Final decision of restricted committee No. SAN-2021-008 of 14 June 2021 concerning

The Commission nationale de l'Informatique et des Libertés (CNIL - French Data Protection Authority), met in its Restricted Committee consisting of Mr. Alexandre LINDEN, Chairman and

Having regard to Regulation (EU) 2016/79 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data and on the free movement of such data;

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

Having regard to the French Post and Electronic Communications Code;

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. 2018-238C of 27 September 2018 of the CNIL Chair to instruct the secretary general to carry out or have a third party carry out an assignment to conduct verifications of the processing implemented by that organisation or on behalf of

Having regard to the decision of the CNIL Chair appointing a rapporteur before the Restricted Committee of 19 December 2019;

Having regard to the report of commissioner rapporteur, notified to on 2 October 2020;

Having regard to the written observations submitted by on 2 November 2020;

Having regard to the rapporteur's response to the observations notified on 24 November 2020 to the company's counsel;

Having regard to the written observations of received on 16 December 2020 and the oral observations made at the restricted committee meeting;

Having regard to the document relating ent of the procedure for the intermediate archiving and anonymisation of the data of 's prospects and customers submitted by the counsel of at the meeting of the restricted committee;

Having regard to the bailiff's minutes drawn up on 5 February 2021 and its appendix, sent by the company's counsel to the chairman of the restricted committee and to the rapporteur on 10 February 2021;

Having regard to the other documents in the file;

The following were present at the Restricted Committee session on 28 January 2021:

- Commissioner, heard in her report;

In their capacity as representatives of

- […]

having last spoken;

The restricted committee adopted the following draft decision:

I. Facts and proceedings

1. (hereinafter "the company") is a simplified joint stock company with a single shareholder, created in 2012. Its registered office is located at It is chaired by a simplified joint stock company, located at the same address.

2. The company publishes the website, which has been accessible in France and Spain since 2015, Italy since 2016, and Portugal since 2017. It is a sales were only available if you had created an account on the site. Since then, sales are visible without the need to create an account prior to viewing them. However, to make a purchase, it is still necessary to create an account on the website. In 2018, the company had users in France, users in Spain, users in Italy, and users in Portugal.

3. In 2018, the company generated revenue of approximately euros and a net profit of approximately euros. In 2019, it generated revenue of euros and a net profit of approximately euros. In 2020, the Company generated revenue of approximately euros and a net profit of approximately euros. In 2018, employed approximately 150 persons.

4. On 13 November 2018, pursuant to the CNIL chair's Decision No. 2018-238C of 27 September 2018, a CNIL delegation carried out an audit at the premises of The purpose of this audit was to verify compliance by the company 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 the 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. The audit focused on the processing of personal data of the company's customers and prospects. The verifications concerned in particular the retention periods for personal data are kept, the information provided to data subjects regarding the processing carried out by the company, compliance with requests for the erasure of personal data from data subjects, the obligation to ensure data security and the obligation to obtain the consent of the data subject to receive marketing messages by e-mail.

6. At the end of the audit, minutes No. 2018-238/1 were notified to the company by letter dated 19 November 2018. The company sent the CNIL, by e-mail sent that same day, the additional documents requested at the end of the audit.

7. By e-mail of 5 February 2019, the company provided the delegation with several additional documents on its own initiative, including a document entitled "Personal data storage procedure".

8. As the investigations established the cross-border nature of the processing concerned, the CNIL informed all the European supervisory authorities on 27 August 2019, in accordance with Article 56 of the GDPR, of its competence to act as lead supervisory authority, and thus opened the procedure for the declaration of the authorities concerned in this case.

9. On 27 September 2019, the CNIL Chair submitted a draft order to the authorities concerned. Following this communication, three authorities raised relevant and reasoned objections within the meaning of Article 60 GDPR, requesting for two of them that the draft order be amended into a draft penalty, and more specifically an administrative fine for one of the two authorities. In support of this request, the authorities concerned highlighted the number of breaches, the number of data subjects, and the size of the company.

10. In order to complete its investigations, on 6 February 2020, pursuant to the aforementioned Decision No. 2018-238C, the CNIL carried out an online audit of all processing accessible from the [redacted] domain.

11. This audit focused more specifically on the methods of informing the data subjects on the [redacted] website and on the depositing of cookies on the users' terminal when they arrive on the site.

