passwords using a non-reversible and secure encryption function since 7 September 2022, such that there is no need to issue an injunction to the company on this point. The Restricted Committee nevertheless recalls that the compliance measures taken cannot absolve the company from its responsibility for past events.

G. <u>On the breach of obligations under Article 82 of the French Data Protection Act</u>

[Breach not subject to cooperation on which the supervisory authorities concerned do not have to take a position.]

100. Pursuant to Article 82 of the French Data Protection Act, transposing Article 5(3) of the "ePrivacy" directive, it is provided that: *"Any subscriber or user of an electronic communications service must be informed in a clear and complete manner, unless he or she has been previously informed by the data controller or their representative:*

1° of the purpose of any action aimed at electronically accessing information already stored in their electronic communications terminal equipment, or writing information to this equipment;
2° Of how he or she can object to it.
Such access or recording may only take place provided that, after receiving such information, the subscriber or user has expressed his or her consent which may result from the appropriate parameters of his/her connection device or any other device under his or her control.
These provisions shall not apply if access to the information stored in the user's terminal equipment or the recording of information on the user's terminal equipment:
1° Either is for the exclusive purpose of enabling or facilitating communication by electronic means;
2 Or is strictly necessary for the provision of an online communication service at the express request of the user."

a. <u>On the storage of cookies on the user's device without consent</u>

101. **The rapporteur** notes that during the online audit of 1 December 2020, the delegation found during two different browsing sessions, based on a blank browsing history and before any action on its part, that two cookies were stored on its device as soon as it reached the home page of the website www [redacted].fr. The rapporteur notes that the company said that the purpose of one of these cookies, the cookie called "[redacted], was to circulate targeted advertising.

102. **In its defence**, the company does not dispute these facts. It nevertheless argues that the storage of the advertising cookie before any action by the user resulted from its dual purpose, technical and advertising, and says that it had finalised its compliance as of 21 December 2020. During the dialogue, it demonstrates by the communication of a bailiff's report that as of 29 August 2022, no cookies other than strictly technical cookies are now stored on users' devices before their consent is obtained.

103. **The Restricted Committee** recalls that Article 82 of the French Data Protection Act expressly states that the operations of accessing or registering information on a user's device may only take place after the user has expressed his/her consent, only cookies whose exclusive purpose is to allow or facilitate communication by electronic means, or cookies being strictly necessary for the provision of an online communication service at the express request of the user, being exempt from this obligation.

104. The Restricted Committee considers that advertising cookies, not having the exclusive purpose of allowing or facilitating communication by electronic means and not strictly necessary for the provision of an online communication service at the express request of the user, may not be stored or read on the person's device, in accordance with Article 82 of the French Data Protection Act, if he or she has not provided his/her consent.

105. **Consequently**, the Restricted Committee considers that by allowing the storage and reading of the "[redacted]" cookie on the device of persons when they reach the [redacted].fr website, without first obtaining their consent, while its purpose is to distribute targeted advertising, the

company deprived them of the possibility granted to them by Article 82 of the French Data Protection Act to make a choice as to the storage of trackers on their terminal equipment. The Restricted Committee notes that several million people were concerned, with the company claiming around 276 million unique visitors to the [redacted].fr website between February 2020 and February 2021.

106. The Restricted Committee notes that [redacted] demonstrated during the procedure that from 29 August 2022, no cookies other than strictly technical cookies are now stored on users' devices before their consent is obtained, such that there is no need to send an injunction to the company on this point. The rapporteur nevertheless reiterates that the compliance measures taken cannot absolve the company from its responsibility for past events.

b. <u>On the inadequacy of the mechanism offered to users to reject the storage of cookies</u>

107. **The rapporteur** notes that the delegation found, during the online audit of 1 December 2020, the presence of a mechanism allowing users to "configure cookies" ("consent management platform" mechanism, hereinafter CMP). During this audit, the delegation clicked on the box titled "REJECT ALL" at the bottom-right of the CMP displayed on the site. However, the rapporteur noted that the "[redacted]" advertising cookie, which had already been stored, remained stored on the user's terminal equipment. Subsequently, the rapporteur noted that after browsing to another page of the website to view an article online, the delegation found that the same [redacted] cookie previously stored was still stored on the user's terminal equipment. Lastly, the rapporteur also noted that the delegation noted the storage on the user's terminal equipment of two new cookies for the purpose of distributing targeted advertising, called "[redacted]" and [redacted], respectively stored by third parties, the partners [redacted] and [redacted], under the domain names "[redacted].com" and "www.[redacted].fr", despite the user's rejection.

108. **In its defence**, the company does not dispute these facts. Nevertheless, the company reiterates the particular context in which the online audit took place, as CNIL had published on 17 September 2020 its new guidelines on cookies, which had important consequences for tools to collect consent and reject cookies. In addition, the company argues that unintentional technical malfunctions led to the storage of the two advertising cookies after the delegation rejected and produces a conversation taken from a [redacted] forum dating from January 2021, in which a publisher of a website reported a malfunction to [redacted] relating to the cookie called [redacted]. It therefore argues that the breach is unintentional. Lastly, the company demonstrates by the communication of the aforementioned bailiff's report that from 29 August 2022, in the event of rejection by the user, no cookies other than strictly technical cookies are now stored on his/her device.

