Deliberation of the Restricted Committee SAN-2020-003 of 28 July 2020 relating to [redacted]

The Commission Nationale de l'Informatique et des Libertés (French Data Protection Authority), meeting under its Restricted Committee, comprised of [redacted], members;

Having regard to Convention no. 108 of the Council of Europe of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data;

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

Having regard to amended Act no. 78-17 of 6 January 1978 on information technology, data files, and civil liberties, notably Articles 20 et seq.;

Having regard to Decree no. 2019-536 of 29 May 2019, implementing Act no. 78-17 of 6 January 1978 on information technology, data files and liberties (French Data Protection Act);

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

Having regard to Decision no. 2018-076C of 30 March 2018 of the Chair of the Commission Nationale de l'Informatique et des Libertés to entrust the secretary-general with carrying out a verification mission, or having such verification mission carried out by this entity or on behalf of [redacted];

Having regard to the Decision of the Chair of the Commission Nationale de l'Informatique et des Libertés appointing a Rapporteur before the Restricted Committee, dated 29 April 2019;

Having regard to the report submitted by [redacted] Rapporteur commissioner, notified to [redacted] on 23 September 2019;

Having regard to the written submissions from [redacted] on 24 October 2019;

Having regard to the Rapporteur's response to these submissions notified on 7 November 2019 to the company's counsel;

Having regard to the new written submissions from [redacted]'s counsel received on 22 November 2019 as well as the oral observations made during the Restricted Committee session on 28 November 2019;

Having regard to the other items in the case file;

The following were present during the Restricted Committee session of 28 November 2019:

- [redacted], commissioner, his report having been read;

As representatives of [redacted]:

- [redacted];

[redacted]

The company [redacted] having addressed the Committee last;

The Restricted Committee adopted the following decision:

I. Facts and proceedings

1. The company [redacted] (hereinafter "the company") is a simplified joint-stock company [redacted].

2. In 2018, [redacted] achieved a net turnover of over EUR 108 million and a negative net income of around EUR 600,000. The same year, the [redacted] group, comprised of [redacted] SAS and its subsidiaries, achieved a net turnover of around EUR 160 million and a negative net income of around EUR 2 million. The [redacted] group employs around 1,000 people.

3. For the requirements of its business, the company operates 16 websites within 13 European Union (EU) countries: France, Spain, Germany, Italy, the Netherlands, Slovakia, Denmark, Poland, Sweden, Finland, Belgium, the Czech Republic and Hungary as well as in the United Kingdom. Two other websites ([redacted] and ([redacted] are intended for consumers from other countries, paying in euros and dollars.

4. On 31 May 2018, pursuant to the Chair's decision no. 2018-076C, a delegation of the Commission Nationale de l'Informatique et des Libertés (hereinafter "the CNIL" or "the Commission") conducted an investigation within [redacted]'s premises. The purpose of this investigation was to check the company's compliance with all of the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter "Regulation" or "GDPR") and Act no. 78-17 of 6 January 1978 amended on information technology, data files and civil liberties (hereinafter "Act of 6 January 1978 amended" or "Data Protection Act"). The investigations were especially carried out for the processing of data of prospects and clients and the recording of telephone conversations between customer advisers and customers.

5. During this investigation, the delegation was informed that the company carries out processing aimed at combating fraud and non-payment, during payments made on its websites. When the 3DSecure protocol is not validated, an email is sent to the person having placed the order for them to send proof of residence and a scan of the front of their bank card. Moreover, the company informed the delegation that no retention period had been defined where personal data

is concerned, and that it did not take steps at regular intervals to erase data concerning customers and prospects after a defined period of time

6. The delegation observed that, for the recording of telephone conversations between customer advisers and customers, data subjects calling the company could object to telephone calls being recorded by pressing a key on their telephone.

7. Finally, the delegation found that, when a user creates an account on the company's website, passwords made up of six digits, containing only one type of character, are accepted. The company also explained that account passwords are stored in a production base in hashed form using the MD5 function, with the addition of a salt directly present in the database field related to the corresponding password.

8. Furthermore, following the investigation and by email of 7 June 2018, the company provided the Commission with the additional pieces of evidence requested, particularly a breakdown from the database of the number of customers and prospects who have not signed in, since 2008, to its websites across the different countries in which it operates. The following items were provided by the company:
   - 118,768 customers, whose personal data featured in the database, had not signed in since 25 May 2008;
   - 682,164 customers had not signed in since 25 May 2010;
   - 3,620,401 customers had not signed in since 25 May 2013;
   - 5,790,121 customers had not signed in since 25 May 2015;
   - 25,911,675 prospects had been inactive since 25 May 2015.

9. This breakdown also showed that the company [redacted] had over 11 million customer accounts and over 30 million prospects.

10. In addition, by email dated 27 June 2018, the company furnished the CNIL with the new data protection policy for its various websites.

