Deliberation of the Restricted Committee no. SAN-2024-002 of 31 January 2024 concerning the company [redacted]

The Commission nationale de l'informatique et des libertés (CNIL), meeting in its Restricted Committee composed 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 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on the processing of personal data and the protection of privacy in the electronic communications sector;

Having regard to the French Data Protection Act no. 78-17 of 6 January 1978, and in particular Articles 20 et seq.;

Having regard to amended decree no. 2019-536 of 29 May 2019, adopted for the application of the Data Protection Act no. 78-17 of 6 January 1978;

Having regard to deliberation no. 2013-175 of 4 July 2013 adopting the internal regulations of the French Data Protection Authority;

Having regard to Decision no. 2021-193C of 29 June 2021 of the Chair of the French Data Protection Authority to instruct the Secretary General to carry out, or instruct others to carry out, verification of the processing of personal data implemented by or on behalf of the company;

Having regard to the decision of the Chair of the French Data Protection Authority appointing a rapporteur before the Restricted Committee, dated 6 February 2023;

Having regard to the report of [redacted], reporting auditor, notified to [redacted] on 20 July 2023;

Having regard to the written observations submitted by [redacted] on 8 September 2023;

Having regard to the observations in response of the rapporteur on 6 October 2023;

Having regard to the observations in response of [redacted] on 2 November 2023;

Having regard to the other documents in the case file;

The following were present at the Restricted Committee session of 21 December 2023:

- [redacted], rapporteur, whose report was read out;

As representatives of [redacted]:

- [redacted];

- [redacted],
  [redacted].

[redacted] having spoken last;

The Restricted Committee adopted the following decision:

I. Facts and proceedings

1. The company [redacted] (hereinafter "the company"), whose registered office is located at [redacted], Paris ([redacted]), was registered in the Trade and Companies Register on [redacted]. In 2021, its turnover amounted to €[redacted] for a net result of €[redacted] and, in 2022, to €[redacted] for a net result of €[redacted].

2. [redacted] provides individuals with a range of publications and services that enable them to enter into real estate transactions without an intermediary. The company publishes the [redacted] website, which gives individuals the opportunity to publish or consult real estate advertisements and access various tools for managing real estate projects [redacted].

3. Two investigations were carried out pursuant to Decision no. 2022-041C of 2 March 2022 of the President of the CNIL in order 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 GDPR") and Act no. 78-17 of 6 January 1978 on information technology, files and freedoms, as amended (hereinafter "the French Data Protection Act"). On 8 March 2022, the CNIL departments carried out an online inspection from the "[redacted]" website. On 7 April 2022, the CNIL departments carried out an on-site inspection at the company's premises located in [redacted] ([redacted]).

4. The main purpose of the online inspection of the [redacted] website was to verify the procedures for informing individuals and the procedure for creating a user account. The on-site inspection focused more specifically on the verification of the retention periods applied to user account data, the supervision by a legal act of the processing carried out by a processor, the technical and organisational measures intended to ensure the security of the data collected through the website, and the notification of individuals of prospecting for similar products and services.

5. In emails dated 10 April and 7 June 2022, the company supplied the Commission with additional information.

6. On 17 January 2023, in accordance with Article 56 of the GDPR, the CNIL informed all European supervisory authorities of its competence to act as lead supervisory authority with regard to cross-border processing operations implemented by the company, resulting from the fact that the company's sole establishment is located in France. After discussion between the CNIL and the European data protection authorities within the framework of the one-stop-shop mechanism, it transpires that the German, Austrian, Belgian, Danish, Spanish, Finnish, Greek, Irish, Italian, Dutch, Norwegian, Polish, Portuguese and Swedish authorities are concerned by the processing of user accounts that have been created by persons residing in these States.

7. On 6 February 2023, for the purpose of examining this information, the Chair of the Commission appointed [redacted] as rapporteur under Article 22 of the French Data Protection Act.

