Decision of the Restricted Committee No. SAN-2021-022 of 30 December 2021 concerning [redacted]

The *Commission Nationale de l'Informatique et des Libertés* (CNIL - the French Data Protection Authority), met in its Restricted Committee consisting of [redacted],

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

Having regard to the 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 Act No. 78-17 of 6 January 1978 on data protection;

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

Having regard to Decision No. 2019-084C of 24 April 2019 of the CNIL Chairman to instruct the secretary general to carry out or have a third party carry out a task to verify the processing implemented by that organisation or on behalf of [redacted];

Having regard to the decision of CNIL's Chairman appointing a rapporteur before the Restricted Committee of 12 April 2021;

Having regard to the report of [redacted], commissioner and rapporteur, notified to [redacted] on 9 July 2021;

Having regard to the written observations made by [redacted] on 3 September 2021;

Having regard to the other documents in the file;

The following were present at the Restricted Committee session on 16 September 2021:

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

As representatives of [redacted]:

- [redacted]

with [redacted] addressing the session last.

The Restricted Committee adopted the following decision:

I. Facts and proceedings

1. [redacted] (hereinafter "the company") is a public limited company with a Board of Directors and with share capital of [redacted] located at [redacted] Its main activity is the sale of furniture on the Internet and in store.

2. [redacted] started its business in 2007 and has approximately [redacted] employees. In 2020, it generated turnover of [redacted] with a net loss of [redacted].

3. [redacted] markets its products in France and several European Union countries from the website "[redacted]" (hereinafter "the website"). It also has two stores in France owned by its subsidiary, [redacted]

4. Pursuant to Decision No. 2019-084C dated 24 April 2019 of the Chairman of the *Commission nationale de l'informatique et des libertés* (hereinafter "CNIL" or "the Authority"), a CNIL team carried out an online investigation into the processing accessible from the domain [redacted] on 9 May 2019, and an on-site investigation at [redacted] on 5 June 2019. The purpose of these investigations was to verify the company's compliance with all the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter "the Regulation" or "GDPR") and with amended Act No. 78-17 of 6 January 1978 on data protection (hereinafter "the amended Act of 6 January 1978" or "the French Data Protection Act").

5. In particular, the investigations focused on the processing of personal data of the company's customers and prospective customers. The checks performed concerned the retention periods of the personal data, the information brought to the attention of the data subjects concerning the processing carried out by the company, compliance with data subjects' requests for erasure of their data, the obligation to provide a legal act for the processing operations carried out on behalf of the data controller as well as the obligation to ensure data security.

6. At the end of the checks, report no. 2019-084/1 and no. 2019-084/2 were notified to [redacted] in two letters dated 15 May and 11 June 2019. The company sent the Authority the additional documents requested at the end of the investigation by email on 12 June 2019.

7. By email of 22 August 2019, the company sent the investigation team several additional documents, relating in particular to the change in the company's name, the privacy policy displayed in store or in emails sent at the time of the creation of a user account.

8. As the investigations established the cross-border nature of the processing concerned, the CNIL informed all European supervisory authorities on 1 July 2020, in accordance with Article 56 of the GDPR, of its competence to act as lead supervisory authority. Seven authorities declared themselves involved in this procedure, within the meaning of Article 4 (22) of the GDPR.

9. On 5 October 2020, the CNIL Chairman submitted a draft order to the seven authorities concerned. Following this communication, the Berlin authority raised a relevant and reasoned

objection within the meaning of Article 60 of the GDPR, requesting that the draft order be transformed into a draft penalty, and more specifically an administrative fine. In support of this request, the authority concerned pointed out, in particular, the number of data subjects and the duration of the violations.

10. In order to examine these elements, the Authority's Chairman appointed [redacted] as rapporteur on 12 April 2021, pursuant to Article 39 of Decree No. 2019-536 of 29 May 2019 implementing the amended Act of 6 January 1978 (hereinafter the "Decree of 29 May 2019").

11. At the end of his investigation, on 7 July 2021, the rapporteur sent [redacted] a report detailing the breaches of the GDPR that he considered to have occurred in this case and indicating to the company that, in view of the summer break, it had an additional period to the one month initially provided for in which to submit its written observations pursuant to the provisions of Article 40 of the Decree of 29 May 2019. It was also given a letter informing it that the case file was on the agenda of the Restricted Committee of 16 September 2021.