11. Pursuant to Article 56 of the GDPR, the CNIL informed, on 27 July 2018 all of the European supervisory authorities of its competence to act as the lead supervisory authority regarding the cross-border processing carried out by the company and opening the proceedings for the declaration of the authorities concerned on this case

12. In order to investigate these elements, on 18 April 2019, the Chair of the Commission appointed [redacted] in the capacity of Rapporteur on the basis of Article 47 of the Act of 6 January 1978, amended, according to its version applicable on the date of his appointment.

13. By email dated 17 May 2019, the company was summoned by the Rapporteur to a hearing pursuant to Article 74 of Decree no. 2005-1309 of 20 October 2005 amended.

14. Following his investigation, on 23 September 2019, the Rapporteur served the company [redacted] by court bailiff with a report providing details on the GDPR breaches that he considered had been committed in this case.

15. This report suggested that the Commission's Restricted Committee issue an order to bring processing into compliance with the provisions of Articles 5-1-c), 5-1 e), 13, 32 and 35-1 of the Regulation, and a penalty after a period of three months following notification of the Restricted Committee's deliberation, as well as an administrative fine. It also suggested that this decision be rendered public and that the company no longer be identifiable by name upon expiry of a period of two years from its publication.

16. A summons to the Restricted Committee session of 28 November 2019 was also appended to the report informing the company that it had a period of one month to provide its written submissions.

17. On 23 October 2019, the company produced submissions through the intermediary of its counsel. The Rapporteur responded to these submissions on the following 7 November.

18. On 22 November 2019, the company produced new submissions in response to those of the Rapporteur.

19. During the Restricted Committee session of 28 November 2019, the company and the Rapporteur presented their oral observations.

20. The draft decision adopted by the Restricted Committee was communicated to the European supervisory authorities concerned on 16 February 2020 in accordance with Article 60.4 of the GDPR. In its draft decision, the Restricted Committee ruled on the breaches proposed by the Rapporteur in its report and discussed by the parties in respect of the adversarial principle, i.e breaches of articles 5-1-c), 5-1-e), 13, 32 and 35-1 of the GDPR; no breach of Article 6 of the GDPR and of the Directive 2002/58/EC of the Parliament and of the Council, known as the "ePrivacy Directive", having been raised by the Rapporteur.

21. On following 13 and 17 March, the supervisory authorities of Italy, Portugal and Lower Saxony expressed relevant and reasoned objections on the draft decision. The Restricted Committee decided to revise its draft decision to take into account these objections. As these objections did not propose to depart from the draft decision by taking into account a new factual circumstance, to add a breach or to aggravate the nature of the corrective measure initially proposed, the Restricted Committee decided not to communicate them to the rapporteur and to [redacted].

22. The revised draft decision was submitted to the supervisory authorities concerned on 25 June 2020.

II. Reasons for the decision

A. On the breach of the principle of data minimisation (requirement to ensure that data is adequate, relevant and limited to what is necessary)

1. The recording of telephone calls

23. Article 5-1. (c) of the Regulation provides that personal data shall be *"adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')"*.

24. **Firstly**, the Rapporteur submits that the full and permanent recording of telephone calls from customer service employees appears excessive with regard to the purpose of assessment of employees by the company.

25. The company argues that telephone recordings are neither permanent nor systematic given that customers can object to the call being recorded. It also considers that full recording of telephone conversations is proportionate to the purposes of assessing and training employees pursued by the company. Lastly, it maintains that the Rapporteur is incorrect in asserting that recording telephone calls is an excessive measure as the person responsible for training usually only listens to one recording a week per employee, whereas, according to the Company, this average is likely to evolve in line with its needs. It states that the number of recordings that the trainer should be able to listen to should be higher than the number of recordings that he actually listens to.

26. First, the Restricted Committee notes that although some customers object to their telephone call being recorded, the company carries out processing to record all of its employees' telephone calls, without said employees being able to object. It further considers that the company does not justify its need to record the whole of telephone conversations with the customer service department, with regard to the processing purpose, i.e. training employees. The Restricted Committee notes that, during its hearing dated 19 June 2019, the company indicated that the person in charge of such training only usually listens to one recording per week per employee. Furthermore, while the company asserted during the session of 28 November 2019 that the rate of recording of telephone conversations had been reduced from 100% to 30%, it does not provide any proof of this.

27. Although the number of recordings can vary depending on each employee and on circumstances, particularly as regards employees' training needs, the Restricted Committee considers that the company does not prove that it has limited, both in the past and for the future, the recording of employees' telephone conversations to what is necessary in light of the purpose pursued. Yet, a data controller cannot process personal data without checking that such processing is necessary in light of its needs, *a fortiori* when it is based on a particularly intrusive measure for employees.

28. In light of this, the Restricted Committee therefore considers that a breach to Article 5-1-c) of the GDPR has been committed.