8. On 20 July 2023, the rapporteur sent the company a report detailing the breaches of Articles 5-1-e), 12, 13, 28 and 32 of the GDPR, and of Article L.34-5 of the French Postal and Electronic Communications Code, which she considered to have been demonstrated in this case.

9. On 8 September 2023, the company submitted observations in response to the sanction report.

10. On 6 October 2023, the rapporteur responded to the company's observations.

11. On 3 November 2023, the company sent further observations in response to the rapporteur's observations.

12. In a letter dated 9 November 2023, the rapporteur informed the company that the investigation was closed, pursuant to Article 40, III, of amended Decree no. 2019-536 of 29 May 2019.

13. In a letter dated the same day, the company was informed that the case file had been included on the agenda of the Restricted Committee of 30 November 2023.

14. In an email dated 14 November 2023, the company's counsel requested a postponement of the Restricted Committee session.

15. In a letter dated 16 November 2023, the company's counsel was informed of the postponement of the meeting to 21 December 2023.

16. The rapporteur and the company made verbal observations at the Restricted Committee session.

II. Reasons for the decision

A. With regard to the European cooperation procedure

17. Pursuant to Article 60(3) of the GDPR, the draft decision adopted by the Restricted Committee was sent on 29 December 2023 to the relevant European supervisory authorities.

18. As of 26 January 2024, none of the supervisory authorities concerned had raised a relevant, reasoned objection to this draft decision, so that, pursuant to Article 60(6) of the GDPR, they are deemed to have approved it.

B. On the breach of the obligation to limit the data retention period

19. Pursuant to Article 5-1, e) of the GDPR, personal data must be "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed*".

20. **The rapporteur** noted that, during the on-site inspection, the company stated that it had specified different data retention policies according to the type of users of the [redacted]

website. Thus, with regard to customer data (individuals using the site's paid services), the rapporteur noted that the company had specified a retention period of 10 years from the date of acceptance of the order. It noted that the consistent and indiscriminate retention of all account data for 10 years did not appear justified with regard to the legal obligation stemming from the French Consumer Code, and that the extracted data from the supplied database included data relating to transactions of less than 120 euros whose retention did not appear justified. With regard to user data (persons using the free services of the site), the rapporteur noted that although the company had specified a retention period of 5 years from the date of the last login to the account, it was apparent from the on-site inspection that the company had retained 2,394,538 lines for more than 5 years and less than 10 years, and 737,563 lines for more than 10 years.

21. **In defence**, with regard to the data of customers using paid advertisements, the company specified during the investigation that it retained the advertisement and email address for 10 years for the purposes of compliance with the legal obligations arising from Articles L.213-1, D.213-1 and D.213-2 of the French Consumer Code and anti-fraud measures, and because of the specific characteristics related to the real estate business. It set out the two paid packages offered to customers: either a no-commitment contract for 59 euros per month which is considered as a permanent contract, or a 3-month contract for 135 euros. For non-binding contracts, considering that it was unable to determine the time of the contract in advance, the company stated that it retained all data relating to these contracts for a period of 10 years, regardless of the final amount. It also considers that account should be taken of the financial implications of subsequent advertisements and contracts for the sale of goods worth well over €120. It also stated that the retention period for birth years had been reduced to 25 months, and that data relating to an inactive account was retained for a reduced period of 3 years of inactivity.

22. With regard to data relating to users, during the investigation, the company specified that it retained the email address and the associated account for a period of 5 years only for litigation and anti-fraud purposes, and that it had deleted the data retained beyond this period of 5 years.

23. **The Restricted Committee** pointed out that it is the responsibility of the data controller to specify and implement a data retention period which does not exceed a period necessary for the purpose for which it is being processed.

24. With regard to the relevant periods, the Restricted Committee notes by way of illustration that in its reference framework relating to the processing of personal data for the purposes of managing commercial activities, the CNIL specifies that the data necessary for the performance of a contract are to be retained during the contractual relationship and that factors such as compliance with a legal obligation incumbent on the organisation may justify a longer retention period. Failing this, retention must be founded on another legal basis provided for in Article 6 of the GDPR.