12. This report proposed to the Authority's Restricted Committee to impose an injunction to make the processing compliant with the provisions of Articles 5(1)(e), 13, 17, 28 and 32 of the GDPR, accompanied by a penalty per day of delay at the end of a three-month period following notification of the Restricted Committee's decision, as well as an administrative fine. 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.

13. On 3 September 2021, the company submitted observations through its counsel.

14. The company and the rapporteur presented oral observations at the Restricted Committee's session.

II. Reasons for the decision

15. According to Article 56(1) of the Regulation "*the supervisory authority of the main establishment or sole establishment of the controller or processor shall be competent to act as lead supervisory authority regarding the cross-border processing carried out by that controller or processor, in accordance with the procedure laid down in Article 60*".

16. In this case, the Restricted Committee found, firstly, that the company's registered office has been in France since the creation of the company in 2007, that the company has been entered in the Trade and Companies Register in France since its inception and that it does not have any other establishment in the EU.

17. It follows from the above that the CNIL is competent to act as the lead supervisory authority for the cross-border processing implemented by this company, in accordance with Article 56(1) of the Regulation.

18. In accordance with the cooperation and consistency mechanism provided for in Chapter VII of the GDPR, on 1 July 2020, CNIL informed all European supervisory authorities of its competence to act as the lead supervisory authority concerning the cross-border processing carried out by the company, thus opening the notification procedure for the relevant authorities in this case.

19. The supervisory authorities of the following countries were affected by this procedure: Germany, Belgium, Spain, Italy, Luxembourg and the Netherlands.

20. Pursuant to Article 60(5) of the GDPR, the revised draft decision adopted by the restricted formation was transmitted to these supervisory authorities on 15 December 2021.

21. On 29 December 2021, none of the supervisory authorities concerned had raised any relevant and reasoned objections to the draft decision, so that, pursuant to Article 60(6) of the GDPR, they are deemed to have approved it.

A. Regarding the proceedings

22. In defence, the company contests the objection made by the Berlin supervisory authority to the CNIL's draft order, by which the authority requested the company be given an administrative fine. The company considers that it should have been the subject of an order, as initially proposed by the CNIL, and not penalty proceedings before the Restricted Committee.

23. In particular, the company expresses its surprise at the importance given to Berlin's objection, while the sales made by the company in Germany only represented 3.7% of its turnover in 2020 with a German customer base of 11,168 customers.

24. The Restricted Committee notes first of all that, as part of the cooperation process set up by the GDPR, all supervisory authorities concerned within the meaning of Article 4(22) of the GDPR may issue relevant and reasoned objections to the draft decision submitted to them by the lead supervisory authority. It is then the responsibility of the lead supervisory authority to decide whether to uphold or reject the objections made, which was done in this case by the CNIL's Chairman, in accordance with the provisions of Article 52 of Decree No. 2019-536 of 29 May 2019.

25. The Restricted Committee then notes that the criteria for determining whether a supervisory authority is concerned are set out in Article 4(22) of the GDPR and that, therefore, the turnover of a company in a Member State of the European Union or the number of customers concerned are irrelevant, provided that these criteria are met, which is the case here.

26. In addition, while indicating that the assessment of the follow-up given to the objection made by Berlin's supervisory authority was the responsibility of the CNIL's Chairman, the Restricted Committee emphasises that this objection was part of the cooperation and consistency mechanism provided for in Chapter VII of the GDPR intended to ensure harmonisation of the implementation of this regulation, in particular regarding the application of supervisory authorities' enforcement policy.

27. Finally, the Restricted Committee notes that, with regard to the objection relating to the absence of a prior order, the Conseil d'Etat ruled (EC, 9 October 2020, SERGIC, no. 433311) that it "*clearly emerges [from the provisions of Article 20 of the amended Act of 6 January 1978], that the imposition of a penalty by the CNIL's Restricted Committee is not subject to CNIL's Chairman giving the data controller or its data processor a prior order. […]*".