12. Following the audit, minutes No. 2018-238/2 were notified to the company [redacted] by letter dated 19 February 2020. The company sent the CNIL, by emails dated 4 March and 9 July 2020, the additional documents and information requested at the end of the audit.

13. On 13 January 2021, a delegation from the CNIL, pursuant to the aforementioned Decision No. 2018-238C, carried out a new online audit of any processing accessible from the [redacted] omain. As the company indicated that changes had been made to the way in which cookies are deposited, it was decided to carry out a new audit in order to update the findings made on 6 February 2020.

14. At the end of the audit, minutes No. 2018-238/3 were notified to the company [redacted] by letter dated 14 January 2021. By e-mail dated 26 January 2021, the company sent the Commission the additional documents requested during the inspection.

15. In order to examine these items, the CNIL chair appointed [redacted] as rapporteur on 19 December 2019, pursuant to Article 22 of the amended Act of 6 January 1978.

16. At the end of her investigation, on 2 October 2020, the rapporteur sent [redacted] a report detailing the breaches of the GDPR that she considered to have occurred in this case and indicating to the company that it had a period of one month in which to submit its written observations pursuant to the provisions of Article 40 of Decree No. 2019-536 of 29 May 2019.

17. This report proposed to the CNIL's restricted committee to pronounce an injunction to bring the processing into line with the provisions of articles L. 34-5 of the French Post and Electronic Communications Code (hereinafter, "CPCE"), 82 of the French Data Protection Act, and 5(1)(e), 13, 17 et 32 of the GDPR, accompanied by a penalty fine at the end of a period of three months following notification of the decision of the restricted committee 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 period of two years following its publication.

18. On 2 November 2020, through its counsel, the company submitted observations.

19. On 5 November 2020, the company was sent a notice to attend the meeting of the restricted committee on 10 December 2020.

20. On 13 November 2020, the rapporteur asked for time to respond to the observations made by [redacted] By e-mail of 16 November 2020, the chairman of the restricted committee informed the rapporteur that she had an additional eight days to submit her observations. By letter dated 24 November 2020, the company was informed that it had also been granted an additional period of eight days and that, as a result, the meeting of the restricted committee initially scheduled for 10 December 2020 was postponed.

21. On 16 December 2020, the company submitted further observations in response to those of the rapporteur.

22. On 11 January 2021, the CNIL sent the company a notice to attend the restricted committee meeting on 28 January 2021.

23. The company and the rapporteur presented oral observations at that meeting.

24. On 19 May 2021, a draft decision was submitted to the concerned supervisory authorities as part of the cooperation procedure, on the basis of Article 60 of the GDPR.

25. This draft decision did not give rise to relevant and reasoned objections.

II. Reasons for the decision

A. On 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) GDPR

26. 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')".*

27. The rapporteur noted that, during the audit on 13 November 2018, the company told the delegation that no retention period for the personal data of customers (customers being, according to the company, holders of an account on the site who have already made at least one purchase) and prospects (holders of an account on the site who have never made a purchase) had been determined, and that it did not lawfully delete or archive such data at the end of a defined period.

28. In its defence, although it did not mention it during the audit, the company first argued that a retention period policy had been specified as early as 26 October 2018, so that it could not be accused of any breach for failure to specify retention periods.

29. In its observations of 16 December 2020, the company then indicated that the data of customers and prospects used for the purposes of marketing or managing their account was now retained in the active

database until their account is deleted or, in the event of inactivity, for three years from the last time they signed in to their account. At the end of those periods, the company specified that only the data necessary for pre-litigation or litigation purposes are archived until the date corresponding to the statute of limitations justifying their retention, after which they would be deleted.

30. Finally, at the meeting of the restricted committee and after the investigation procedure had been closed, the company produced a document intended to provide proof of the deployment of an intermediate archiving procedure and a data anonymisation process. By e-mail dated 10 February 2021, the company sent, through its counsel, a report drawn up on 5 February 2021, as well as its appendix, relating to the anonymisation process for the data of [redacted] s prospects and customers.

31. **According to the restricted committee**, with regard to the specification of retention periods applicable to the data of [redacted]'s customers and prospects, it should first be noted that the document entitled "Personal Data Retention Procedure" is dated 26 October 2018, i.e. prior to the audit. However, it was not communicated to the delegation until two months after the audit, on 5 February 2019, and on the day of the audit, 13 November 2018, the company informed the delegation that *"no retention period is implemented in the database"*.