109. **Firstly, the Restricted Committee** notes that information reading and/or writing on the user's electronic communications terminal equipment takes place after he/she has stated his/her rejection of the storage and reading of cookies for advertising purposes and browsed to another

page of the website. The Restricted Committee considers that the means provided to persons to enable them to reject any action aimed at accessing information already stored on their terminal equipment or to record information on this equipment are not effective.

110. Subsequently, the Restricted Committee considers that [redacted], as it publishes the [redacted].fr website, has a share of responsibility in compliance with the obligations of Article 82 of the French Data Protection Act for the operations of reading and/or writing information carried out on users' devices when visiting its website, including those carried out by third parties that are its business partners. The Restricted Committee notes that the Council of State ruled that the obligations incumbent on the publisher of a site include that of checking with its partners, firstly, that they do not issue trackers through the site that do not comply with the regulations applicable in France and, secondly, to take any useful steps with them to put an end to any breaches (EC, 6 June 2018, Editions Croque Futur, no.412589). The Restricted Committee recalls that it has already sanctioned a breach of Article 82 of the aforementioned Act in connection with operations of reading and/or writing information carried out by third parties on the device of users in deliberation No. SAN-2021-013 of 27 July 2021 against [redacted].

111. **Secondly,** the Restricted Committee recalls that the CNIL has implemented a compliance plan on the issue of cookies spread over several years and that it particularly communicated on these developments, notably from 2019 on its website, and on 1 October 2020 alongside the publication of the guidelines and the recommendation of 17 September 2020. Compliance was due by 1 April 2021 and hundreds of thousands of stakeholders, from the smallest to the largest websites, have complied and have introduced a "Reject" or "Continue without accepting" button in their consent collection interface. The Restricted Committee notes that the breaches found during the online audit of 1 December 2020, on storing cookies on the user's device without their consent and before any action, as well as after they have clicked on the " REJECT ALL" button, were practices identified by CNIL as being contrary to Article 82 of the French Data Protection Act as early as 2013. It considers that the context of the publication by the CNIL of its new guidelines on cookies, of which the audit of 1 December 2020 is part, does not therefore make it possible to mitigate the scope of the breaches identified and that the company had to be both particularly vigilant with regard to compliance with its obligations in terms of cookies and also attentive to developments in the regulations on this subject, particularly following the enhancement of the conditions of consent following the entry into force of the GDPR.

112. **Thirdly**, concerning the dialogue and the documents communicated as part of the investigation, the Restricted Committee considers that the failures invoked by the company do not minimise its liability in that they are subsequent to the CNIL's audit and concern another website publisher. The Restricted Committee considers, in any event, that [redacted] was responsible for ensuring compliance with the obligations of Article 82 of the French Data Protection Act and thus to check with its partners that they did not issue, through its site, trackers that do not comply with the regulations applicable in France and to take all useful steps with them to put an end to breaches, which the company did only after the CNIL's audit of 1 December 2020.

113. **Consequently**, it follows from all of these elements that by storing cookies subject to consent on the user's device before any action on his/her part and depriving of any effect the rejection of the storage and reading of cookies for advertising purposes, [redacted] disregarded the provisions of Article 82 of the French Data Protection Act.

114. The Restricted Committee notes that [redacted] demonstrated during the procedure that from 29 August 2022, no cookies other than strictly technical cookies are now stored on users' devices before their consent is obtained, or in the event of users' rejection, such that there is no need to send an injunction to the company on this point. The rapporteur nevertheless recalls that the compliance measures taken cannot absolve the company from responsibility for past events.

III. <u>On the corrective measures and their publication</u>

115. Under the terms of Article 20 III of the amended Act of 6 January 1978:

"When the controller or its subcontractor fails to comply with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or this law, the chairman of the CNIL may also, if applicable, after sending the warning provided for in point I of this article or, where applicable, in addition to an order provided for in II, contact the CNIL's Restricted Committee with a view to the imposition, after proceedings in which both sides are represented, of one or more of the following measures: […] 7. With the exception of cases where the processing is implemented by the State, an administrative fine may not exceed EUR 10 million or, in the case of an undertaking, 2% of the total worldwide annual turnover of the preceding financial year, whichever is 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."

116. Article 83 of the GDPR states that *"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. <u>On the issue of an administrative fine and its amount</u>

a. <u>On the issue of an administrative fine</u>

117. The company considers that the proposed administrative fine is disproportionate to the alleged breaches relating to old facts and its conduct, as it has implemented the necessary remedial measures.

118. The Restricted Committee notes that, in imposing an administrative fine, it must take into account the criteria specified in article 83 of the GDPR, such as the nature, severity and duration of the infringement, the scope or purpose of the processing concerned, the number of people affected, the measures taken by the data controller to mitigate the damage suffered by the data subjects, the fact that the breach was committed due to negligence, the degree of cooperation with the supervisory authority and, in some cases, the level of damage suffered by the data subjects.