28. In light of these elements, the Restricted Committee considers that the CNIL has complied with the procedure applicable under the national provisions and the GDPR.

B. Regarding the breach of the obligation to specify 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

29. According to Article 5(1)(e) of the Regulation, personal data must be "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ("storage limitation")".*

30. The rapporteur noted that during the on-site investigation of 5 June 2019, the company had indicated to the investigation team that no retention period for personal data of customers (who are according to the company the persons who have created an account and placed an order) or prospective customers (who are according to the company the persons who contact [redacted] in order to obtain information on the products and services offered and who subscribe to the newsletter) had been determined or implemented by the company. The company also informed the investigation team that it did not carry out any regular deletion or archiving of such data at the end of a defined period, thereby retaining it in an active database, while its processing was no longer necessary in view of the purpose for which it was initially collected.

31. In defence, in its observations of 3 September 2021, the company firstly argued that a data retention period policy applicable to customers and prospective customers was defined from the on-site investigation on 5 June 2019, so that it could not be accused of any breach under the definition of retention periods. However, it admits that at the time of the investigation there was no functionality to determine the date of a user's or prospective user's last activity on their account and that this element was therefore not taken into account.

32. The company also indicated that the data of customers and prospective customers used for the purposes of marketing or managing their account was now stored in the active database until their account is deleted or, in the event of inactivity, for three years from the last time they signed into their account, their last contact with the company or their last order online or in store. At the end of those periods, the company specified that only the data necessary for pre-litigation or litigation purposes is retained and archived until the date corresponding to the statutory time limit justifying their retention, after which they would be deleted.

33. According to the Restricted Committee, with regard to the definition of retention periods applicable to the data of [redacted]s customers and prospective customers, it should first be noted that on the date of the investigation of 5 June 2019, the company indicated to the investigation team that it had not determined and implemented any retention period for the personal data of customers and prospective customers.

34. The Restricted Committee then notes that the investigation team observed the presence, in an active database, of personal data of 550,645 customer accounts created since the start of the business in 2007. The company informed the investigation team that it kept in a database the personal data for 310,198 user accounts created without any order having been placed for more than three years or relating to 128,712 user accounts created but not having placed an order since 2007.

35. Therefore, whereas the Restricted Committee notes that [redacted] now implements retention periods, compliance with which makes it possible to comply with the provisions of Article 5(1)(e) of the GDPR – by ensuring that the data is not stored for longer than necessary in view of the purposes for which it is processed – it considers, in any event, that on the day of the investigation, the company had not defined and implemented any satisfactory retention period policy, or data deletion procedure at the end of the period for which the processing of the data was necessary and justified, or even an archiving procedure, and that it therefore kept personal data for excessive periods.

36. With regard to all of these elements, the Restricted Committee considers that the breach of Article 5(1)(e) of the GDPR is established.

37. It points out, however, that the changes made by the company during the penalty proceedings enabled its compliance with the Regulations.

C. Regarding the breach of the obligation to inform individuals pursuant to Article 13 of the GDPR

38. Article 13 of the GDPR requires the data controller to provide, at the time the data is collected, information on its identity and contact details and that of its data protection officer, the purposes and legal basis of the processing, the recipients or categories of recipients of the personal data, information on transfers of personal data where applicable, the retention period of the personal data, the rights of individuals and the right to lodge a complaint with a supervisory authority.

39. The rapporteur notes that, during the checks carried out online on 9 May 2019 and then on site on 5 June 2019, the investigation team found that the information made available to users of the website and customers, during their visit to the store, was not complete within the meaning of Article 13 of the Regulation. Certain mandatory information provided for by this Article – namely the legal bases for processing and the data retention periods – was not brought to the attention of the data subjects on the [redacted] website or in store, either through the "Privacy Policy" on the website or the document entitled "Privacy and protection of personal data collected in store" placed on the store's sales counter.

40. In its observations in defence, the company did not dispute that no information on the legal bases was made available to the data subjects in its privacy policy. However, it argued that the document entitled "Privacy and protection of personal data collected in store" placed on the store's sales counter did not contain information on the legal bases of processing because its "*purpose was to give the main information*" while referring to the amended privacy policy made available on the [redacted] website, which constitutes additional information and is more complete. The company also argued that the lack of information related to data retention periods was only a repeat of the breach of the principle of limiting retention periods.