32. The restricted committee then noted that during the audit of 13 November 2018, the delegation noted the presence, in the active database, of personal data of 16,653 persons who had not placed an order in more than five years, without the company being able to provide an explanation or justification as to the length of the retention period or to provide proof of more recent contact with the said customers (exchanges with customer service, clicking on a promotional link in an e-mail, etc.). In addition, the restricted committee found that, in response to a request for additional data from CNIL, on 4 March 2020 the company provided an Excel table, which shows the retention in its database of personal data of more than 130,000 persons who have not signed in to their customer account in more than five years.

33. Consequently, while 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) GDPR – by guaranteeing that the data are not retained for longer than is necessary for the purposes for which they are processed – it considers, in any case, that on the day of the audit, the retention policy was not complied with and that the data was retained for excessive periods. The CNIL's supervisory delegation found that personal data were kept for much longer periods than those specified in the aforementioned document, and that those periods did not appear to be appropriate for the purposes for which the data were processed.

34. Moreover, the restricted committee considered that the company had not provided, as at the closing date of the investigation, any evidence of compliance on this point. In any event, it considers that, in accordance with Article 40 of the decree of 29 May 2019 issued for the application of the "French Data Protection Act", the information provided at the meeting of 28 January 2021 is not, as it stands, sufficient to give an opinion at this stage on whether it has been brought in compliance with Article 5(1)(e) GDPR.

35. In the light of all these elements, the restricted committee considered that the breach of Article 5(1)(e) GDPR has been established, and that the company had not completely come into compliance by the closing date of the investigation.

B. On the breach of the obligation to inform individuals pursuant to Articles 13 GDPR

36. Article 13 GDPR requires the data controller to provide, at the time the data is collected, information on its identity and contact details, that of its data protection officer, the purposes and legal basis of the processing, the recipients or categories of recipients of the personal data, 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.

37. The rapporteur notes that, as it appears from the findings of the on-site inspection conducted on 13 November 2018 and the online audit of 6 February 2020, the information made available to users of the website was not complete within the meaning of Article 13 of the Regulation. In fact, certain mandatory information provided for by that Article – namely the contact details of the data protection officer, the retention periods, the legal bases of processing and certain data protection rights – were not brought to the attention of the data subjects on the [redacted] website, whether through the general terms and conditions of sale, the "legal and personal data notices" or the personal data retention policy.

38. In its defence, the company stated that it had made corrections in the course of the proceeding, in order to provide information that complied with the requirements of the GDPR.

39. **According to the restricted committee, firstly**, with regard to the contact details of the data protection officer, the restricted committee noted that the company acknowledged that these were not present on the [redacted] website until the notification of the penalty report, but specified that it was nevertheless possible to send it a request via an "unsubscribe and unregister" section within a contact form.

40. On this point, the restricted committee recalls first of all that, although it may be a useful modality, allowing customers and prospects to be put in touch with the data protection officer via a contact form dedicated to "unsubscribing and unregistering" is not a measure likely to enable compliance with the provisions of Article 13 GDPR, which requires the provision of the "contact details" for the data protection officer. Moreover, the restricted committee finds that, as at the date of the on-site inspection of 13 November 2018, the contact form was accessible from a *"Customer Service – Contact Us"* section, which, it is specified, can be used to ask *"questions about an order or for information about [the] products [of the company]"*. In such circumstances, data subjects could not spontaneously expect to be put in touch with the data protection officer to exercise their rights under the GDPR. In any event, individuals may wish to use the data protection officer's contact details to send requests to exercise rights that are not limited to requests for unsubscribing and unregistering, such as a right of access request.

41. Under such conditions, the restricted committee therefore considers that the company breached the provisions of Article 13 GDPR.

42. The restricted committee nevertheless notes that the company had adopted measures in the context of the penalty proceeding and had demonstrated having brought into compliance its data protection policy, which now contains the contact details of the data protection officer.

43. **Secondly**, with regard to data retention periods, the company indicated that it had informed the CNIL by email on 5 February 2019 that its data retention policy had been made available to data subjects on its [redacted] website following the on-site inspection on 13 November 2018.

