Deliberation of the Restricted Committee No. SAN-2023-008 of 8 June 2023 concerning [redacted]

The Commission nationale de l'Informatique et des Libertés (CNIL - French Data Protection Authority), met in its Restricted Committee consisting of Mr Alexandre Linden (Chair), Mr Philippe-Pierre Cabourdin (Vice Chair), Mr Alain Dru, Mr Bertrand du Marais and Ms Christine Maugüé (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 ("GDPR");

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. 2020-267C of 20 October 2020 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;

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

Having regard to the report of Mrs Sophie Lambremon, the commissioner rapporteur, notified to [redacted] on 7 July 2022;

Having regard to the written observations made by [redacted] on 8 August 2022;

Having regard to the other exhibits;

The following were present at the Restricted Committee session on 15 September 2022:

- Mrs Sophie Lambremon, Commissioner, heard in her report;

In the capacity of representatives of [redacted]:

- […]

[redacted] having spoken last;

The Restricted Committee has adopted the following decision:

I. Facts and proceedings

1. [redacted] (hereinafter [redacted] or the "company") is a simplified joint-stock company incorporated in the [redacted], whose registered office is located at [redacted]. The company operates several websites to provide its customers with clairvoyance readings by chat or phone, [redacted]. The company employs [redacted] people.

2. In 2019, the company generated net revenue of [redacted] and net income of [redacted]. In 2020, its net revenue amounted to [redacted], with a net loss of [redacted].

3. A news article [redacted] revealed the existence of a personal data breach concerning the data stored on [redacted]'s server. The article claimed that the company's database had been freely accessible on the Internet until [redacted] 2020, since it was not protected by any specific security measures. A large amount of data, including identifying data and contact details, would therefore have been exposed.

4. On 21 January 2021, an auditing delegation from France's data protection authority "Commission nationale de l'informatique et des libertés" (hereinafter "CNIL" or the "Commission") carried out a document audit by sending a questionnaire to the company, which replied with a letter that was received on 25 March 2021.

5. An online audit was also carried out on 15 April 2021 into the [redacted] website published by the company. Report no. 2020-267/1 prepared at the end of the audit was served to the company on 26 April 2021. The company provided the delegation with additional information by email on 17 May and 18 June 2021.

6. An on-site audit was conducted on 15 July 2021. Report no. 2020-267/2 prepared at the end of the audit was served to the company on 21 July 2021. Subsequently, the company provided the delegation with additional information in its letters of 26 August, 20 September, 19 October and 3 November 2021.

7. [redacted]'s database includes the email addresses of [redacted] customers and [redacted] prospects, as can be seen from the company's observations in response.

8. In accordance with Article 56 of the GDPR, the CNIL informed all European supervisory authorities of its competence to act as lead supervisory authority for cross-border processing implemented by [redacted], due to the fact that the company's single establishment is located in France. Following exchanges between the CNIL and the European data protection authorities as part of the one-stop-shop mechanism, Belgium, Luxembourg, Italy, Spain, Portugal, Bulgaria, Berlin and Ireland warranted that they were concerned by the processing operation.

9. To examine these items, the CNIL Chair appointed Ms Sophie Lambremon as rapporteur on 23 December 2021, on the basis of Article 22 of the amended Act of 6 January 1978 (hereinafter the "French Data Protection Act").

10. On 7 July 2022, the rapporteur served a report to [redacted] containing details of the breaches of the GDPR and French Data Protection Act that she considered had been committed in the case in point. This report contained a proposal for the Restricted Committee to impose an administrative fine on the company. It also proposed that this decision be made public and that the company no longer be identifiable by name upon expiry of a two-year period following its publication.

11. On 2 August 2022, [redacted] asked for time to respond to the rapporteur's report. By letter of 4 August 2022, the Chair of the Restricted Committee notified the company of its decision to deny the request.

12. The company responded to the sanction report with written observations dated 08 August 2022.

13. In a letter dated 16 August 2022, 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.

14. In a letter dated 22 August 2022, the company was informed that the case file was on the agenda of the Restricted Committee session of 15 September 2022.

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

II. Reasons for the decision

16. Pursuant to Article 60(3) of the GDPR, the draft decision adopted by the Restricted Committee was transmitted to the eight competent European supervisory authorities concerned on 4th May 2023.

17. As of 1st 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.

A. Regarding the breach of the obligation to ensure the appropriateness, relevance and non-excessive nature of the personal data processed in accordance with Article 5(1)(c) of the GDPR

18. Article 5(1)(c) of the GDPR states that personal data must be *"adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)"*.

19. **Firstly, the rapporteur** points out that the company systematically records all phone calls between telephone operators and prospects, as well as between clairvoyants and customers, with the aim of checking service quality, proving that a contract has been formed and responding to potential court orders. The rapporteur considers that this leads the company to collect data that are not limited to what is necessary in relation to the purposes pursued.

20. **In its defence, the company** indicates that it has stopped offering its customers clairvoyance readings over the phone.

21. To justify the past events, the company indicates that the recordings allowed it to check what the clairvoyants said during the readings, especially to assess their skills. In its view, recording just a sample of the readings would fail to meet its needs.

22. **The Restricted Committee** duly notes that phone-based clairvoyance readings have been stopped, which means that there are no recordings of phone calls between telephone operators and prospects, and between clairvoyants and customers.

23. However, the Restricted Committee notes that, on the day of the audit, the company systematically recorded such phone calls in full for the purpose of checking service quality, proving that a contract has been formed and responding to potential court orders.

24. The Restricted Committee notes that the company does not provide any justification for the previous need to systematically record all calls between telephone operators and prospects, as well as between clairvoyants and customers, in order to check service quality, prove that a contract has been formed and respond to potential court orders.

25. However, a controller cannot implement a personal data processing operation without first ensuring that it is necessary for fulfilling its needs, especially where it is based on a mechanism that is particularly intrusive for its employees.

26. With regard to systematically recording phone calls in full for quality control purposes, the Restricted Committee considers that the purpose of checking the quality of the service provided by the telephone operators and clairvoyants can be achieved by a less intrusive method.

27. In this respect, it notes that the implementation of an ad hoc and random system for recording only a few phone calls would allow the person responsible for quality control to have access to the information required to assess the quality of the services offered by the company.

28. Where quality control can be performed by sampling, the Restricted Committee considers that the introduction of a system for systematically recording phone calls between telephone

operators and prospects, and between clairvoyants and customers, is excessive in relation to the purpose pursued.

29. The Restricted Committee points out that it has already considered, in its deliberation no. SAN-2020-003 of 28 July 2020 with regard to a company that recorded the phone calls received by the employees in its customer service department for training purposes, that "*the company does not provide any justification for the need to record all phone calls made by the customer service department, with regard to the purpose of the processing, i.e. training for employees. (...) Although the number of recordings may vary depending on each employee and the circumstances, especially the training needs for each employee,* (…) *the company does not demonstrate that it has implemented, for the past and the future, a system for recording employees' phone calls that is limited to what is necessary in relation to the intended purpose. However, a controller cannot implement a personal data processing operation without first ensuring that it is necessary for fulfilling its needs, especially where it is based on a mechanism that is particularly intrusive for its employees. In light of these elements, the Restricted Committee considers that a breach of Article 5(1)(c) of the GDPR has occurred."*

30. With regard to systematically recording phone calls in full for the purpose of proving that a contract has been formed, the Restricted Committee notes that, in this case, prospects disclose their telephone numbers to the company via one of its websites for the purpose of obtaining information about the proposed clairvoyance services. After enquiring about the services, telephone advisers call the prospects to provide such information and possibly arrange an appointment with a clairvoyant.