41. The company added that it had drafted, as part of the proceedings, a new privacy policy which now includes all the missing information, and which has been made available on the [redacted] website in order to provide information that complies with the requirements of the GDPR.

42. The Restricted Committee first of all notes that, with regard to information relating to the legal bases, the company acknowledged that such information was not present in the privacy policy accessible from the [redacted]website and to which the information document on data protection, located in the store, refers as stated by the investigation team.

43. The Restricted Committee also notes that, until the penalty proceedings, the data subjects were not informed of all the legal bases of the processing carried out, in breach of the provisions of Article 13 of the GDPR.

44. The Restricted Committee then notes that the investigation team found, during the investigation of 5 June 2019, that the information on retention periods was not included in the privacy policy. The company also acknowledged this specifying that the information was incomplete due to no definition and implementation of a personal data retention period policy.

45. Under such circumstances, the Restricted Committee considers that the breach of Article 13 of the GDPR is established on this point, since the information on the retention periods is among the information that must be communicated, in that it makes it possible to guarantee fair and transparent processing of the personal data concerned. Thus, for example, information on retention periods allows data subjects to know how long the data is kept by the controller and, consequently, for how long they can exercise their right of access.

46. The Restricted Committee also considers that the link between the company's failure to implement data retention periods and the lack of information for individuals does not prevent these two breaches existing as such.

47. In light of the above, the Restricted Committee considers that the company did not comply with the provisions of Article 13 of the GDPR.

48. The Restricted Committee nevertheless notes that, as part of the penalty proceedings, the company demonstrated having made its privacy policy compliant, which now contains the

notices concerning retention periods for the data processed and complete information on the legal bases of the processing, to which the information document displayed in store refers.

D. Regarding the breach of the obligation to comply with requests to delete personal data pursuant to Article 17 of the GDPR

49. Under Article 17 of the GDPR, the data subject has the right to *"obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall be obliged to erase personal data without undue delay where one of the following grounds applies:*
a) the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;

b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1) (...) and where there is no other legal ground for the processing;

c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2) (...)".

50. The rapporteur notes that during the investigation on 5 June 2019, the investigation team was informed that when an individual requests the deletion of their account, the company deactivates the account in question, preventing the individual from logging in and blocking the sending of marketing messages. The team thus noted the presence in the database of the personal data of a customer of the company who had previously made a request by email for deletion. Access to their account had simply been disabled.

51. In defence, the company first demonstrated the deletion of the data of the customer who had exercised their right to erasure of data after the CNIL's investigation. It then stated that it had taken various measures to improve its internal procedure for managing requests to exercise rights, by centralising the receipt of requests, by putting a form for exercising rights online and by creating the email address "dp[redacted]", dedicated to questions about personal data and managed by the company's data protection officer. In addition, the company indicated that it had developed a document containing letter templates for responding to requests to exercise rights, including a letter for responding to requests for erasure.

52. The Restricted Committee notes that at the time of the investigation of 5 June 2019, when a request for deletion was sent to it, the company simply deactivated the account of the data subject without deleting their personal data, namely their surname, first name, email address, postal address and telephone number, which was actually observed by the CNIL's team during the checks.

53. However, the Restricted Committee notes that when a person requests the erasure of their personal data, the data controller or its data processor must, in principle, actually delete the data once the conditions set out in Article 17 of the GDPR are met.

54. The Restricted Committee considers that whereas, after a request for deletion, certain personal data of customers may be kept in intermediate storage for specific purposes, in particular for legal obligations or evidential purposes or when the company has an overriding legitimate ground, that which is not necessary in order to comply with such obligations or purposes must be deleted after the exercise of this right, provided that the conditions laid down in Article 17 of the GDPR are met.

55. In view of the foregoing, the Restricted Committee considers that the breach of Article 17 of the GDPR is established.

56. However, it notes that, as part of the penalty proceedings, the company has demonstrated having taken measures to ensure compliance with this regulation.