44. In this respect, the restricted committee first notes that the observations made during the inspection of 13 November 2018 attest to the absence of information on retention periods in the "legal and personal data notices", the "general terms of sale" or any other document available on the company's website. The restricted committee then notes that, although during the online inspection of 6 February 2020, the

delegation noted the presence of a link to a personal data retention policy, it also noted that the link was inactive. The policy was therefore inaccessible to users, as it was not otherwise available on the site.

45. Under such circumstances, the restricted committee considers that the breach of Article 13 of the GDPR is indeed demonstrated on this point, since the personal data are collected from the data subject and the information on the retention periods is among the information that must be communicated in this case, 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 are kept by the controller and, consequently, how long they can exercise their right of access.

46. The restricted committee nevertheless notes that, in the context of the penalty proceeding, the company had demonstrated having brought into compliance its data protection policy, which now contains the notices concerning retention periods for the data processed.

47. **Thirdly**, with regard to information concerning lawful bases, the company does not dispute that until 30 October 2020 no information on the lawful bases was made available to data subjects in the document entitled "Legal and personal data notices". However, it argued that *"it cannot be blamed for a total lack of information on the legal bases insofar as some of them were available through different media"*, e.g. in the general terms and conditions of sale, and that *"compilation work was in progress at the time of the audits"*.

48. The restricted committee notes that until 30 October 2020, the data subjects were not informed of all the legal bases of the processing operations implemented. In any case, if some information was available in other documents, the restricted committee notes that it was not exhaustive, and furthermore that the accessibility and provision of information at the time of collection of the data subject's data is a condition required under Recital 61 and Articles 12 and 13 GDPR.

49. In light of the foregoing, the restricted committee therefore considers that the company did not comply with the provisions of Article 13 GDPR.

50. The restricted committee nevertheless notes that, in the course of the penalty proceeding, the company had demonstrated having brought into compliance its data protection policy, which now presents complete information on legal bases.

51. **Fourthly**, with regard to information relating to data subject rights, the company argues that *"the lack of any mention of certain data protection rights on the* [redacted] *website results from a mere oversight and does not in any way constitute a desire on the part of* [redacted] *to prevent the exercise of certain rights by data subjects"*.

52. However, the restricted committee notes that, during the verifications carried out on 13 November 2018 and 6 February 2020, the supervisory delegation found that the company did not inform data subjects of their right to restriction of processing, to data portability and to lodge a complaint with a supervisory authority.

53. Under such circumstances, the restricted committee considers that the breach of Article 13 of the GDPR is established on this point since the personal data are collected from the data subject and the information missing in this case is among those that must be communicated in such cases. Indeed, providing information to individuals of all their rights helps to guarantee fair and transparent data processing, in

that it facilitates their exercise and thus helps to ensure that data subjects have control over the processing of their data.

54. However, the restricted committee notes that the company has demonstrated that it has brought into compliance its data protection policy, which now contains full information on the rights of data subjects. In addition, the company states that it has put a page online describing the rights of individuals under the GDPR, accessible via a link at the foot of each page of its website.

55. Consequently, the restricted committee considers that the aforementioned facts constitute a breach of Article 13 of the GDPR, but that the company had complied with all the points raised by the end of the investigation.

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

56. Under Article 17 GDPR, the data subject has the right to *"obtain from the controller the erasure of personal data relating to him or her without undue delay and the controller shall be obliged to erase such 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 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) (...)".

57. During the inspection on 13 November 2018, the supervisory delegation was informed that when an individual requests the deletion of their account, the company does not delete the personal data but only deactivates the account in question, preventing the individual from logging in and blocking the sending of marketing messages. The delegation thus noted the presence in the database of the personal data of a customer of the company (surname, first name and e-mail address) who had previously made a request by e-mail for deletion. Access to his account had simply been disabled.

58. The restricted committee holds that it was thus established that the company did not fully comply with deletion requests.

59. The restricted committee considers that if, after a request for deletion, certain personal data of customers may be kept in intermediate storage, in particular for legal obligations or evidential purposes or when the company has an overriding legitimate ground, those not necessary in the context of compliance with such other obligations or purposes must be deleted after the exercise of this right, provided that the conditions laid down by Article 17 GDPR are met. It notes in this respect that this was at least the case for the processing of the e-mail address used for marketing purposes, since such processing is based on consent and the right to erasure is available in the event of withdrawal of consent, and that it does not appear from the elements of the proceeding that the retention of the data in question was legitimate on any other basis.