31. The Restricted Committee considers that a controller wishing to record phone calls for evidential purposes must demonstrate that it does not have any other less intrusive means to prove that a contract has been entered into remotely with the data subject.

32. In this case, the Restricted Committee considers that the existence of a contract entered into remotely can be proven by other less intrusive means.

33. Article L. 221-16 of the French Consumer Code states that when a professional contacts a consumer by telephone with a view to entering into a contract relating to the sale of a good or the provision of a service, the consumer is only bound after signing and accepting the contract on a durable physical medium.

34. Therefore, the Restricted Committee considers that once proof of an online contract following a marketing call can be provided by means of written confirmation of the proposal, it does not appear to be necessary to record phone calls between telephone operators and prospects for the purpose of obtaining proof that a contract has been executed.

35. In addition, the Restricted Committee notes that no contract is formed during phone calls between clairvoyants and customers, so the need to record those conversations is not justified for the purpose of obtaining proof that a contract has been executed.

36. With regard to systematically recording phone calls in full with a view to responding to potential court orders, the Restricted Committee notes that while it is necessary for controllers to comply with any court orders relating to the data that they are processing for their own purposes, they do not have to organise the collection of personal data in anticipation of responding to a potential court order.

37. Therefore, the Restricted Committee considers that the recording of phone calls between telephone operators and prospects, and between clairvoyants and customers, for the purpose of responding to a potential court order is not justified.

38. In light of these elements, the Restricted Committee considers that a breach of Article 5(1)(c) of the GDPR has occurred. The Restricted Committee duly notes that the company has stopped offering its customers clairvoyance readings over the phone, which implies that it has at least stopped recording calls between clairvoyants and customers, but this fact cannot release the company from its liability for past events.

39. **Secondly, the rapporteur** points out that customers are invited to disclose their bank account details during phone calls with telephone operators. However, the rapporteur considers that recording the part of the call relating to the collection of the customers' bank account data cannot be justified for quality control or evidential purposes.

40. **In its defence, the company** justifies that its customers' bank account data were previously collected for the purpose of booking an appointment with a clairvoyant, simplifying the payment for subsequent readings, paying for subscriptions, and combating fraud.

41. The company also indicates that implementing a mechanism to pause recordings when customers disclose their bank account data requires the development of complex systems that would entail significant financial and human resources.

42. **The Restricted Committee** notes that, on the day of the audits, the company recorded calls between telephone operators and prospects for the purpose of checking service quality, providing proof of contract formation or responding to potential court orders. During such calls, telephone operators collected the prospects' bank account data (credit card number, expiry date and security code) and informed them that collecting such data enabled them to *"participate in securing the line for only one symbolic euro*".

43. The Restricted Committee notes that the company has not implemented any specific measures to pause the recording of the phone call when collecting customers' bank account data. However, it considers that recording the part of the call relating to customers' bank account data is not useful to the company for quality control, evidential or security purposes.

44. For example, the Restricted Committee points out that it has already considered, in its deliberation no. SAN-2020-003 of 28 July 2020 with respect to a company that, when recording

phone calls for training purposes, recorded the bank account details of customers who placed orders over the phone, that *"bank account details are data which, given their nature and the associated risk of fraud, must be subject to reinforced protective measures implemented by the controllers. (...) their use by unauthorised third parties in the context of fraudulent payments is likely to cause harm to the data subjects. The Restricted Committee noted that the company recorded and retained data for which it had no use in relation to the purpose of the processing concerned, namely employee training. In light of these elements, the Restricted Committee considers that a breach of Article 5(1)(c) of the GDPR has occurred."*

45. Furthermore, the Restricted Committee considers that recording the part of the call relating to customers' bank account data is also not relevant to the purposes claimed by the company during the proceedings: booking an appointment with a clairvoyant, simplifying the payment for subsequent readings, paying for subscriptions, and combating fraud.

46. **Consequently,** and in light of these elements, the Restricted Committee considers that a breach of Article 5(1)(c) of the GDPR has occurred, since the company collects excessive data with regard to the purposes pursued.

B. Regarding the breach of the obligation to define and comply with a personal data retention period in proportion to the purpose of the processing in accordance with Article 5(1)(e) of the GDPR

47. According to the terms of 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.*"

48. **The rapporteur** notes that, after reading both the company's data storage period policy and privacy policy, the storage period for customer data, for the purpose of managing the business relationship and monitoring its customers, is set at three years from the end of the business relationship.

49. However, the rapporteur observes that, during the audit procedure, the company indicated that its active database contained the personal data of [redacted] customers who not had a reading with a clairvoyant in more than three years, including at least [redacted] customers who had not had a reading with a clairvoyant in more than five years.

50. The rapporteur accuses the company of retaining its customers' data for an excessive period of time.

51. **In its defence**, **the company** disputes the amount stated by the rapporteur. It considers that the database contains duplicate entries. For example, it indicates that a person using a free 10-minute chat-based reading, followed by a premium chat-based reading and finally a phone-based reading is counted three times in the database.

52. Furthermore, the company accuses the rapporteur of referring to the customer's last reading with a clairvoyant when assessing the data retention period, without taking account of the fact that there is no time limit for customers to use their credit.

53. In addition, the company justifies the retention period for its customers' data of three years from the end of the business relationship by the fact that a customer may get back in contact with a clairvoyant several years after the last reading and that it is necessary for the clairvoyant to recognise a customer who has not used the company's services for a long time.

54. The company states that since the report was notified, it has implemented a purge mechanism to keep its customers' data for only one year after the end of the contractual relationship.

55. **The Restricted Committee** notes that, during the document audit, the company's active database contained the personal data of [redacted] customers who had not had a reading in more than three years, including [redacted] customers who had not had a reading in more than five years.

56. The Restricted Committee notes that, although this figure includes duplicate entries according to the company, the company has failed to notify the CNIL of the number of unique customers whose data had been kept for more than three and five years since their last reading.

57. The Restricted Committee also notes that the company justifies the data storage period by the fact that there is no time limit for customers to use their credit. However, the company did not inform the CNIL during the audit that the [redacted] customers who had not had a reading in more than three years, including [redacted] customers who had not had a reading in more than five years, are actually customers who still have credit.

58. Finally, the Restricted Committee notes that the company retained, as of the date of the audits, its customers' data for three years from the end of the business relationship and, as of the date of the Restricted Committee session, for one year from the end of the business relationship. The Restricted Committee notes that the company justifies this retention period by the need to re-identify a customer who has not used its services in a long time with the aim of providing a personalised service on the day on which that customer wishes to receive a new reading.

59. The Restricted Committee notes that the company did not inform the CNIL during the audit that these data are kept in intermediate storage.

60. The Restricted Committee considers that there is no justification to retain customers' personal data in an active database after the end of the business relationship for the aforementioned purpose. However, it considers that certain types of customer data may be retained in intermediate storage for this purpose after the end of the business relationship.

61. By way of illustration, the CNIL's reference guidelines of 23 September 2021, relating to personal data processing activities that are implemented for the purposes of managing

commercial activities, state that "*the data necessary for performing contracts are retained throughout the term of the contractual relationship. **At the end of the contract, the data must be kept in intermediate storage for a reasonable period of time** if the controller needs to fulfil a legal obligation (such as to meet its accounting or tax obligations) or if the controller wishes to establish proof in the event of a dispute, and within the applicable limitation period. Therefore, the controller **must provide a dedicated archive database or logical separation in the active database after sorting the relevant data that need to be retained.** (...)"*

62. **Therefore,** the Restricted Committee considers that these facts constitute a breach of the provisions of Article 5(1)(e) of the GDPR.