29. **Secondly**, the Rapporteur criticises the company for not having taken measures to avoid the recording of customers' bank details during telephone calls with the company. He also considers that the measure suggested by the company following the hearing, which consists of erasing calls relating to orders placed by phone with payment by bank card on a daily basis, is not satisfactory given that the processing of bank data for a whole day is not justified in light of the purpose of the processing, which is staff assessment. He reminds the company that the purpose of processing of bank details is to complete a payment and that such data should not be recorded by the company, even for only a day, once payment has been confirmed.

30. The company argues that the daily erasure of bank data recorded during telephone conversations decided following the hearing of 19 June 2019 ensures that data are stored in accordance with the principle of minimisation. It specifies that the implementation of a measure to suspend recording when a customer's bank details are provided would require developing complex technical tools and would incur significant financial and human costs.

31. The Restricted Committee notes that, at least up until 19 June 2019, the company recorded the bank details of customers placing orders by telephone when recording its employees' conversations for training purposes and stored such data in clear text in its database for fifteen days.

32. It notes that bank details are data which, due to their nature and the associated risks of fraud, must be granted greater protection by data controllers. As highlighted by the Rapporteur, use of such data by unauthorised third parties for fraudulent payments is likely to prejudice data subjects.

33. The Restricted Committee observes that the company recorded and stored data for which it had no use in light of the purpose pursued by the processing in question, i.e. the training of employees.

34. In light of this, it therefore considers that a breach to Article 5-1-c) of the GDPR has been committed.

2. Data collected to combat fraud

35. **Firstly**, the Rapporteur argues that the company disregards the principle of data minimisation by storing supporting documents provided by customers such as copies of national identity cards, for anti-fraud purposes, when they are not required.

36. The company states that storage of a document provided spontaneously by an individual is not excessive. It considers that it can store copies of national identity cards provided by individuals spontaneously given that the CNIL indicates in its practical guide on "online purchases" that a data

controller may ask for documentary proof of identity and/or address in order to make sure of the cardholder's identity.

37. The Restricted Committee notes that, during the hearing of 19 June 2019, the company informed the CNIL that it was asking customers located in France to provide a copy of proof of address and a scan of their bank card for anti-fraud purposes. However, it informed the Commission that although it does not request a copy of an identity card, some individuals provide such a document and that in this case, it stores this document for six months, the same period as for the other documentary proof provided to it.

38. The Restricted Committee notes that a copy of an identity card may constitute appropriate documentary proof for the purposes of combatting fraud. Consequently, given the purpose of the processing carried out by the company and the residual nature of the number of copies of identity cards processed by the company, it considers that, in this case, there is no reason to observe a breach.

39. **Secondly**, in his report, the Rapporteur highlighted that, for anti-fraud purposes, the company collected copies of "health cards" ("*tessera sanitaria*") and valid identity cards in Italy. He accused the company of not being able to specify during the hearing why the collection of such a document was necessary for anti-fraud purposes. The Rapporteur subsequently noted that information provided by the company by which it declared that its statements made during the hearing of 19 June 2019 were false and that it actually only asked customers to provide their identity card to the exclusion of all other documentary proof. The company also stated that following a communication error, from 27 June to 18 July 2019, the company's marketing department requested that customers provide a copy of said health card, but that this practice had been brought to an end and that the documents thus collected have been erased. The Rapporteur therefore considered that there was no longer a need to take this fact into account as regards the abovementioned breach.

40. The Restricted Committee notes that the Italian "health insurance card" contains a range of information concerning its holder, namely his or her first and last names, gender, tax code and place of birth which, for citizens born in Italy, corresponds to the municipality of birth and, for foreign nationals, to the country of birth. It can also be deduced from the card's expiry date that the holder has a permit to stay in Italy.

41. It considers that the communication of two documents allowing to prove the identity of the person in the context of combating fraud, namely the "health insurance card" and the identity document, was excessive and irrelevant under article 5-1-c) of the GDPR. Indeed, it appears that only the collection of the identity card was relevant to the purpose of the processing operation. In the present case, the collection of the "health insurance card" containing more information than the identity card, not relevant in the context of combating fraud, was excessive. In this regard, the Restricted Committee notes that the company acknowledges that such collection was not necessary, as it stopped in July 2019. The Restricted Committee considers that even if the company would have collected such a document only for a limited period of three weeks, such elements

constitute a breach of the obligation of the data controller to process only data that are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed, in accordance with the data minimisation principle.

42. The Restricted Committee considers that a breach of Article 5-1-c) of the GDPR has been committed as regards these events.

B. On the breach of the requirement of data storage limitation

43. Article 5-1-e) of the Regulation provides that personal data shall 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 the Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')".*

44. **First**, the Rapporteur observed that, during the investigation of 31 May 2018, the company informed the CNIL that no storage period had been defined for customer and prospects' data and that it did not regularly erase or archive such data after a set period. During the hearing of 19 June 2019, the company informed the Rapporteur that it had set out a five year storage period for such data in an active database as from the date on which customers and prospects were last active, which could, for example, be connection to their customer account, a click on a newsletter or the opening of a newsletter.