60. In view of the foregoing, the restricted committee considers that the breach of Article 17 GDPR is established.

61. However, it notes that, in the context of the penalty proceeding, the company has demonstrated having taken measures to come into compliance with Article 17 GDPR.

62. The company first demonstrated the deletion of the data of the customer who had exercised his right to erasure of data. It then stated that it had taken various measures to improve the processing of requests to exercise rights, by centralising the receipt of requests, by putting a form for exercising rights online - which can be downloaded via a direct link inserted on the information page dedicated to the rights of individuals - and by creating the e-mail address [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 to exercise the right to erasure. Finally, the company has undertaken to set up a tracking system for requests to exercise rights in a specific tool.

D. On the breach of the obligation to ensure the security of personal data pursuant to Article 32 GDPR

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

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

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[…]".

64. **Firstly**, the rapporteur notes that at the time of the inspection on 13 November 2018, authentication when creating an account on the [redacted] website was based on a password composed solely of six numeric characters, of the "123456" type. The rapporteur then notes that, as regards the company's employees, the password for accessing the [redacted] customer relationship management software was composed of eight characters, containing at least one number and one letter. Finally, the rapporteur notes that the authentication of employees to the databases was insufficiently secure because the passwords for accessing them were stored, unencrypted, in a text file located on a company computer.

65. Firstly, the company does not dispute these facts, but maintains that the security obligation resulting from Article 32 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 rendering them null and void. The company also stressed that it has never suffered a personal data breach.

66. The restricted committee considers that the absence of a personal data breach is not sufficient to demonstrate the absence of an offence, nor is a data breach in itself sufficient to characterise a breach of this article. It is the task of the restricted committee to verify that the controller or, where applicable, the processor, has implemented, in accordance with this article, appropriate technical and organisational measures to prevent the risks of violation and misuse of such data. The appropriateness of the measures is assessed by verifying that the respondent has proportioned those measures, on the basis of the information available to it through reasonable diligence, to the seriousness and likelihood of the foreseeable risks, taking into account the nature and context of the data processing and the cost and complexity of the possible measures.

67. Next, 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 recalled 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 intensive 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 their composition, the strength of the passwords accepted by the company was too weak, leading to a risk of compromise of the personal data it contains.

70. Finally, the restricted committee recalled that storing database access passwords unencrypted in a text file on a company computer is not a secure password management solution. Indeed, authentication based on the use of a short or simple password can lead to attacks by unauthorised third parties, such as "brute force" attacks, which consist of systematically testing numerous passwords in succession and thus allowing the associated accounts and the data they contain to be compromised.

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 GDPR.

72. However, it notes that, in the course of the penalty proceeding, the company indicated that, with regard to customer accounts, it now requires a strong password comprising a minimum of twelve characters, including one upper-case letter, one lower case letter, one numeric character and one special character, which was corroborated by a screen print. For employees, the company has implemented a strong password on access to [redacted] Concerning the storage of database access passwords in an unencrypted file, the company demonstrated having discontinued the practice and that it has implemented a secure password management solution by subscribing to the [redacted] solution, which guarantees encrypted password storage.

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

74. In its defence, the company did not contest these facts, but repeated the same argument on the best-efforts obligation.

75. The restricted committee recalls that the use of the MD5 hash function by the company has not been considered state of the art since 2004 and its use in cryptography or security is prohibited. 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 system used did not make it possible to guarantee the security of the data, within the meaning of Article 32 GDPR.

77. However, it notes that, in the context of the penalty proceeding, the company demonstrated having implemented a satisfactory hashing system, in SHA256, of all users' passwords.

78. **Thirdly,** the rapporteur notes that the company's employees had access to a copy of the [redacted] production database through an account shared by four employees.

79. In its defence, the company did not contest these facts, but repeated the same argument on the best-efforts obligation.

80. The restricted committee recalls that the attribution of a unique identifier per user and the prohibition of shared accounts are among the indispensable precautions to guarantee effective traceability of access to a database. In this case, the sharing of the account allowing access to the copy of the production 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. Such a lack of traceability of access does not allow the identification of fraudulent access or the author of any deterioration or deletion of personal data.

81. In these circumstances, the restricted committee considers that the use of a generic account does not guarantee data security within the meaning of Article 32 GDPR.

82. However, it notes that, in the context of the penalty proceeding, the company demonstrated having taken measures by setting up an authentication system for accredited users.