E. Regarding the failure to provide a legal act for the processing operations carried out on behalf of the data controller pursuant to Article 28 of the GDPR

57. Article 28 of the Regulation provides that the processing carried out by a data processor on behalf of a controller is governed by a contract which defines 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. This contract also provides for the conditions under which the data processor shall carry out the processing operations on behalf of the data controller.

58. The rapporteur notes that, regarding the relations with its processors, the company sent two quotes countersigned with [redacted] which did not contain any of the clauses laid down in Article 28 of the GDPR and did not provide any legal act to govern its processing relationship with [redacted].

59. In defence, the company disputes these facts, and indicates that an agreement relating to the data processing had been signed by [redacted] on 17 April 2018, but that it had not been sent to the investigation team due to the inaccurate nature of its request for supporting documents made in the on-site investigation report. The company acknowledges the absence of an act to govern its relationship with [redacted].

60. The Restricted Committee notes that the data controller and the processor must enter into a contract which includes all the mandatory information laid down in Article 28 of the GDPR in order to organise their respective relationships and data protection obligations.

61. In this case, the Restricted Committee notes that the processing relationship with [redacted] was governed by a legal act at the time of the investigation carried out on 5 June 2019, under the provisions of Article 28 of the GDPR. However, on the day of the investigation, the processing relationship with [redacted] - which collects and records, on behalf of [redacted], customer data for the purposes of creating a customer account at the time of their visit to the store - was not governed by any legal act.

62. The Restricted Committee therefore considers that on the day of the investigation, the breach relating to Article 28 is established as regards the processing relationship between [redacted] and [redacted] due to the absence of a contract specifying in particular the data controller's rights and obligations and the conditions under which the data processor should carry out the processing operations on behalf of the data controller.

63. It nevertheless highlights that, as part of the penalty proceedings, the company provided evidence of a processing agreement signed with [redacted] on 26 August 2021, which meets the requirements of Article 28 of the GDPR.

F. Regarding the breach of the obligation to ensure the security of personal data pursuant to Article 32 of the GDPR

64. Under 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;

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing[…]".

65. **Firstly**, the rapporteur notes that at the time of the online investigation carried out on 9 May 2019, authentication when creating a customer account on the [redacted] website was based on a password composed only of a single numeric character, such as "1", without any criteria for the complexity of the password being provided.

66. In defence, the company does not dispute these facts, but maintains that the security obligation resulting from Article 32 of the GDPR is a best efforts obligation, not a performance obligation, so the controller's security obligation is to implement measures to reduce risks to an acceptable level, without it being compulsory, or even possible, to obtain a level of security so that the risks have no effect. The company also emphasises that the assessment of compliance with the security obligation by the controller requires consideration of the impact on the data subjects and its severity according to the categories of personal data concerned by the processing. It argues that, in the course of its business, it only collected and processed standard personal data, without any serious impact for the data subjects.

67. The Restricted Committee considers that the length and complexity of a password remain basic criteria for assessing its strength. It noted in this respect that the need for a strong password is also highlighted by ANSSI.

68. For the sake of clarity, the Restricted Committee notes that in order to ensure a sufficient level of security and satisfy the password strength requirements, when authentication relies solely on an identifier and password, the CNIL recommends, in its Decision No. 2017-012 of 19 January 2017, that the password have at least twelve characters - containing at least one upper-case letter, one lower-case letter, one number and one special character - or at least eight characters - containing three of these four characters - if it is accompanied by an additional measure such as, for example, the timing of access to the account after several failures (temporary suspension of access, the duration of which increases as attempts are made), setting up a mechanism to guard against automated and multiple attempts (e.g. a "captcha") and/or locking the account after several failed login attempts.

69. In this case, the Restricted Committee considers that, in view of the rules governing password composition, the strength of the passwords accepted by the company - containing one single number, such as "1", with no criteria for the complexity of the password being provided - was too weak, risking the related accounts and personal data they contain being compromised.

70. The Restricted Committee also considers that the lack of collection of so-called sensitive data by the company, which indicates only collecting identifying or contact data, does not prevent the occurrence of malicious acts such as phishing, which is mainly based on the use of accurate and directly identifying data in order to create confusion for the user who is the subject of it.

71. In these circumstances, the Restricted Committee considers that the respondent company's password management policy was not sufficiently robust and binding to ensure data security within the meaning of Article 32 of the GDPR.