C. Regarding the breach of the obligation to process data lawfully in pursuance of Article 6 of the GDPR

63. According to Article 6 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." »

64. **The rapporteur** notes that in the case of chat-based readings, the company retains its customers' bank account data longer than is strictly necessary for completing the transaction and facilitating subsequent payments, without obtaining their prior consent, such as on the data collection form.

65. **In its defence,** the company considers that the purpose for storing its customers' bank account data is to purchase credit and is based on the binding contract between the company and its customers. The company also considers that the storage of such data for anti-fraud purposes is based on its legitimate interest.

66. **The Restricted Committee** advises that the legal basis for processing bank account data may vary, especially depending on the purpose pursued.

67. **Firstly**, with regard to the purpose of combating fraud, the Restricted Committee considers that the legal basis for storing bank account data is, in accordance with the company's claims, the legitimate interest of the company, which is not disputed by the rapporteur.

68. In this respect, the Commission states, in its deliberation no. 2018-303 of 6 September 2018 adopting a recommendation on the processing of payment card data relating to the online sale of goods or the online provision of services, that *"the retention of payment card data beyond the completion of a transaction for the purpose of combating payment card fraud is not within the scope of the contract. It considers that such processing is in the legitimate interest of the controller, provided that it does not adversely affect the interests or rights and freedoms of individuals pursuant to Article 6(1)(f) of the GDPR, in particular by ensuring compliance with the principles of transparency and the effectiveness of the exercise of their rights by the data subjects."*

69. **Secondly**, with regard to the purpose of topping up credit, the Restricted Committee considers that customers' bank account data are retained to provide an additional service to customers, namely that they do not have to re-enter their card number when purchasing additional credit, which goes beyond the execution of the contract.

70. Therefore, it considers that the processing of customers' bank account data for this purpose cannot be based on the contract between the customer and the company, and requires prior consent from customers.

71. By way of illustration, the Restricted Committee points out that the Commission considers, in its aforementioned deliberation, that for single payment purposes, "*the bank card number can only be collected and processed to complete a transaction as part of the performance of a contract to which the data subject is party in accordance with Article 6(1)(b) of the GDPR (contractual performance). Therefore, in the event of a contract involving a single payment, the Commission considers that the data should therefore not be retained beyond the commercial transaction time."*

72. Still by way of illustration, the Commission indicates in the aforementioned deliberation that *"the retention of the customer's card number to facilitate any subsequent payments and potentially allow for a "one-click" purchase on the merchant's website goes beyond the performance of the contract formed. The Commission confirms that this facility constitutes an option that is independent of the initial act that led to the collection of the bank account data, and notes that such processing requires individuals to freely give their specific, informed and unambiguous consent beforehand, in pursuance of Article 6(1) of the GDPR"*.

73. The Restricted Committee also advises that the Council of State, in its decision no. 429571 of 10 December 2020, held that *"the CNIL was rightly able to consider that, in general, retaining the credit card numbers of customers using e-commerce sites to facilitate their subsequent purchases should be subject to the explicit consent of those data subjects. It follows that the*

argument based on the contested decision's breach of the Regulation of 27 April 2016 must be ruled out."

74. **Consequently,** the Restricted Committee considers that there is a breach of Article 6(1) of the GDPR where the company retains its customers' bank account data beyond the completion of the transaction to facilitate the purchase of additional credit without first obtaining their consent.

D. Regarding the breach of the obligation to obtain consent prior to collecting the special categories of personal data under Article 9 of the GDPR

75. According to Article 9 of the GDPR, the processing of personal data revealing data concerning health or a natural person's sexual orientation shall be prohibited unless one of the conditions provided for in Article 9(2)(a to j) of the GDPR applies.

76. **The rapporteur** points out that clairvoyants have the possibility of adding comments to the company's customer records after a reading. The rapporteur notes that these comments include information that customers have disclosed about their health and sexual orientation. She notes that the company does not obtain the data subject's consent to use such data when creating the user account.

77. **In its defence, the company** argues that the simple fact for a person to contact a clairvoyant and spontaneously disclose sensitive information during the call constitutes a clear affirmative act of providing certain types of data and therefore constitutes consent.

78. In addition, the company maintains that most of the clairvoyants' comments do not identify the data subject, since data are pseudonymised.

79. First of all, the **Restricted Committee** notes that customers may disclose data about their health and sexual orientation to clairvoyants during readings. At the end of the reading, clairvoyants write comments in their customers' records. These records are stored in their business software. The Restricted Committee notes that clairvoyants' comments mention details about their customers' health and sexual orientation that were collected during the reading.

80. The Restricted Committee considers that the measures taken by the company do not anonymise, but simply pseudonymise customer data, insofar as the identifier associated with the comment and the information contained can be used to re-identify the customer concerned.

81. Subsequently, the Restricted Committee considers that, in the absence of any other conditions that can be invoked under Article 9(2)(b to j) of the GDPR, such processing can only be implemented where data subjects have given explicit consent to the processing of their 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 for processing sensitive data. Where the service requested by users

necessarily involves the processing of sensitive data, it is however necessary for users to be fully aware that their sensitive data will be processed and sometimes retained by the controller, which in principle implies explicit information on this point when collecting consent.

82. The Restricted Committee advises that Article 4(11) of the GDPR states that consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

83. One the one hand, the Restricted Committee considers that the explicit nature of the consent provided for in Article 9(2)(a) of the GDPR assumes that data subjects must be able to express, by an affirmative action, their acceptance of the processing of sensitive data, demonstrating their actual consent.

84. By way of clarification, the Restricted Committee recalls that the European Data Protection Board (hereinafter the "EDPB"), in its guidelines of 10 April 2018 on consent under Regulation 2016/679, states that *"the GDPR prescribes that a "statement or clear affirmative action" is a prerequisite for "regular" consent. As the "regular" consent requirement in the GDPR is already raised to a higher standard compared to the consent requirement in Directive 95/46/EC, it needs to be clarified what extra efforts a controller should undertake in order to obtain the explicit consent of a data subject in line with the GDPR.* ***The term explicit refers to the way consent is expressed by the data subject. It means that the data subject must give an express statement of consent****. An obvious way to make sure consent is explicit would be to expressly confirm consent in a written statement. Where appropriate, the controller could make sure the written statement is signed by the data subject, in order to remove all possible doubt and potential lack of evidence in the future. However, such a signed statement is not the only way to obtain explicit consent […]*" (Guidelines on consent under Regulation 2016/679 - WP259 rev.01 of 10 April 2018, page 21).

85. The Restricted Committee points out that it has repeatedly taken corrective measures against controllers who fail to obtain explicit consent from individuals for collecting and processing their "sensitive" data, especially in its deliberation no. 2016-405 of 15 December 2016, deliberation no. 2016-406 of 15 December 2016 and deliberation no. SAN-2017-006 of 27 April 2017 in which it considered that "*the spontaneous disclosure of such data does not release the company from its obligation to obtain express consent from the individuals who must be able to give consent to the processing of sensitive data by a clear affirmative act, thereby confirming that consent has been given with full knowledge of the facts*."

86. Therefore, the Restricted Committee notes that the simple wish to receive a clairvoyance service and the spontaneous disclosure of sensitive information do not constitute explicit consent from the data subjects.

87. It considers that the company should have provided the individuals from whom it collects special categories of personal data with a means for giving their explicit consent by a clear affirmative act.