E. On the breach of obligations relating to information (cookies) stored on users' electronic communications terminal equipment, in accordance with Article 82 of the French Data Protection Act

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

83. Article 82 of the French Data Protection Act requires that users be informed and that their consent be obtained before any registration or access to information already stored in their equipment. Any deposit of cookies or other trackers must therefore be preceded by the information and consent of the persons concerned. This requirement does not apply to cookies whose "exclusive purpose is to enable or

facilitate electronic communication", or those "strictly necessary for the provision of an online communication service at the express request of the user".

84. The rapporteur considers that the company did not comply with these provisions since it emerged from the online inspections of 6 February 2020 and 13 January 2021 that, on arrival at the [redacted] website, several cookies that did not fall within the scope of the two exceptions mentioned above were deposited on the user's terminal as soon as they arrived on the site's home page, and before any action on their part.

85. The company does not dispute these facts.

86. In fact, the restricted committee notes that it emerged from the findings of the online inspection of 6 February 2020 that thirty-two cookies were automatically deposited as soon as the user arrived on the site's home page, and before any action was taken by the user. In response to a request for further information from the CNIL, the company indicated on 4 March 2020 that the purposes of the cookies deposited were to have *"better knowledge of customers"*, *"better advertising targeting"* and to personalise *"the offering and promotional operations"*.

87. The restricted committee also noted that, even though the company had stated, in its observations in response of 16 December 2020, that it had *"stopped, since 10 November 2020 automatic depositing cookies subject to consent"* when users arrived on its site, the delegation noted, during the online inspection of 13 January 2021, the deposit of thirteen cookies upon arrival on the website. By e-mail dated 26 January 2021, the company sent the additional documents requested during the inspection and confirmed, in particular, that some of the cookies deposited were for advertising purposes.

88. Consequently, since the cookies deposited were not exclusively for the purpose of allowing or facilitating electronic communication and were not strictly necessary for the provision of the service, the company is required to obtain the consent of users prior to their deposit.

89. The restricted committee therefore considers that there has been a breach of Article 82 of the French Data Protection Act.

90. However, the restricted committee emphasised that the company had made significant changes to its website during the penalty proceeding, and that the cookies for which users' consent was required were no longer automatically deposited on the user's terminal when they arrived on the site's homepage since 26 January 2021.

F. On the breach of the obligation to gather consent from the data subject of a direct marketing operation using an electronic communications system in accordance with Article L. 34-5 CPCE

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

91. According to Article L. 34-5 CPCE: *"Direct marketing by means of automated electronic communication systems within the meaning of Article L. 32, 6°, is prohibited, by fax or electronic mail using the contact details of a natural person, subscriber or user, who has not expressed their consent prior to receiving direct marketing by this means.*

For the application of the present article, consent shall mean any expression of free, specific and informed intent whereby a person agrees that personal data related to them is used for direct marketing purposes. […]

However, direct e-mail marketing is authorised if the recipient's contact details have been collected from them, in compliance with the provisions of French Data Protection Act No. 78-17 of 6 January 1978, in connection with a sale or provision of services, if the direct marketing concerns products or services similar to those previously provided by the same natural person or legal entity, and if the recipient is offered, expressly and unambiguously, the opportunity to object, without charges, other than those related to the transmission of the refusal, in a simple manner, to the use of his/her contact details at the time they are collected and every time a marketing e-mail is sent to them if they have not initially refused such use".

92. The rapporteur notes that during the inspections carried out on 13 November 2018 and 6 February 2020, the delegation found that, when an account was created without a purchase being made on the company's website, no procedure for obtaining consent to the collection and processing of personal data for the purpose of marketing by e-mail was implemented.

93. In its defence, the company argued that because of the information on the site, individuals who had created an account could not have been unaware that the company would regularly send them commercial communications by e-mail. It also recalls that in order to validate a registration when creating an account on the company's website, the person must accept the company's general terms and conditions of sale, which provide that their personal data will be used by the company to inform them by e-mail of upcoming sales and special offers.

94. The restricted committee considers that the creation of an account does not prejudge the eventual ordering of products from the company [redacted] The restricted committee considers that, in the absence of purchases, the company cannot validly plead the benefit of the exception created by Article L. 34-5 CPCE allowing marketing without prior consent when the recipient's contact details have been collected from them in connection with a sale or provision of services and if the direct marketing concerns products or services similar to those provided by the same natural person or legal entity.