72. However, it notes that, in the course of the penalty proceedings, the company indicated that, with regard to user accounts, it now requires a strong password comprising a minimum of twelve characters, including at least one upper-case letter, one lower-case letter, one numeric character and one special character, which was corroborated by supporting documents.

73. **Secondly**, the rapporteur notes that the hash function used for the storage of account passwords of customers using the [redacted] website was obsolete (MD5).

74. In defence, the company does not dispute these facts.

75. The Restricted Committee emphasises that since the algorithm of this hash function is obsolete and has for a long time had well-known vulnerabilities, making it liable to be easily "broken", this hash function no longer guarantees the integrity and confidentiality of passwords in the event of a brute force attack after compromise of the servers hosting them. Thus, the use of this algorithm would allow a person with knowledge of the hashed password

to decrypt it without difficulty in a very short time (e.g. by means of freely accessible websites that allow the value corresponding to the password *hash* to be retrieved).

76. In these circumstances, in view of the risks incurred by the individuals mentioned above, the Restricted Committee considers that the hash function used by the company did not make it possible to guarantee the security of the data of its 550,000 customers, within the meaning of Article 32 of the GDPR.

77. However, it notes that, as part of the penalty proceedings, the company demonstrated having implemented a satisfactory hashing function, in BCRYPT, for all customers' account passwords.

78. **Thirdly**, the rapporteur notes that the company's employees accessed the "read/write" version of [redacted]'s database via a joint account for four employees, which is not a satisfactory measure to ensure data security.

79. In defence, the company argues that the rapporteur did not take into account the complexity of the password kept secret between the four employees authorised to access the "read/write" version of the database, nor of the authentication system based on the network addresses allowing for traceability of the access and actions of these four authorised employees.

80. The Restricted Committee notes that assigning a unique identifier per user and prohibiting shared accounts are among the essential precautions to guarantee effective traceability of access to a database. It also emphasises that the use of shared access by several people does not make it possible to accurately attribute the actions carried out on the equipment in the event of simultaneous login-in, complicating for example audits of the use of the shared account. In this sense, ANSI recommends using, by default, individual administration accounts and specifies that generic accounts on the equipment should not be used, or then exceptionally and restricted to a very limited number of administrators, since only the creation of individual accounts allows for the implementation of a relevant access control and the attribution of the actions carried out by each of the administrators.

81. In this case, the sharing of the account allowing access to the "read/write" version of the database by four employees does not make it possible to guarantee proper authentication of users and, consequently, effective management of accreditations and proper traceability of access. The Restricted Committee observes that, for example, in the event of deletion or modification of data in the database, it would be complicated to attribute responsibility to one of the four authorised individuals if several of them were connected at the same time to this generic account.

82. Therefore, such a lack of traceability of access does not allow for the identification of fraudulent access or of the individual causing the deterioration or deletion of personal data.
83. In these circumstances, the Restricted Committee considers that the use of a joint account shared by four employees does not guarantee data security within the meaning of Article 32 of the GDPR.

84. It notes, however, that the company justified, during the proceedings, having set up a single sign-on system for each user from the creation of individual accounts for access to the database in order to ensure more detailed traceability of database access.

85. In view of all the above elements, the Restricted Committee considers that the breach of Article 32 of the GDPR is established.

86. However, the Restricted Committee notes that, as part of the penalty proceedings, the company has demonstrated having taken all measures to ensure compliance with this regulation.

III. Regarding corrective powers and their publication

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

"When the controller or its processor fails to comply with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or this law, the chairman of the CNIL may also, if applicable, after sending the warning provided for in point I of this article or, where applicable, in addition to an order provided for in II, contact the CNIL's Restricted Committee with a view to the announcement, after adversarial proceedings, of one or more of the following measures: […]
2. An injunction to make the processing compliant with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or this law or to comply with the requests made by the data subject to exercise their rights, which may be accompanied, except in cases where the processing is implemented by the State, with a penalty fine not exceeding 100,000 euros per day of delay from the date fixed by the Restricted Committee; […]
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 turnover. In determining the amount of the fine, the Restricted Committee shall take into account the criteria specified in the same Article 83."