88. On the other hand, consent collected under the aforementioned Article 9(2)(a) of the GDPR must be read in light of the definition provided in Article 4(11) of the GDPR. In this case, it implies that for data subjects to give their valid consent, they must first be fully informed of the specific nature of the data that they are disclosing, particularly that such data may reveal their health and sexual orientation. They must also be informed of the way in which their data will be used.

89. The Restricted Committee notes that the company does not provide data subjects with specific information about the collection and processing of their health data and information relating to their sexual orientation.

90. It considers that the company should have provided data subjects with specific information, such as when creating their user account.

91. Therefore, the Restricted Committee considers that the company does not collect explicit consent from the data subjects, such that it cannot claim an exception to the restrictions on collecting and processing special categories of personal data, as provided for in Article 9(2)(a) of the GDPR.

92. **Consequently**, the Restricted Committee considers that there has been a breach of Article 9 of the GDPR insofar as the company does not obtain its customers' prior explicit consent to the collection of their health data and information about their sexual orientation.

E. Regarding the breach of the obligation for transparent information pursuant to Article 12 of the GDPR

93. 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.*"

94. **The rapporteur** accuses the company of not providing data subjects with the information specified in Article 13 of the GDPR in a sufficiently accessible manner when collecting personal data for the purpose of creating a user account.

95. **In its defence, the company** maintains that there is no legal provision specifying the practical arrangements that the controller should take to inform its users of the processing of their

personal data. The company also states that it is separating its privacy policy from its "standard terms and conditions of sale".

96. **The Restricted Committee** advises that information is easily accessible, within the meaning of Article 12 of the GDPR, if it is provided to users without users having to actively search for that information.

97. On the one hand, the Restricted Committee notes that the form for creating a user account does not contain information on the personal data processing operations implemented by the company or any link to such information.

98. The Restricted Committee notes that, for users to access this information, they must exit the registration process and return to the homepage, scroll down to the bottom of the page, click on the company's standard terms and conditions of sale and actively search for the information relating to personal data protection.

99. When users need to perform several actions to obtain comprehensive information about data protection, the Restricted Committee holds that the information is not easily accessible.

100. On the other hand, the Restricted Committee notes that the information is contained in a document entitled "standard terms and conditions of sale", which contains both general information about the "terms and conditions of sale", the conditions for using the website, and information about the personal data processing operations implemented by the company.

101. Since the information is contained in a document that cannot be easily identified as relating to personal data protection, the Restricted Committee considers that the information is not easily accessible.

102. By way of illustration, the Restricted Committee also recalls that the EDPB, in its guidelines of 11 April 2018 on transparency, states that "*the "easily accessible" element means that the data subject should not have to seek out the information; it should be immediately apparent to them where and how this information can be accessed, for example by providing it directly to them, by linking them to it […]*." As a best practice, the EDPB recommends that *"at the point of collection of the personal data in an online context,* ***a link to the privacy statement / notice is provided or that this information is made available on the same page on which the personal data is collected****."* The guidelines also specify that this information *"should be clearly* ***differentiated from other non-privacy related information*** *such as contractual provisions or general terms of use."* The guidelines add that *"the data subject must not* ***have to actively search for information*** *covered by [Articles 13 and 14] amongst other information, such as terms and conditions of use of a website […]*."

103. **Consequently,** the Restricted Committee considers that the way in which information on personal data protection is provided on the [redacted] website does not meet the transparency requirements of Article 12 of the GDPR.

F. Regarding the breach of the obligation to inform data subjects pursuant to Article 13 of the GDPR

104. Article 13 of the GDPR requires the data controller to provide the data subject with various information, in particular concerning its identity and contact details, the purposes of the processing operation, its legal basis, the recipients or categories of recipients of the data, and, where applicable, the fact that the data controller intends to transfer data to a third country. In addition, the Regulation requires, where necessary to ensure *"fair and transparent processing"* of personal data in this case, that individuals are informed of the period for which the personal data will be stored, the existence of various rights that individuals have, the existence of the right to withdraw consent at any time and the right to lodge a complaint with a supervisory authority.

105. **The rapporteur** observes that some information referred to in Article 13 is not provided to users on the [redacted] website, especially the data storage period, their right to data portability and their right to lodge a complaint with a supervisory authority.

106. Furthermore, the rapporteur notes that the sample of records submitted to the delegation shows that individuals are not informed that their call is being recorded, that they have the right to object or that the data collected during the call will be processed by the company.

107. **In its defence, the company** indicates that it is taking the necessary remedial action by including the missing mandatory information in its privacy policy. In terms of the lack of information during phone calls, the company indicates that it has stopped offering phone-based clairvoyance services.

108. **The Restricted Committee** notes that the company is currently taking action to comply with the requirement to inform data subjects and that it has stopped offering phone-based readings.

109. However, the Restricted Committee notes that the company does not dispute that, on the day of the audits, certain mandatory information under Article 13 of the GDPR was not provided to people using the [redacted] website and that prospects were not informed that their call was being recorded, that they had the right to object and that the data collected during the call would be processed by the company.

110. **Consequently,** the Restricted Committee considers that there has been a breach of Article 13 of the GDPR, since users will continue to be given incomplete information until such time as the company has modified the information notice on its website, and due to the lack of information provided to prospects on the day of the audits.

G. Regarding the breach of the obligation to regulate the relationship between the controller and the processor (Article 28 of the GDPR)

111. Article 28(3) of the GDPR requires that processing carried out by a processor for a controller shall be governed by a contract which sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data, the categories of data subjects and the obligations and rights of the controller. That contract shall also stipulate the conditions according to which the processor shall carry out the processing operations on behalf of the controller.

112. **The rapporteur** notes that two of the subcontracts and appendices provided by the company have not been signed by the service providers, while others do not include all the mandatory information.

113. **In its defence, the company** does not dispute that two subcontracts have not been signed by its service providers, and that certain mandatory information is missing from the subcontracts provided. However, the company asks the Restricted Committee to note that these subcontracts exist, which reflects its desire to comply with Article 28 of the GDPR.

114. First of all, the **Restricted Committee** notes that the appendix of the binding subcontract between the company and its processor, which attributes responsibility for any security incidents, does not include all the information provided for in Article 28(3) of the GDPR and has not been signed by the service provider.

115. Secondly, it notes that the contract between [redacted] and the telephone service provider does not contain a clause relating to processing by a processor, within the meaning of Article 28(3) of the GDPR.

116. Finally, it notes that the appendices to the contracts between [redacted] and the affiliated partners contain a subcontracting clause that does not comply with Article 28(3) of the GDPR, since it does not refer to all the mandatory information, including the obligation for the processor to process personal data only on documented instructions from the controller. It also notes that one of the appendices has not been signed by the affiliated partner.

117. The Restricted Committee considers that these facts show that contractual safeguards are unable to ensure effective protection of the personal data processed.

118. **Consequently,** the Restricted Committee considers that these facts constitute a breach of Article 28(3) of the GDPR, which the company does not dispute.

H. Regarding the breach of the obligation to ensure the security of data in pursuance of Article 32 of the GDPR

119. According to Article 32 of the 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;
[…]".

120. **Firstly, the rapporteur** points out that people can choose a single-character password when creating a user account on the [redacted] website. Furthermore, employees access the company's CRM system with a username and password created either by the company's CEO and the employee concerned, without any special rules concerning the complexity of the passwords or the need to automatically change the password when signing in for the first time, or by the administrator using a generator that returns a password between 9 and 12 characters, including alphanumeric and special characters.