45. To determine the number of customers and prospects to be taken into account, those located in the United Kingdom should also be included given that this State was a member of the European Union at the time of the events in question and that the GDPR therefore applies. In addition, as part of the withdrawal agreement between the European Union and the United Kingdom, a transition period has been agreed during which European Union law will continue to apply in the United Kingdom.

46. The readings taken by the company at the investigation delegation's request, showed that the company stored the data of 118,768 customers who had not connected to their account since 25 May 2008, that of 682,164 customers who had not connected to their account since 25 May 2010 and the data of 3,620,401 customers who had not connected to their account since 25 May 2013.

47. The Restricted Committee deduced that, at least up until the database count of 7 June 2018, the company stored a significant amount of data relating to customers who had not connected to their account in over ten years.

48. Furthermore, the fact that the company alleges that only the legal director had access to customer's stored data is of no significance as the storage period has no relation to access.

49. As regards prospects, the Rapporteur considers that the company does not prove the need to apply a five-year data storage period as from the date of last contact made by the latter.

50. However, the company argues that the five-year storage period for such data is appropriate given the specificity of its general e-commerce platform. Furthermore, it is known that certain prospects connect to the website to look at what is on offer after four years of inactivity.

51. The Restricted Committee notes that, in June 2018, in the different European Union countries in which the company performed its business and in the United Kingdom, the company stored the data of over 25 million prospects having been inactive since 25 May 2015, i.e. for over three years. Furthermore, as a striking example, the data of 4,801,596 prospects in Spain having been inactive for over three years, that of 5,616,503 prospects in Italy and that of over 12 million prospects in France were stored. The Restricted Committee notes that after having informed the CNIL's departments that their data were stored without period limitation, the company indicated during the hearing that it now stored such data for five years as from the date of last contact, even though it states that it no longer contacts them after two years of inactivity. The Restricted Committee considers that the company has not demonstrated how the storage of prospects' data, as individuals having never placed an order on the company's website or as former customers whose data are used for prospection purposes after their commercial relationship has ended, is necessary after the period of two years during which it carries out its marketing campaigns. Under such conditions, the company stores prospects' data for a period exceeding that which is necessary in light of the purposes for which they are processed. Indeed, the company stated that it sends emails to carry out its commercial prospection to the prospects only during two years.

52. On this point, the Restricted Committee considers that in this case, the data retention period of two years is proportionate for the purpose for which the personal data are processed. This retention period answers to the company's aspiration to promote, as any merchant, its products to its former customers and to people who have not objected to receiving such messages. The company also specifies that people can unsubscribe, at any time, to the reception of prospecting messages. However, the retention period set up by the company for prospects data, i.e. five years, exceeds what is necessary for the purposes for which they are processed.

53. The Restricted Committee therefore considers that the company has violated the provisions of Article 5-1 e) of the GDPR.

54. **Secondly**, the Rapporteur criticises the company for setting the opening of a marketing email as a starting point for the storage period for prospects' data.

55. The Restricted Committee notes that prospects' data enables data controllers to send messages, by email for example, to individuals showing an interest in its products or services. The Commission considers in this respect that when the starting point of the data storage period is the date of last contact made by the prospect, this must be an event demonstrating the individuals' interest in the message received, such as a click on the hypertext contained in an email. However, the mere

opening of an email cannot be considered as contact made by the prospect, given that such an email may be opened involuntarily due to the way in which the email software used works or by mistake.

56. The Restricted Committee therefore considers that the company cannot consider that the mere opening of a marketing email by an individual may trigger the start of the storage period for prospects' data and therefore store such data without breaching the principle of data storage limitation when prospects have not shown interest in the company's products or services by taking clear action for several years.

57. **Thirdly**, the Rapporteur maintains that, on expiry of the storage period for customers' data, the company does not erase all data stored, but keeps customers' email address and passwords under a pseudonymised format, which does not ensure compliance with the principle of data storage limitation.

58. The Company maintains that *"anonymisation"* of former customers' email addresses is carried out via a procedure based on a SHA256 technology and that decryption of data that has been hashed thereby requires highly sophisticated technical skills. It therefore considers that inactive customers' data is *"undecryptable and therefore anonymous"*.

59. The Committee notes that after a customers' period of inactivity, the company erases certain data, i.e. the customers surname, name and date of birth, but stores other data such as his/her email address and password which are hashed by an algorithm and transferred to another table. By doing so, the company wishes to enable a customer to reconnect to his/her account using the same login and password as those used when creating the account, after the data storage period set out.

60. The Restricted Committee considers that the data belonging to its former customers, although hashed, are not anonymised but pseudonymised and individuals could therefore be identified.

61. The company submits that the email addresses and passwords of its former customers are hashed using a particularly strong SHA256 algorithm which anonymises data.