88. 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 elements to be taken into account when deciding whether to impose an administrative fine and when deciding on the amount of that fine.

89. **Firstly**, on the principle of imposing a fine, the company maintains that such a measure is not justified. The company asserts that it has complied with its legal obligations and that it

has cooperated with the CNIL in a diligent manner and in good faith since the start of the proceedings. It therefore argues that imposing an administrative fine would go against the principles of the need for penalties and proportionality. It points out in particular that it has never been penalised by the Restricted Committee, that the aforementioned breaches do not in any way constitute a deliberate breach of the GDPR, that the data subjects have not suffered any damage, and that no specific data referred to in Articles 9 and 10 of the GDPR is concerned.

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

91. Firstly, the Restricted Committee notes that the company has demonstrated significant negligence with regard to the fundamental principles of the GDPR, since five breaches have been established, in particular concerning the principle of limiting the data retention period, the obligation to inform data subjects of the processing of their personal data and the obligation to respect their rights.

92. The Restricted Committee then notes that at least some breaches have been established over a period of several years and have affected a large number of people, almost 550,000 individuals, established in France and in six other Member States of the European Union.

93. The Restricted Committee also notes that, within the framework of the penalty proceedings, the company's cooperation with the supervisory authority meets the obligation of cooperation laid down in Articles 31 of the GDPR and 18 of the Act and cannot constitute a level of cooperation exceeding that which is reasonably expected. Therefore, the company's cooperation with the CNIL as part of the penalty proceedings cannot be considered as an extenuating circumstance when imposing an administrative fine.

94. In addition, the Restricted Committee notes that whereas the company only processes standard personal data, it is still required to implement appropriate technical and organisational measures in order to ensure a level of security for this data appropriate to the risk, in accordance with Article 32 of the GDPR and in accordance with the principles set out in Article 5 of the GDPR.

95. Finally, the Restricted Committee notes that compliance measures were only put in place by the company following the penalty proceedings and that they did not exempt it from its responsibility for the past.

96. Consequently, the Restricted Committee considers that an administrative fine should be imposed in view of the breaches of Articles 5(1)(e), 13, 17, 28 and 32 of the GDPR.

97. **Secondly**, with regard to the amount of the fine, the company considers that the amount of the fine proposed by the rapporteur is disproportionate in view of its economic situation. It highlights its poor financial situation and specifies that a high fine would have a significant impact on its business and economic development, particularly in terms of job creation.

98. The Restricted Committee notes that Article 83(3) of the Regulation provides that in the event of multiple breaches, as in the case in point, the total amount of the fine may not exceed the amount set for the most serious breach. Insofar as the company is alleged to be in breach of Articles 5(1)(e), 13, 17, 28 and 32 of the GDPR, the maximum fine that can be imposed is 20 million euros or 4% of annual worldwide turnover, whichever is higher.

99. The Restricted Committee also notes that administrative fines must be dissuasive but proportionate. In particular, it considers that the company's activity and financial situation must be taken into account when determining the penalty and, in particular, in the case of an administrative fine, its amount. In this regard, it notes that the company reports turnover in 2019 and 2020 of approximately 23 million euros, then approximately 30 million euros, with a net loss of -932,078 euros and then -1.7 million euros, respectively.

100. In view of this information, the Restricted Committee considers that imposing a fine of 120,000 euros seems justified for the breaches of Articles 5(1)(e), 13, 17, 28 and 32 of the GDPR.

101. **Thirdly**, an injunction to make the processing compliant with the provisions of Articles 5(1)(e), 13, 17, 28 and 32 of the GDPR was proposed by the rapporteur when the report was notified.

102. The company argues that the actions it has taken in relation to all the breaches identified should lead to no further action in respect of the Rapporteur's proposed injunction.

103. The Restricted Committee considers that the company has taken the necessary measures to ensure compliance. Consequently, the Restricted Committee considers that there are no longer grounds to impose an injunction for these points.

FOR THESE REASONS

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

- **impose an administrative fine against [redacted] for an amount of 120,000 (one hundred and twenty thousand) euros in respect of the breaches of Articles 5(1)(e), 13, 17, 28 and 32 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016**.

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