95. Consequently, the restricted committee considers that the company was required to obtain the free, informed, specific prior consent of persons creating an account on its website without having made a purchase, to receive direct marketing messages by e-mail, in accordance with Article L. 34-5(1) CPCE.

96. In these circumstances, the restricted committee considers that the breach of Article L. 34-5 of the CPCE is established.

In the course of the proceeding, the company demonstrated having inserted a checkbox on the online account creation form to allow for specific and unambiguous consent to be taken into account for persons wishing to create an account in the future.

97. For individuals who already had an account on the [redacted] ebsite, the company says it plans to send marketing emails only to those who have already made a purchase on its site. It also reported that it had sent emails to obtain the consent of 549 prospects who had not yet given their consent to receive electronic marketing messages or made a purchase following the creation of their account.

98. During the meeting of the restricted committee, the company also specified that in order to comply with the provisions of Article L. 34-5 CPCE, it intended to send each prospect who had not yet given their consent five e-mails aimed at obtaining their consent to receive electronic marketing. Those five emails would be sent within a period of 100 days from the date of the prospect's last activity. The company indicated that after 100 days of inactivity on the part of the prospect and without the latter's consent to receive marketing messages following the five e-mails it had sent to them, it would stop marketing to them.

99. The restricted committee considers that the fact of soliciting the persons in question to ask them if they wish to receive marketing e-mails constitutes in itself a processing operation which cannot be based, in this case, on any legitimate interest of the company. It is clear from the documents in the file that, by choosing to create an account on the company's website in order to access its offers, the prospective customers have shown a certain interest in the services offered by the company and that they can therefore reasonably expect the company to contact them. However, it considers that sending prospects five emails, let alone over a period of 100 days, exceeds the number of emails they could reasonably expect to receive.

100. In these circumstances, the restricted committee considers that the company has not been brought in full compliance by the closing date of the investigation.

III. On corrective powers and their publication

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

"When the controller or his processor fails to comply with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or this law, the chair 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 restricted committee of the CNIL with a view to the announcement, after adversarial procedure, of one or more of the following measures: […]
2. An injunction to bring the processing into compliance 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 his/her 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 said turnover. In determining the amount of the fine, the Restricted Committee shall take into account the criteria specified in the same Article 83."

Article 83 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 to decide on the amount of that fine.

102. **Firstly**, on the principle of imposing a fine, the company maintains that such a measure is not justified. It points out in particular that it has never been condemned 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, that no specific data referred to in Articles 9 and 10 GDPR is concerned, that it has cooperated in good faith with the CNIL throughout the procedure and that it has taken measures to bring itself into compliance.

103. The rapporteur recalls that in determining the amount of an administrative fine, the restricted committee must take into account the criteria specified in Article 83 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.

104. Firstly, the restricted committee considers that the company has demonstrated gross negligence with regard to the fundamental principles of the GDPR, since six breaches have been found, particularly of 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.

105. The restricted committee then noted that several breaches found concerned a significant number of individuals, namely [redacted] users in France, [redacted] in Spain, [redacted] n Italy and [redacted] in Portugal.

106. Finally, the restricted committee notes that the compliance measures put in place following the notification of the penalty report do not concern all the breaches and do not exonerate the company from its responsibility for the past, in particular in view of the breaches observed,

107. Consequently, the restricted committee considers that an administrative fine should be imposed in view of the breaches of Articles 5(1)(e), 13, 17 and 32 GDPR, 82 of the French Data Protection Act and L. 34-5 of the CPCE.

108. **Secondly**, with regard to the amount of the fine concerning breaches of the GDPR, the restricted committee recalls that Article 83(3) GDPR 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 and 32 GDPR, the maximum fine that can be imposed is 20 million euros or 4% of annual worldwide turnover, whichever is higher.

109. With regard to the amount of the fine relating to the breach of Article 82 of the French Data Protection Act and Article L. 34-5 CPCE, the restricted committee recalls that with regard to breaches of provisions originating in texts other than the GDPR, as is the case with Article L. 34-5 CPCE, which transposes into domestic law the "ePrivacy" Directive, Article 20, paragraph III, of the "French Data Protection Act" gives it the competence to impose various penalties, in particular an administrative fine, the maximum amount of which may be equivalent to 2% of the total annual worldwide turnover of the previous financial year generated by the controller. Furthermore, the determination of the amount of this fine is assessed in light of the criteria specified in Article 83 GDPR.