62. The Restricted Committee notes that the SHA256 algorithm is a hash function ensuring the integrity of the personal data processed by the company. Although it is, to date, a function which cannot be reversed and is therefore considered to ensure a sufficient level of data security by the National Cybersecurity Agency of France (ANSSI) and by the CNIL, it does not anonymise data and therefore justify their indefinite storage by a data controller.

63. Consequently, the Restricted Committee considers that the company stores the data in question for a period exceeding that which is necessary in light of the purposes for which they are processed. In this respect, it notes that the company itself states that the purpose of taking such a measure is to enable its customers to reconnect to their account, even though the data is meant to have been erased. Former customers' personal data must be definitely erased on expiry of the storage period

of such data in an active database or in an archive data based, once legal requirements have expired, and cannot be stored for a hypothetical future use.

64. The Restricted Committee therefore considers that the company has, once again, breached the provisions of Article 5-1 e) of the GDPR.

B. On the breach of the requirement to inform data subjects

65. Article 13 of the GDPR requires that the data controller, at the time when data are obtained, provide information relating to its identity and contact details, the contact details of the data protection officer, the purposes of the processing and its legal basis, the recipients of the personal data, where applicable the transfer of personal data, the period of storage of the personal data, the rights of data subjects and the right to lodge a complaint with a supervisory authority.

66. **As regards customers**, the Rapporteur accused the company of not informing customers, in the data privacy policy accessible on the company's website and via a link on the form to create an account, that their data are transferred to Madagascar in the context of telephone calls. He also criticised the company for only citing one legal basis in these documents for all of its processing, i.e. consent, when several processing operations were based on a different legal basis.

67. In his submissions of 7 November 2019, the Rapporteur noted that despite the company's assertions, its privacy policy had not been corrected to include the transfer of data to Madagascar.

68. As regards the legal bases of processing, the company affirmed that it based its processing on data subjects' consent, which, in its opinion, it could not be reproached for given that this legal basis provides data subjects with greater protection and that, as a result, a breach to the lack of information of data subjects could not be held against it for these events.

69. The Restricted Committee notes that it results from the company's statements on the various processing operations carried out that several of them, i.e. for example the fight against fraud or the processing carried out for purchases placed on the company's website, could not be based on data subjects' consent but rather, as indicated by the Rapporteur, on a contract or on the legitimate interests pursued by the company. Recalling that recital 41 of the GDPR requires that the legal basis of processing be *"clear and precise"*, it considers that the company cannot only refer in its data privacy policy to the legal basis of consent for all processing carried out.

70. Consequently, although the company has indeed included information on the legal basis, as required by texts, and taken the care to select the basis that provides in its view the most protection to data subjects' rights, the Restricted Committee reminds it that Article 13 of the GDPR requires granular information relating to the legal basis of each processing operation. It can therefore only note that the company has not fully complied with the provisions of this article by abstaining to provide, for each processing operation carried out, the corresponding legal basis in its privacy policy.

71. Furthermore, the Restricted Committee notes the changes made on its website as regards the transfer of data to Madagascar. However, it considers that a breach to Article 13 of the GDPR was committed up until 18 November 2019, the date on which the company stated that it had made changes to its website.

72. **As regards employees**, the Rapporteur criticises the company for not having informed them individually of the recording of their telephone calls.

73. The company submits that employees are informed of the recording of telephone calls with customers, via several documents, such as a certificate of presence "information project telephone recording" dated 14 January 2016, a document dated May 2014 and performance assessment forms dated 2017. The company also provided statements from three customer advisors confirming that they had read the document dated 14 January 2016, that they have understood the purpose of such recording and that they may contact the legal department for further information.

74. The Restricted Committee recalls that informing employees of the use of measures to listen to and record telephone conversations in the work place is vital and is related to the fair and transparent nature of any processing implemented by a data controller. As indicated in recital 39 of the GDPR, *"The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used"*.

75. The obligation of transparency requires the company to provide information on such a measure to each employee, with the former unable to only provide information once, as in this case in 2016, which is not provided to new employees hired subsequently.

76. Moreover, the Restricted Committee also noted that Article L. 1222-4 of the French Labour Code provides that *"no information personally concerning an employee may be collected by a measure which has not previously been brought to his or her attention"*. Furthermore, the Commission has repeated on several occasions, including in a guide for employers and employees available on its website and in recommendation no. 2014-474 of 27 November 2014 relating to the recording of phone calls at the work place, that employees must be provided a certain amount of information relating to the processing carried out by employers.

77. Lastly, the Restricted Committee notes that the documents produced by the company do not allow it to provide employees with information on the purposes pursued by the processing, on the legal basis of the measure, on the recipients of the data produced by the measure, on the data storage period, on their rights, particularly to access the data concerning them and on the possibility of lodging a claim with the CNIL, ensuring the full information of employees pursuant to Article 13 of the GDPR.

78. In light of the above, the Restricted Committee therefore considers that a breach to Article 13 of the GDPR has been committed.