121. **In its defence, the company** does not provide any response to the lack of rules for creating robust passwords.

122. **The Restricted Committee** recalls that, pursuant to Article 32 of the GDPR, in order to protect personal data, the controller must take "*appropriate technical and organisational measures to ensure a level of security appropriate to the risk*".

123. The Restricted Committee considers that the use of overly lenient rules governing password complexity, which would allow users to choose passwords that are insufficiently strong, can lead to attacks by unauthorised third parties, such as "brute force" or dictionary" attacks, which involve successively and systematically testing numerous passwords and which therefore compromise the associated accounts and the personal data contained in those accounts.

124. In this respect, the Restricted Committee notes that the need for a strong password is recommended by both the ANSSI (French National Agency for Information Systems Security) and the CNIL in its deliberation no. 2017-012 of 19 January 2017, where such a requirement is confirmed in its deliberation no. 2022-100 of 21 July 2022.

125. The Restricted Committee points out that it has repeatedly imposed financial penalties where a breach of Article 32 of the GDPR is caused by insufficient measures to guarantee the security of the data processed. Deliberations no. SAN-2019-006 of 13 June 2019, no. SAN-2019-007 of 18 July 2019 and no. SAN-2022-018 of 8 September 2022 specifically refer to weak passwords.

126. In this case, the Restricted Committee notes that the passwords for users of the [redacted] website may comprise a single character.

127. The Restricted Committee considers that data subjects are incurring a real risk: a third party with access to the password could access the personal data present in the data subject's account, view the credit usage history and/or change the account password without the user's knowledge.

128. Furthermore, the Restricted Committee notes the lack of strong passwords allowing company employees to access the CRM system, given that there are no complexity rules when they are created by the CEO and the employee concerned, and that there are no additional security measures when they are created by the administrator (passwords comprising 9 to 12 alphanumeric and special characters).

129. The Restricted Committee also considers that the procedure for creating passwords does not ensure data confidentiality, since when the password is created by the administrator, he/she sends it to the company's CEO, who forwards it to the relevant employee concerned, and when the password is not created by the administrator, the CEO creates it in liaison with the relevant employee.

130. These facts constitute a real risk to data subjects: an unauthorised third party with access to the password could access a large amount of personal data, including sensitive data.

131. Consequently, taking into account these risks for the protection of personal data and the privacy of individuals, the Restricted Committee considers that the measures implemented to guarantee data security in this case are insufficient.

132. As such, in light of the risks incurred by data subjects as stated above, as well as the sensitivity of certain types of data (health data, data relating to sexual orientation and bank account data), the Restricted Committee considers that the company has breached the obligations under Article 32 of the GDPR.

133. **Secondly**, the rapporteur notices that the mechanism used by the company to encrypt the bank details presents vulnerabilities (determination in advance of the vector initialisation, reuse of it and obsolescence of the library used), which does not, in view of the sensitivity of this data, ensure a level of security appropriate to the risk.

134. **In defense, the company** explains that its data processor, the company [redacted], should have advised it concerning the encryption of data.

135. **The restricted committee** mentions again that protection of bank details requires the implementation of increased security measures, such as encryption, in view of their highly personal nature.

136. In this case, the restricted committee notes that the documents in the file show that [redacted] was not in charge of encrypting the banking data of [redacted]'s customers, but rather of managing the information system and hosting the data.

137. The restricted committee also notices that the documents in the file show that [redacted] has encrypted its customers' bank details itself, and in an unsecured manner.

138. Indeed, the restricted committee observes that the MITRE (American non-profit organisation involved in particular in systems engineering and information technology) CWE (Common Weakness Enumeration) list, which lists software weaknesses, identifies generating a predictable initialisation vector with CBC mode as a vulnerability, as in this case, such as reusing an initialisation vector. The restricted committee notes that when the initialisation vector is not random but determined, the clear message is still encrypted in the same way. It is therefore possible to compare several encrypted messages and identify the clear messages to which they correspond. Moreover, by reusing the initialisation vector, this vector is common to all data encrypted with the unique key.

139. The restricted committee also notes that Mycrypt, the encryption library used by the company, was considered obsolete and removed in 2017, so that the use of this functionality is not recommended in the PHP documentation.

140. As a consequence, the restricted committee considers that the above-mentioned facts constitute an infringement of Article 32 of the GDPR, since the mechanism implemented by the company [redacted] to encrypt its customers' the bank details does not ensure a level of security appropriate to the risk.

141. **Thirdly, the rapporteur** points out that the [redacted] website was accessed at the time of the audit using the "HTTP" protocol, including the page for collecting bank account data. However, "HTTP" is not a secure protocol, meaning that the site is vulnerable to attacks and allows transmissions containing personal data (including bank account data) between the user's browser and the server hosting the website to be read in plain text format.

142. **In its defence, the company** advises that it changed its "HTTP" protocol to the TLS protocol on the [redacted] website after receiving the report.

143. **The Restricted Committee** recalls that, pursuant to Article 32 of the GDPR, the controller must take "*appropriate technical and organisational measures to ensure a level of security appropriate to the risk*".

144. The Restricted Committee notes that the "HTTP" protocol is a communication protocol that does not allow for authentication of the website or encryption of the data when sent to the servers hosting the company's website, which does not guarantee the authenticity of the website viewed or the integrity and confidentiality of the data exchanged, thereby exposing the personal data processed through these pages to the risks of eavesdropping, interception or modification without the user's knowledge, which could lead to a breach of the data subjects' privacy.

145. By way of clarification, the Restricted Committee notes that the need to ensure confidentiality over the channels used to transmit personal data has been highlighted by ANSSI since 2013, especially in its *"Recommendations for the implementation of a website: achieving proficiency in the standards of browser security"*, which specify 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."

146. The Restricted Committee also finds 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.

147. The Restricted Committee also holds that the personal data in question are highly personal, since they are bank account data. Therefore, taking into account the risks to the protection of the data subjects' personal data and privacy, the Restricted Committee considers that the measures deployed to guarantee data security in this case are inadequate, given that personal data are transmitted between the user's browser and the server hosting the website.

148. **Consequently**, the Restricted Committee considers that, with regard to the personal data that are subject to the processing (especially bank account data), the failure to implement the basic security measure, such as the use of the "HTTPS" protocol or another equivalent security measure, constitutes a breach of Article 32 of the GDPR. Nevertheless, the Restricted Committee notes that the company changed the protocol during the audit. However, the Restricted Committee reiterates that the remedial measures taken do not release the company from its liability for the breach observed.

I. Regarding the breach of the obligation to notify personal data breaches to the CNIL in pursuance of Article 33 of the GDPR

149. Article 4(12) of the GDPR defines a personal data breach as a *"breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."*

150. Article 33 of the GDPR states that *"in the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay (...) Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay." »*

151. Recital 87 of the GDPR states that *"It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject".*

152. **The rapporteur** notes that the company became aware of the personal data breach on 29 September 2020 after receiving a sample of the affected data from a journalist, or no later than 30 September 2020, following its internal investigation.

153. According to the rapporteur, the personal data breach was likely to result in a risk to data subjects' rights and freedoms, particularly in light of the duration of the breach (two months and four days) and the potential number of data subjects ([redacted] customers and prospects in the database).

154. Consequently, the rapporteur considers that the company should have notified the existence of the personal data breach to the CNIL in phases, where applicable.

155. **In its defence, the company** acknowledges that it became aware of the existence of the security incident on 29 September 2020. However, the company indicates that access to the server in question had been closed since 10 July 2020, which brought an end to the security incident.