110. The restricted committee also recalls 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 from 2018 to 2020 of approximately [redacted] euros, then approximately [redacted] euros and finally approximately [redacted] euros, for a net profit of [redacted] euros, then [redacted] euros and finally [redacted] euros, respectively. Consequently, the amount proposed in the report is far from reaching the maximum amount of financial penalty stipulated by the GDPR since it represents only [redacted]% of the company's turnover. In view of these elements, the restricted committee considers that the imposition of a fine of 500,000 euros appears justified, i.e. 300,000 euros for the breaches of Articles 5(1)(e), 13, 17 and 32 GDPR and 200,000 euros for the breaches of Article 82 of the French Data Protection Act and Article L. 34-5 CPCE.

111. **Thirdly,** an injunction to bring the processing into compliance with the provisions of Article 5(1)(e) GDPR and Article L. 34(5) CPCE was proposed by the rapporteur when the report was notified.

112. The company argues that the actions it has taken in relation to all the breaches identified should lead to the Rapporteur's proposal for injunctions not being followed.

113. With regard to the breach of the obligation to define and respect a retention period for personal data proportionate to the purpose of the processing pursuant to Article 5(1)(e) GDPR, the company indicated that it had implemented an internal procedure for archiving and then anonymising the data.

114. However, the restricted committee considered that the company had not provided, as at the date of the close of the investigation, any information enabling it to attest to compliance on this point. In any case, it considers that the information provided during the session is not sufficient to decide at this stage whether it will comply with Article 5(1)(e) GDPR.

115. With regard to the breach of the obligation to obtain the consent of the data subject of a direct marketing operation by means of an automated electronic communications system pursuant to Article L. 34-5 CPCE, the restricted committee considers that the company has taken satisfactory measures to obtain the consent of persons when creating an account on the [redacted] website. The restricted committee also noted that the company had undertaken, in the course of the procedure, to stop sending direct marketing messages by e-mail to prospective customers without their prior consent. However, it considers that it has not demonstrated full compliance with Article L. 34-5 CPCE insofar as it intends to seek the consent up to five times of persons who have created an account in the past. Consequently, the restricted committee considers that an injunction should be imposed on this point.

116. **Fourthly,** the restricted committee considers that the publication of the penalty is justified in view of the plurality of breaches identified, their persistence, their seriousness and the number of data subjects.

FOR THESE REASONS

The CNIL's restricted committee after having deliberated, intends to decide to:

- **Impose an administrative fine on [redacted] in the amount of 500,000 (five hundred thousand) euros for all the breaches found, which breaks down as follows:**
    - **300,000 (three hundred thousand) euros** for breaches of Articles 5(1)(e), 13, 17 and 32 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter "GDPR");
    - **200,000 (two hundred thousand) euros** for breaches of Article 82 of the amended French Data Protection Act of 6 January 1978, and of Article L. 34-5 of the French Post and Electronic Communications Code (hereinafter "CPCE");
- **Issue an injunction against [redacted] to bring the processing operations into compliance with the obligations** resulting from Articles 5(1)(e) GDPR and L. 34-5 CPCE, and in particular:
    - **With regard to the breach of the principle of limiting the retention period of personal data, specify and implement a personal data retention policy which does not exceed the period necessary for the purposes for which it is collected and processed, and in particular:**
        - Stop retaining the personal data of former customers of the company's website after a fixed period of inactivity, purge such data retained by the company up to the date of the restricted committee's decision, and provide proof of the deletion of such personal data beyond a specific inactivity period, which the company is responsible for proving;
        - Provide proof that a procedure has been set up for the intermediate archiving of customers' personal data, after having sorted the relevant data to be archived and deleted the non-relevant data, and provide proof of the starting point of this archiving (e.g. invoices archived for accounting purposes);
    - **With regard to the breach of the obligation to obtain the consent of the individual data subject concerned by a direct marketing operation by means of an automated electronic communications system:** cease marketing to non-customers who have not expressed their consent, unless their consent is obtained;
- Attach to the injunction a penalty fine of 500 (five hundred) euros per day of delay at the end of a period of three months following notification of this decision, with proof of compliance to be sent to the restricted committee within this period;
- Make public, on the CNIL website and on the Légifrance website, its decision, which will no longer identify the company at the end of a period of two years following its publication.

The Chairman

Alexandre LINDEN