C. A breach of the requirement to ensure data security

1. The absence of security regarding passwords providing access to customer accounts

79. Article 32-1 of the Regulation provides that: *"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 *"the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services"*.

80. Thus, pursuant to Article 32-2 of the GDPR, the data controller must take account of the risks that are presented by processing, in particular from destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed, whether accidentally or unlawfully.

81. During the investigation of 31 May 2018, the CNIL delegation observed that the individuals wishing to create a user account on the company's website could create a password comprised of six characters containing only one character category. During the hearing of 19 June 2019, the company specified that since the CNIL investigation, a measure to block the account for one minute had been put in place, after 19 unsuccessful attempts to access an account from a single IP address in less than one minute.

82. In its defence, the company submits that it has changed the rules for the creation of passwords for accounts and now requires that its customers create passwords comprised of at least eight characters. It also questions the CNIL's recommendations on the topic and maintains that the technical recommendations in terms of password security in deliberation no. 2017-190 of 22 June 2017 of the Commission have been disputed by cybersecurity experts. Claiming that overly complex rules have resulted in the standardisation of passwords, it preferred to opt for requiring shorter and simpler passwords, with these being less predictable for potential attackers, with the risk being based on human logic.

83. The Rapporteur maintains that passwords comprised of six or eight characters, without any complexity criteria, are not strong enough and do not ensure the security of the data processed by the company. He considers that such passwords to not prevent attacks "by brute force" which consist of successively and systematically testing many passwords and can therefore compromise associated accounts and the personal data they contain.

84. The Restricted Committee considers that, contrary to what the company states, the length and complexity of a password are elementary criteria to assess the strength of the latter. It reminds the company that in order to ensure a sufficient level of security and meet password strength requirements, when authentication is based only on an identifier and a password, the password must contain at least twelve characters – containing at least one uppercase letter, one lowercase

letter, one number and one special character – or the password must contain at least eight characters – containing three of these four character categories – and be completed by an additional measure such as the timing out of access to an account after several failed attempts (temporary suspension of access for an increasing period of time for each attempt), the implementation of a mechanism to prevent automated and intensive attempts (e.g.: "captcha") and/or the blocking of the account after several unsuccessful authentication attempts.

85. The Restricted Committee notes that the need for a strong password is also underlined by ANSSI, which states that *"a good password is above all a strong password, i.e. difficult to find even using automated tools. A password's strength depends on its length and the number of possibilities that exist for each character comprising it. A password comprised of lowercase letters, uppercase letters, special characters and numbers is technically more difficult to find than a password comprised of only lowercase letters".*

86. In this case, it considers that the strength of a password comprised of eight characters and only one category of characters is very weak and that the company does not, at any time, demonstrate how a short and simple password would be likely to better resist an attack by brute force than a password comprised of more characters and several categories of characters.

87. As a consequence, the Restricted Committee considers that the passwords put in place by the company to access customer accounts created on its website do not meet requirements in terms of strength.

2. Request to provide a copy of the payment card

88. During the investigation of 31 May 2018, the delegation observed that the company requested that its customers provide it with a scan of the bank card used on ordering, for anti-fraud purposes. For its customers in France, an email specifying *"out of the 16 numbers on the front, please make sure that at least the first 4 and last 4 are clearly visible, and that the expiry date and cardholder's name are also legible*" was therefore sent to data subjects. Emails making this request were also sent to individuals placing orders on the Italian, Spanish, Hungarian, Slovakian, Danish and Greek websites. It was noted that the company stored the scans of un-blanked bank cards.

89. In this regard, the Rapporteur therefore considers that the company's email sent to individuals, particularly to French citizens, prompts customers to submit a full copy of the payment card instead of encouraging them to hide a minimum of numbers on it.

90. It was also observed that payment card scans are stored by the company in clear-text for six months from recording of the documents, in case of dispute.

91. By letter of 28 June 2019, the company stated that an online platform dedicated to sending supporting documents would be set up at the end of August 2019. Furthermore, the company maintains that it was authorised by the CNIL to carry out processing the purpose of which is to combat fraud and that it may validly collect bank card expiry dates and truncated numbers.

92. **First**, the Restricted Committee notes that the company was indeed authorised by a CNIL deliberation of 2 July 2009 to process truncated bank card numbers as well as the expiry date, for processing the purpose of which is to combat fraud. However, it has been demonstrated that the company processed the copies of customers' bank cards containing all numbers, when it was only authorised to process a truncated part of these. The Restricted Committee therefore considers that the authorisation issued by the CNIL cannot justify the processing of all of customers' bank card numbers.

93. **Secondly**, the Restricted Committee notes that the CNIL delegation observed that the measures put in place by the company enabled customers to send photographs or scans of their bank cards containing all bank card numbers in clear text by unencrypted email from their mailbox, or that such data were stored, as was the documentary proof requested for the purposes of combatting fraud, for six months in clear text in the database.