156. It attributes liability for the security incident to its facilities management subcontractor. The company advises that after it had asked its subcontractor to provide its developer with access to its server, its subcontractor acted outside its instructions by making the server accessible to unauthorised third parties.

157. Finally, the company disputes the number of customers and prospects in its database as claimed by the rapporteur. The company considers that the database contains the email addresses of [redacted] customers and [redacted] prospects.

158. **The Restricted Committee** recalls that, in accordance with Article 33 of the GDPR, the principle in the event of a personal data breach is to notify the supervisory authority. Controllers are only exempt from this obligation where the breach is unlikely to result in a risk to the rights and freedoms of natural persons.

159. The Restricted Committee also recalls that in the event of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the controller is required to notify the breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it.

160. By way of illustration, the Restricted Committee indicates that the EDPB, in its guidelines on personal data breach notification of 6 February 2018, considers *that "**a controller should be regarded as having become aware*** [of the personal data breach] *when that controller has a **reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised**. The GDPR requires the controller to **implement all appropriate technological protection and organisational measures to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject*** (...). *The controller is therefore required to take the necessary measures to*

ensure that it becomes "aware" of any breaches in a timely manner so that it can take appropriate action."

161. By way of example, *"a third party informs a controller that they have accidentally received the personal data of one of its customers and provides evidence of the unauthorised disclosure**. As the controller has been presented with clear evidence of a confidentiality breach, then there can be no doubt that it has become "aware".**"*

162. Still by way of illustration, the EDPB states that "*after first being informed of a potential breach by an individual, a media organisation (...),* ***the controller may undertake a short period of investigation in order to establish whether or not a breach has in fact occurred****. **During this period of investigation, the controller may not be regarded as being "aware"**. However, it is expected that the initial investigation should begin as soon as possible and **establish with a reasonable degree of certainty whether a breach has taken place**; a more detailed investigation can then follow." »*

163. In this case, the Restricted Committee notes that access to the server in question was closed by the company's subcontractor as requested on 10 July 2020, because it was not suited to its needs.

164. The Restricted Committee points out that a journalist notified the company by email on 29 September 2020 of the existence of a security incident due to a port that had wrongly been opened on the server. It also notes that the journalist's email provided the company with a sample of the database that had apparently been disclosed, i.e. identification and contact data.

165. The Restricted Committee notes that the company conducted a short internal investigation on 30 September 2020, following which it concluded that the security incident could be attributed to its facilities management subcontractor, which accidentally opened a port on the server.

166. It notes that the company listed the security incident in its data breach record and identified one of the likely consequences of the breach to be the *"resale of data leading to direct marketing without the consent of the data subjects concerned by the breach*".

167. The Restricted Committee notes, however, that the company did not notify the CNIL. The company justifies this lack of notification by the fact that it would not have been able to observe the data breach, since the journalist's alert occurred after the server had been closed and that its facilities management subcontractor did not keep the connection logs for the server concerned.

168. According to the Restricted Committee, the company did not implement all the appropriate measures to immediately establish the existence of the personal data breach.

169. The Restricted Committee considers that although the company was informed of the security incident after the server had been closed, it was able to identify the existence of a data breach by comparing the sample data provided by the journalist with its own database.

170. In addition, the Restricted Committee draws attention to the delay in sending a request to the subcontractor to provide the connection logs, since that request was only made on 25 November 2020, i.e. two months after the journalist's alert.

171. In light of the foregoing, the Restricted Committee considers that, no later than 30 September 2020, which is the date of the internal investigation, the company had a reasonable degree of certainty that there was a data breach causing a risk to data subjects' rights and freedoms, especially given the duration of the breach (two months and four days) and the potential number of data subjects, i.e. [redacted] customers and prospects.

172. The Restricted Committee notes that the company, in its capacity as the controller, had an obligation to notify the data breach, even if the breach was caused by an error that could be attributed to the subcontractor.

173. Consequently, the Restricted Committee considers that the company breached its obligations by failing to notify the data breach to the CNIL.

174. In light of the foregoing, the Restricted Committee considers that a breach of Article 33 of the GDPR has been committed.

J. Regarding the breach of Article 82 of the French Data Protection Act

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

175. Article 82 of the French Data Protection Act states that *"any subscribers or users of an electronic communications service must be informed in a clear and complete manner, unless they have been previously informed by the controller or its 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 they can object to it […]."
Such access or writing may only take place on the condition that the subscribers or users have given their consent, after receiving this information, which may result from appropriate settings in their connection device or any other device under their control (...) However, these provisions do not apply if access to the information stored in the user's end device or the storage of information in the user's end device: 1° Is for the exclusive purpose of allowing or facilitating electronic communication; 2° Or is strictly necessary for the provision of an online communication service at the express request of the user".

176. These provisions incorporate Article 5(3) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (called the "ePrivacy Directive") into French law.

177. **<u>Firstly</u>, the rapporteur** notes that the delegation reported during the online audit on 15 April 2021 that there was no banner or interface to provide information to users and obtain their consent to cookies when accessing the [redacted] website, even though certain cookies were placed on users' devices.

178. The rapporteur notes that, during the on-site audit on 15 July 2021, the delegation identified a cookie banner when accessing the website.

179. However, the rapporteur considers that the information displayed is unsatisfactory and does not provide data subjects with any further details about their consent, since no information is given on how to refuse trackers, the consequences of refusing trackers and their right to withdraw consent.

180. **In its defence, the company** argues that it has produced a compliant cookie banner on its website since the report was received.

181. **The Restricted Committee** recalls that, as a result of the combined provisions of Article 82 of the French Data Protection Act and Article 4 of the GDPR, tracking cookies requiring consent may, subject to the exceptions provided for by those provisions, only be used to read and write information if users freely give their consent in a specific, unambiguous and informed manner by a clear affirmative action.

182. The Restricted Committee considers that the validity of consent is consequently associated with the quality of the information received.

183. By way of clarification, the Restricted Committee indicates that the CNIL, in its guidelines on the application of Article 82 of the French Data Protection Act relating to read and write operations on a user's device, addresses the informed nature of consent by specifying that "*as a minimum, the following information must be given to users prior to obtaining their consent in order to ensure that consent is informed:*
- *The identity of the controller(s) responsible for the read or write operations*
- *The purpose of the data read or write operations*
- *The procedure for accepting or refusing tracking cookies*
- *The consequences of refusing or accepting tracking cookies*
- *The existence of their right to withdraw consent"*

184. In its recommendation of 17 September 2020 that proposes practical methods for ensuring compliance where cookies and other trackers are used, the Commission states that *"in practice, to reconcile the requirements for clear and concise information with the need to identify all the controllers, the specific and regularly updated information about those entities (identities or link to their personal data processing policy) may, for example, be provided at a second level of information. Therefore, the information can be made available from the first level, such as via a hypertext link or a button accessible from that level."* Information relating to the identity

of the controller(s) for read and write operations may therefore be provided at a second level of information.

185. By way of illustration, the Restricted Committee also notes that the Commission, in the Questions and Answers on the CNIL's Amending Guidelines and Recommendations on *"Cookies and Other Trackers"* of 4 November 2022, states that *"for users to provide an informed indication of their consent, all the information specified in Article 2 of the guidelines on "cookies and other trackers" must be available at the time of their choice. For the* ***first level of information, the recommendation is to clearly indicate the purposes of the cookies, allow users to access the list of controllers****, such as by means of a hypertext link or a button accessible from the first level of information,* ***inform them of their right to withdraw consent at any time and, where applicable, inform them of the consequences of refusing cookies****."*

186. The Restricted Committee notes that, on the day of the online audit, the [redacted] website did not have a banner to inform users about the cookies placed on their devices when accessing the website. Therefore, users were not informed of the operations carried out or were unable to give their prior consent, such as required by Article 82 of the French Data Protection Act, as clarified by Article 4 of the GDPR.