119. The Restricted Committee first notes the number and extent of the breaches alleged against the company, including four breaches of the GDPR.

120. With regard to the breach of the principle of limiting the personal data retention period, the company demonstrated negligence by retaining the data relating to the tests taken by users of the website [redacted] for a period exceeding the purposes for which they were processed. The Restricted Committee notes, however, that this is a breach resulting from the subcontractor's non-compliance with its own contractual obligations and that [redacted] has terminated any contractual relationship with it. With regard to the periods for the retention of accounts created by the website's users, the Restricted Committee recalls that the measures taken by the company did not make it possible to anonymise the personal data of a user whose account had been inactive for more than three years. It notes that this breach concerns a large number of people, with the company claiming around [redacted] users with an account created from the website and [redacted] users who answered a question of a test on the health theme.

121. With regard to the failure to obtain data subjects' consent to the processing of sensitive health-related data, the Restricted Committee first notes that the company has been negligent in refraining from obtaining users' consent when it offered them tests involving the collection of data relating to their health. It then notes that this breach concerns a large number of people, with the company indicating that 5% of the tests offered would be likely to allow the collection of health data, which amounts to around [redacted] responses. The Restricted Committee also considers that it is appropriate, with regard to this breach, to take into account the nature of the actor concerned and its sector of activity. Indeed, since [redacted] circulates digital content relating to health, it cannot avoid such an obligation.

122. With regard to the breach of the obligation to ensure the security of personal data, the Restricted Committee considers that it has contributed to accentuating the fact that the personal data of the persons processed in this context have not benefited from the protection offered by the GDPR.

123. With regard to the breach relating to cookies stored on the user's device when visiting the company's website, the Restricted Committee considers that the absence of obtaining consent concerned each of the persons who visited the website in question, i.e. necessarily several

million people, given the fact that the company claims around [redacted] unique visitors to the [redacted].fr website between February 2020 and February 2021.

124. Lastly, the Restricted Committee notes that the compliance measures put in place following the notification of the sanction report do not concern all of the breaches and do not exonerate the company from its responsibility for the breaches observed.

125. **Consequently,** the Restricted Committee considers that an administrative fine should be imposed with regard to the breaches constituted by Articles 5- 1-e), 9-2, 26 and 32 of the GDPR and with regard to the breach constituted by Article 82 of the French Data Protection Act.

b. <u>On the amount of the administrative fine</u>

126. The Restricted Committee notes first of all that the breaches relating to Articles 5-1-e) and 9-2 of the GDPR are breaches of key principles of the GDPR which, under Article 83 of the GDPR, may be subject to an administrative fine of up to €20,000,000 and up to 4% of annual revenue, whichever is greater.

127. The Restricted Committee subsequently notes that administrative fines must be both dissuasive and proportionate. The Restricted Committee notes that in 2021, [redacted] generated revenue of around €[redacted] and a net loss of around [redacted].

128. The Restricted Committee notes that [redacted] is wholly owned by the single-member simplified joint stock company [redacted], which is itself owned by the [redacted] group. In 2021, the latter generated consolidated revenue of around €[redacted] and an increased net profit of around €[redacted].

129. **Therefore**, with regard to the company's liability, its financial capacity and the relevant criteria of Article 83 of the Regulation mentioned above, the Restricted Committee considers that an administrative fine of two hundred and eighty thousand euros, with regard to the breaches constituted by Articles 5-1-e), 9-2, 26 and 32 of the GDPR, and an administrative fine of one hundred thousand euros with regard to the breaches set out in Article 82 of the French Data Protection Act appear justified.

B. <u>On publication of the decision</u>

130. The company contests the rapporteur's proposal to make this decision public. It considers that given that the facts took place in the past and that the company is now compliant, the educational and informative virtue of the measure to publicise the sanction no longer exists. In order to justify this request to make the decision public, the rapporteur invokes in particular the number of persons concerned and the age of certain data.

131. The Restricted Committee considers that the publication of this Decision is justified in view of the severity of the breaches in question and the number of data subjects. The Restricted

Committee also considers that the publication of the sanction will in particular inform all the data subjects of the consequences of the breaches.

132. Lastly, the measure is proportionate since the decision will no longer identify the company by name upon expiry of a period of two years following its publication.

FOR THESE REASONS

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

- **issue to [redacted] an administrative fine of two hundred and eighty thousand euros (€280,000) in respect of the breaches committed under Articles 5(1)(e), 9(2), 26 and 32 of Regulation (EU) No. 2016/679 of 27 April 2016 on data protection;**

- **issue to [redacted] an administrative fine of one hundred thousand euros (€100,000) in respect of the breach of Article 82 of the French Data Protection Act as amended;**

- **publish its decision on the CNIL and Légifrance websites, which will no longer identify the company at the end of a two-year period following its publication.**

The Vice-Chairman

[redacted]

This decision may be appealed before the *Conseil d'Etat* (French Council of State) within two months of its notification.