94. Under such conditions, the Restricted Committee considers that, at least up until August 2019, the company did not take security measures to ensure the security of its customers' bank data.

95. Based on these elements, the Restricted Committee considers that Article 32 of the Regulation has been breached.

D. <u>On corrective measures and their publicity</u>

96. Pursuant to paragraph III of Article 20 of the Act of 6 January 1978 amended:

> "*Where the data controller or their data processor does not comply with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or from this Act, the Chair of the Commission Nationale de l'Informatique et des Libertés may also, where necessary and after having sent the warning provided for in Paragraph I of this Article or, where necessary in addition to the notice provided for in Paragraph II, refer to the Commission's Restricted Committee to pronounce, following an adversarial procedure, one or several of the following measures: […]*
> *2) An order to bring processing into compliance with the obligations arising from this Act or from the aforementioned Regulation (EU) 2016/679 of 27 April 2016 or to respond to the requests presented by the data subject with a view to exercising his or her rights, which may be completed by a periodic penalty payment not exceeding €100,000 per day overdue as from the date set by the Restricted Committee, save for cases in which the processing is carried out by the State; […]*
> *7) Save for cases in which the processing is carried out by the State, an administrative fine that cannot exceed EUR 10 million or, where it is carried out by a company, 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher. In the cases mentioned in paragraphs 5 and 6 of Article 83 of aforementioned Regulation (EU) 2016/679 of 27 April 2016, these ceilings shall be increased respectively to EUR 20 million and 4% of said*

turnover. The Restricted Committee shall take into account, when determining the amount of the fine, the criteria specified in said Article 83."

97. Article 83 of the GDPR provides that:

"1. 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.
2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58 (2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:
(a) the type, seriousness and duration of the breach in light of the type, scope or purpose of the processing in question, as well as the number of data subjects affected or the level of damage they have suffered;
(b) the intentional or negligent character of the infringement;
(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
(e) any relevant previous infringements by the controller or processor;
(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
(g) the categories of personal data affected by the infringement;
(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
(i) where measures referred to in Article 58 (2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement."

98. **Firstly**, as regards the fine proposed by the Rapporteur, the company submits that it has never been sentenced by the CNIL, that it had few frameworks prior to entry into force of the GDPR and that the Commission had announced a tolerance period as concerns new breaches to the GDPR, such as data minimisation or pseudonymisation.

99. The Restricted Committee considers that in the present case, the abovementioned infringements warrant that an administrative fine be issued against the company for the following reasons.

100. First, it notes that, contrary to the company's assertions, the breaches in question mostly concern requirements that Act no. 78-17 of 6 January 1978 amended already imposed on data controllers and which do not arise from the GDPR, including as regards the principle of data minimisation and storage limitation. Furthermore, it reminds the company that the questions relating to data pseudonymisation had already been asked well before entry into force of the GDPR.

101. It further notes that several of these breaches concern employees and their right to receive information on the processing of their personal data. Here again, the Restricted Committee reminds the company that this is not a new requirement introduced following entry into force of the GDPR.

102. Lastly, it underlines that bank data are data which must be the subject of particular care from data controllers and that the Commission has continued to assist them on this topic for many years.

103. **Secondly**, the company highlights its cooperation with the Rapporteur and the measures put in place, as well as some sanctions previously issued by the Restricted Committee. It also considers that it cannot be reproached a lack of speed when the hearing took place one year after the investigation carried out within its premises and when no formal notice was issued to it within this period.

104. The Restricted Committee notes that although several measures were put in place by the company in order to correct certain breaches in whole or in part, these were only adopted following the CNIL's investigation of 31 May 2018 as regards the implementation of storage periods for customers' and prospects' data, and only following the hearing of 19 June 2019 and the report for the erasure of recording containing customers' bank details and the information of data subjects on the website as regards the transfer of their data outside of the European Union.

105. The Restricted Committee further considers that the seriousness of some breaches is characterised. More specifically as regards the breach relating to the recording of telephone conversations, the Restricted Committee notes that the company recorded full telephone conversations had by its employees for several years, when it had no reason to do so and that such processing can be likened to constant surveillance. It also notes that the information provided to employees on the implementation of measures to record phone calls was particularly lacking, being either incomplete prior to 2016, or non-existent for employees hired by the company after this date.

106. Furthermore, the seriousness of the breaches is characterised given the specific category of personal data processed by the company, i.e. bank data which are considered as data exposing data subjects to a risk of fraud, and thereby of prejudice, and must as such be the subject of particular vigilance. Lastly, the Restricted Committee also considers that the seriousness of the

breaches is characterised due to the number of data subjects concerned by the breaches, particularly as regards data storage periods which affected several thousands of data subjects.

107. The company goes on to argue that it is a medium-sized company and that it operates in a particularly competitive sector. It considers that a high administrative fine would affect its financial health and its market position.