187. The Restricted Committee notes that it was only during the on-site audit on 15 July 2021 that the delegation observed the following cookie banner when accessing this website: *"We use cookies and other tracking technologies to enhance your browsing experience on our website, show you personalized content and targeted advertising, analyse our website traffic and understand where our visitors have come from"*, including the *"I accept"* and *"Change my preferences"* buttons.

188. The Restricted Committee also notes that after clicking on the *"Change my preferences"* button, users are shown the following information: *"You can change your preferences and refuse certain types of cookies on your computer when navigating on our website. You can also delete cookies that are already stored on your computer, but remember that deleting such cookies may prevent you from using parts of our website."*

189. The Restricted Committee notes that, during the on-site audit on 15 July 2021, the first level of information provided to users did not explain the possibility and procedure for refusing cookies, as well as the consequences of refusing cookies and their right to withdraw their consent.

190. The Restricted Committee notes that, when accessing the [redacted] website as of the date of the Restricted Committee session, the cookie banner included the following notice and the *"I accept"*, *"I refuse"* and *"Change my preferences"* buttons: *"We use cookies and other tracking technologies to enhance your browsing experience on our website, show you personalized content and targeted advertising, analyse our website traffic and understand where our visitors have come from.*"

191. **Consequently,** the Restricted Committee considers that the aforementioned facts constitute a breach of Article 82 of the French Data Protection Act, since at the time of the online audit and until the cookie banner had been modified, users accessing the [redacted] website were not informed of the operations allowing access to or storage of information on their devices, in accordance with Article 82 of the French Data Protection Act and Article 4 of the GDPR, and they were therefore unable to give an informed indication of their consent.

192. **Secondly, the rapporteur** notes that during the online audit of 15 April 2021, the delegation found that three cookies requiring prior consent from users were stored on their devices as soon as they accessed the [redacted] website without their prior consent and before they could take any action.

193. **In its defence, the company** argues that no non-essential cookies have been stored on users' devices since the report was notified.

194. **The Restricted Committee** recalls that Article 82 of the French Data Protection Act requires consent for reading and writing information on a user's device, but provides for specific cases where certain trackers are exempt from consent: either when the tracker is for the exclusive purpose of allowing or facilitating communication by electronic means, or when the tracker is strictly necessary for providing an online communication service at the user's express request.

195. With respect to traffic measurement trackers that are exempt from consent and by way of illustration, the Restricted Committee notes that the Commission specifies in its guidelines of 17 September 2020 that *"in many cases, these measures are essential for the proper operation of the website or application, and therefore for the provision of the service. Consequently, the Commission considers that* ***trackers whose purpose is limited to measuring traffic on the website or application, in response to different needs*** *(performance metrics, detection of navigation issues, improvements to technical performance or usability, estimation of the required server power, analysis of the content viewed, etc.),* ***are strictly necessary for the operation and day-to-day administration of a website*** (...) *To remain within the limits of what is strictly necessary for providing the service, the Commission stresses that* ***these trackers must have a purpose that is strictly limited to measuring traffic on the website or application for the publisher's sole use****."*

196. Regarding multi-purpose trackers, the Restricted Committee notes, still by way of illustration, that the Commission specifies in its guidelines of 17 September 2020 that *"****the use of the same tracker for several purposes, some of which fall outside these exemptions, requires prior consent from the data subjects****, according to the conditions specified in these guidelines. For example, in case of a service offered over a platform that requires user authentication (login), the service publisher may use a cookie to authenticate users without requesting their consent (because this cookie is strictly necessary to provide the online communication service). However,* ***it may only use the same cookie for advertising purposes if data subjects have actually given their prior consent to this specific purpose****."*

197. To determine whether the storage of a multi-purpose cookie on the user's device requires prior consent, the Restricted Committee considers that it is necessary to determine whether at least one of the purposes requires prior consent.

198. In this case, the Restricted Committee notes that the company stored and read the following cookies on users' devices as soon as they accessed the [redacted] website without obtaining their prior consent and before they could take any action: "test_cookie", ".ga" and ".gid".

199. The Restricted Committee notes that "test_cookie" is for advertising purposes. Therefore, it does not qualify as an exception under Article 82 of the French Data Protection Act and may not be stored on the user's device without prior consent.

200. The Restricted Committee notes that the ".ga" and ".gid" cookies pursue several purposes, i.e. a purpose for monitoring and analysing the [redacted] website, and a Google-specific purpose for maintaining and protecting the Analytics service. As such, these cookies are not exclusively for the purpose of allowing or facilitating electronic communication and are not strictly necessary for providing the service. Consequently, they do not qualify as an exception under Article 82 of the French Data Protection Act and may not be stored on the user's device without prior consent.

201. Therefore, the Restricted Committee considers that storing and reading these cookies on the user's device requires prior consent from that user, according to the conditions stipulated in Article 82 of the French Data Protection Act, as clarified by Article 4(11) of the GDPR.

202. The Restricted Committee points out that it has repeatedly imposed financial penalties for breaches of Article 82 of the French Data Protection Act where cookies requiring consent have been stored on users' devices without obtaining their consent and before users could take any action (particularly deliberations SAN-2022-023 of 19 December 2022, SAN-2022-025, SAN-2022-026 and SAN-2022-027 of 29 December 2022).

203. Consequently, the Restricted Committee considers that the aforementioned facts constitute a breach of Article 82 of the French Data Protection Act for the acts that were identified on the day of the audits, since cookies that were subject to prior consent were stored on users' devices without their consent and before they could take any action.

204. The Restricted Committee notes that, during the audit, [redacted] indicated that it had taken measures to comply with the requirements of Article 82 of the French Data Protection Act, insofar as it no longer stores a cookie that is not essential for the operation of the [redacted] website.

205. **Thirdly,** the rapporteur notes that, during the on-site audit on 15 July 2021, the auditing delegation found that the cookie banner on the [redacted] website did not allow users to refuse cookies as simply as accepting them.

206. **In its defence, the company** argues that its cookie banner will soon include a *"refuse"* button.

207. **The Restricted Committee** considers that in this case, to guarantee freedom of consent, it should be just as easy to refuse cookies as to accept them.

208. By way of clarification, the Restricted Committee indicates that the Commission, in its guidelines on the application of Article 82 of the French Data Protection Act relating to read and write operations on a user's device, specifies that *"the expression of the user's refusal must therefore not require any procedure from the user or must involve an action offering the same degree of simplicity as the action provided to express the user's consent*."

209. The Restricted Committee notes that, as evidenced by the findings of the on-site audit on 15 July 2021, when users visited the [redacted] website, they could agree to the storage of cookies requiring consent with a single action by clicking on the *"I accept"* button in the cookie banner.

210. However, when it comes to refusing these cookies, the Restricted Committee notes that users had to perform no less than five actions: click on the *"Change my preferences"* button to access the cookie management interface (first click), click on the *"Functionality cookies"* tab (second click) and the *"Monitoring and performance cookies"* tab (third click), click on the *"Targeting and advertising cookies"* tab (fourth click) to decide whether to store these cookies, and click on the *"Save my preferences"* button (fifth click).