108. In this respect, the Restricted Committee considers that the company is an established e-commerce player and that, being founded well before the entry into force of the GDPR, it could not ignore the basic rules of data protection.

109. In addition, the Restricted Committee recalls that Article 83, paragraph 3 of the Regulation provides that in the case of several infringements, as is the case here as four breaches have been established, the total amount of the fine cannot exceed the amount specified for the gravest infringement. Given that the company is accused of infringing Articles 5 and 12 of the Regulation, the maximum amount of the fine that could be imposed is 20 million euros or 4% of the annual worldwide turnover, whichever is higher.

110. However, when determining the amount of the fine issued, the Restricted Committee also takes into account the measures that the company has taken during the sanction proceedings to ensure partial compliance and its cooperation with the Commission's departments.

111. **Thirdly**, as regards the need to issue an injunction, the company considers that formal notice without periodic penalty payments would be more suited given the speed already observed in ensuring compliance for several breaches.

112. While it does not ignore the steps taken by the company to ensure compliance with the GDPR, the Restricted Committee considers that the company did not prove, on the day on which the investigation was closed, the full compliance of the processing carried out under Articles 5-1-c), 5-1 e) 13 and 32 of the Regulation.

113. The company having failed to ensure compliance as regards these breaches, there is reason to issue an injunction.

114. **Fourthly**, the Restricted Committee considers that the publicity of the sanction is justified in light of the importance of the issues raised as regards employees, as well as the nature of the data in question, when the company is an important player in the sector in which it operates.

115. As a result of the above and the consideration of the criteria set out in Article 83 of the GDPR, an administrative fine of 250,000 euros, an injunction with periodic penalty payments and an additional sanction of publication for a period of two years are justified and proportionate.

FOR THESE REASONS

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

- to impose on [redacted] an injunction to bring processing in compliance with the requirements arising from Articles 5-1 c), Article 5-1 e), 13 and 32 of Regulation no. 2016/679 of 27 April 2016 on data protection, and in particular:

- with respect to the breach of the principle of personal data minimisation:
    - prove the end of the non-punctual and non-random recording of advisors' telephone conversations when the purpose pursued is their training or assessment;

- with respect to the breach of the principle of data storage limitation, define and implement a policy concerning the period for which the data concerning customers and prospects will be stored, which shall not exceed what is necessary for the purposes for which they are collected and processed, and particularly:
    - justify the procedure set up for the intermediate archiving of customers' personal data, after sorting the relevant data to be archived and deleting irrelevant data, as well as the starting point for such archiving;
    - justify the restriction of employees' access to personal data contained in the active database to only persons needing to have such data;
    - no longer process prospect data beyond the period of time at the end of which the company stops contacting them (two years in the present case) and no longer take the simple opening of an email as the last point of contact made by prospects;
    - no longer retain the email addresses and hashed passwords of former customers at the end of a set period of inactivity and carry out a purge of such data retained by the company up to the date of the Restricted Committee's deliberation;
    - justify that data concerning customers is deleted after the set period of inactivity, which the company shall have to justify, and that data concerning prospects is deleted after two years of inactivity;

- with respect to the breach of the requirement to inform data subjects:
    - inform employees about the setup of a system for recording telephone conversations, particularly bearing on the intended purposes, the legal basis of the system, the recipients of the data from the system, the data retention period, the rights of employees, particularly to access personal data, and the possibility of lodging a complaint with the CNIL;
    - provide customers with full information, by providing information on the different legal bases of the processing implemented by the company;

- with regard to the breach to the obligation to ensure personal data security, take any measure, for all personal data processing carried out, to ensure the security of such data and to prevent unauthorised third parties from accessing it pursuant to Article 32 of the GDPR, in particular:
    - implement a restrictive password management policy, as regards customer accounts, according to one of the following arrangements:

- passwords shall be composed of at least twelve characters, containing at least one uppercase letter, one lowercase letter, one number and one special character;
- passwords shall be composed of at least eight characters, containing at least three of the four character categories (uppercase letters, lowercase letters, numbers and special characters) and shall be completed by a complementary measure such as the timing out of access to an account after several failed attempts (temporary suspension of access for an increasing period of time for each attempt), the implementation of a mechanism to prevent automated and intensive attempts (e.g.: "captcha") and/or the blocking of the account after several unsuccessful authentication attempts (maximum of ten);

- associate the injunction with a periodic penalty payment of 250 (two hundred and fifty) euros per day of delay on expiry of a period of 3 (three) months following notification of this deliberation, with the documentary proof of compliance being sent to the Restricted Committee within this period;

- for the breaches to Articles 5-1 c), 5-1 e), 13 and 32 of the GDPR, impose on [redacted] an administrative fine of 250,000 (two hundred and fifty thousand) euros;

- to make its decision public on the CNIL website and on the Légifrance website, which will no longer identify the company by name upon expiry of a period of two years from its publication.

The Chair

[redacted]

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