211. Therefore, the Restricted Committee considers that the process for refusing cookies failed to offer the same degree of simplicity as the process for accepting cookies, and that making the cookie refusal mechanism more complex than the acceptance mechanism is actually tantamount to discouraging users from refusing cookies and encouraging them to prefer the ease of the *"Accept all"* button. Internet users are generally prompted to visit many sites. Speed and fluidity are distinctive features of browsing on the Internet. Having to click on *"Change my preferences"* and understand how the page to refuse cookies is built is likely to discourage users, who would nevertheless like to refuse the storage of cookies. In the present case, It is not disputed that the company offered a choice between accepting and refusing cookies before adding the *"Refuse all"* button, but the methods for expressing refusal in the context of Internet browsing skews the choice in favour of consent, which affects the freedom of choice.

212. The Restricted Committee points out that it has repeatedly imposed financial penalties for breaches of Article 82 of the French Data Protection Act in cases where it was not as simple for users to refuse cookies as it was to accept them. In deliberation no. SAN-2022-023 of 19 December 2022 and deliberation no. SAN-2022-027 of 29 December 2022, the Restricted Committee considered that *"making the cookie refusal mechanism more complex than the*

acceptance mechanism is actually tantamount to discouraging users from refusing cookies and encouraging them to prefer the ease of the "Accept" button. Internet users are generally prompted to visit many sites. Speed and fluidity are distinctive features of browsing on the Internet. Having to click on "More options" and understand how the page to refuse cookies is built is likely to discourage users, who would nevertheless like to refuse the storage of cookies. In the present case, It is not disputed that the company offered a choice between accepting and refusing cookies before adding the "Refuse all" button, but the methods for expressing refusal in the context of Internet browsing skews the choice in favour of consent, which affects the freedom of choice" (also in deliberations SAN-2021-023 and SAN-2021-024 of 31 December 2021).

213. The Restricted Committee notes that, when accessing the [redacted] website as of the date of the Restricted Committee session, the cookie banner included the *"I refuse"* button.

214. **Consequently,** the Restricted Committee considers that there has been a breach of the provisions of Article 82 of the French Data Protection Act, as interpreted in light of the GDPR, since at the time of the online audit and until such time as the company had implemented the *"Refuse all"* button, users did not have the possibility of refusing read and/or write operations with the same degree of simplicity as accepting such operations.

III. <u>On the sanction and publicity</u>

215. According to Article 20(III) of the French Data Protection Act:

"*When the controller or its processor fails to comply with the obligations resulting from Regulation (EU) 2016/*679 *of 27 April 2016 or this Act, CNIL's Chair 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 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."

216. 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 a fine.

217. **Firstly,** on the principle of imposing a fine, the company insists in its defence that its subcontractor is liable for the security breaches and the origin of the security incident. The company states that any data that were potentially accessible do not concern highly personal data or sensitive data. Furthermore, it disputes the number of data subjects, but without specifying the exact number.

218. It also advises that no complaints had been received and considers that certain breaches cause little harm to data subjects, especially breaches of Articles 12 and 28 of the GDPR. It also emphasises the efforts that it has undertaken to align and comply with the corresponding requirements after receiving the report.

219. First of all, the Restricted Committee notes that, when deciding to impose an administrative fine, it must give due regard to the criteria specified in Article 83 of the GDPR, such as the nature, gravity and duration of the infringement, the action taken by the controller to mitigate the damage suffered by data subjects, the degree of cooperation with the supervisory authority, and the categories of personal data affected by the infringement.

220. Furthermore, the Restricted Committee points out the particularly high number of breaches, i.e. nine breaches under the GDPR (Articles 5(1)(c), 5(1)(e), 6, 9, 12, 13, 28, 32 and 33) and one breach under the French Data Protection Act (Article 82). Therefore, the company has demonstrated multiple failures, since the established breaches concern a large part of the personal data protection rules, including the controller's fundamental obligations (data minimisation, limitation of the data storage period, accessibility of information, and lawfulness of processing).

221. For example, systematically recording all phone calls in full between telephone operators and prospects, as well as between clairvoyants and customers, for quality control and evidential purposes is a particularly intrusive practice for data subjects.

222. Furthermore, the company failed to comply with several provisions in Article 82 of the French Data Protection Act, including a lack of information, a lack of consent for storing cookies that are not exempt from consent, and a lack of similarity between the means offered to users for accepting or refusing the option of storing cookies on their device. These facts constitute a substantial infringement of data subjects' right to privacy and the protection of their personal data.

223. By way of illustration, the Restricted Committee also points out that the company did not notify the CNIL of the data breach, even though it had all the elements to verify the existence of a breach and that it identified unauthorised direct marketing to be a probable consequence of the breach.

224. The Restricted Committee subsequently notes that some breaches concern special categories of data that are subject to strict legal regulations (health data and information about sexual orientation) and highly personal data (bank account data), for which greater care must be taken in light of the risks of fraud.

225. The Restricted Committee also advises that the company, in its capacity as the controller, is required to comply with its obligations under the GDPR. In particular, the company is required to carry out a satisfactory and regular inspection of the technical and organisational measures implemented by its processor to ensure compliance with the GDPR and particularly ensure the security of the personal data processed.

226. In this respect, the Restricted Committee notes that several basic security measures were lacking in this case, which led to a risk for data subjects. The Restricted Committee points out that the various documents governing the contractual relationship between the company and its subcontractors do not contain all the measures required by Article 28 of the GDPR, and some documents have not been signed by the service providers. These facts show that contractual safeguards are unable to ensure effective protection of the personal data processed.

227. Lastly, the Restricted Committee notes that the remedial measures implemented by the company after receiving the report, especially concerning cookies, do not release the company from its liability for the previous breaches observed.

228. Consequently, the Restricted Committee considers that there are grounds to impose an administrative fine for the breaches of Articles 5(1)(c), 5(1)(e), 6, 9, 12, 13, 28, 32 and 33 of the GDPR and Article 82 of the French Data Protection Act.

229. **Secondly,** in terms of the amount of the fine and in its defence, the company insists on the fact that it generated a net loss.

230. The Restricted Committee considers that the company's financial situation must be taken into account when determining the penalty and, in the event of an administrative fine, its amount. In this respect, it notes that [redacted]'s net revenue in 2020 amounted to [redacted], while its net loss was [redacted]. For information purposes, the company specified during the Restricted Committee session that its projected revenue from January to August 2022 is approximately [redacted].

231. Therefore, in light of the aforementioned relevant criteria of Article 83(2) of the GDPR, the Restricted Committee considers that the imposition of an administrative fine of €150,000 is justified. This fine can be broken down as follows. €120,000 for the breaches of the GDPR and €30,000 for breach of the French Data Protection Act.

232. **Thirdly,** with regard to the publication of the penalty, the company argues that such a measure would be detrimental from a business point of view.

233. The Restricted Committee considers that the publication of this decision is justified in view of the multiple breaches identified, their severity, the specific nature of the data processed and the number of data subjects.

FOR THESE REASONS

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

- **Impose an administrative fine on [redacted] in the amount of €120,000 (one hundred and twenty thousand) for the breaches of Articles 5(1)(c) and (e), 6, 9, 12, 13, 28, 32 and 33 of 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, and €30,000 (thirty thousand) for the breach of Article 82 of the French Data Protection Act.**

- **Publish its decision on the CNIL and Légifrance websites, which will no longer identify [redacted] by name at the end of a period of two years from its publication.**

The Chair

Alexandre Linden

This decision may be appealed before the State Council within two months of its notification.