25. In this respect, pursuant to Article L. 213-1 of the French Consumer Code: "*In cases where the contract is concluded electronically and relates to a sum equal to or greater than an amount fixed by decree, the professional contractor shall ensure the retention of the document bearing witness to that contract for a period determined by the same decree, and shall guarantee access to it at all times to its co-contractor, if the latter so requests*".

26. Article D. 213-1 of the same code provides that "*[t]he amount referred to in Article L. 213-1 is set at 120 euros*" and Article D. 213-2 provides that "*[t]he period referred to in Article L. 213-1 is set at ten years from the conclusion of the contract, in cases where the delivery of the goods or the performance of the service is immediate. Otherwise, the period shall run from the conclusion of the contract until the date of delivery of the goods or performance of the service, and for a period of ten years from this date*".

27. In this case, **the Restricted Committee** notes first of all, with regard to the retention of customer data, that the retention period of 10 years from the date of acceptance of the order specified by the company is justified by its legal obligations under the aforementioned French Consumer Code for contracts of an amount greater than 120 euros. The Restricted Committee is therefore of the view that, for the 3-month contracts proposed by the company for an amount of 135 euros, the retention of data for a period of 10 years is fully justified.

28. However, the Restricted Committee notes that, for non-binding contracts of an amount of 59 euros per month, the company retains the data relating to these contracts by default as soon as they are concluded, and even in cases where the total amount paid by the user is less than 120 euros. However, in a case where a customer has used the company's paid services for only 1 or 2 months, i.e. for a sum less than 120 euros, the data retention period provided for by the French Consumer Code would not apply. The restricted committee points out that Article D.213-1 of the Consumer Code expressly states that *"when the contract (...) is for a sum equal to or greater than"*, the only sum to be considered is therefore that of the contract concluded between company [redacted] and the customer, especially as company [redacted] is a third party to the contract for the sale of goods concluded between the seller and the buyer. The Restricted Committee is therefore of the view that the retention of customer data in the situation described above cannot be justified by citing compliance with the French Consumer Code, contrary to what the company states.

29. In this respect, the Restricted Committee notes that an extraction of 100 lines, corresponding to accounts of customers who placed orders more than 5 years ago, shows that 69 of them related to orders of an amount less than 120 euros. The Restricted Committee is therefore of the view that the company has retained data from accounts not covered by Article D. 213-1 of the French Consumer Code for excessive periods.

30. Next, **the Restricted Committee** notes, with regard to the retention of user data, that the company has specified a period of 5 years which starts on the date of the last login to the user account. The Restricted Committee is of the view that the explanations provided by the company during the investigation justify the retention period for litigation and anti-fraud purposes.

31. Nevertheless, **the Restricted Committee** observes that the on-site inspection shows that the company had retained 2,394,538 lines relating to user accounts more than 5 years old from the date of the last login and less than 10 years old, and 737,563 lines relating to user accounts more than 10 years old from the date of the last login.

32. T**he Restricted Committee** notes that it follows from the above that when the retention period is reached, personal data must be deleted. It thus emerges from the documents in the case file that as of the date of the on-site inspection, the company was retaining user account data beyond the time period required in view of the stated purpose.

33. **Consequently**, the Restricted Committee is of the view that the above acts constitute a breach of Article 5-1-e) of the GDPR. The Restricted Committee notes that during the procedure, the company partially complied with the application of an appropriate retention period for user account data with regard to the various purposes pursued by deleting data relating to such accounts that have been inactive for more than 5 years. It nevertheless points out that this compliance does not exempt the company from its liability for its past actions.

C. On the breach of the obligation to inform individuals

34. Article 13 of the Regulation details the information to be provided to the data subject in cases where the personal data are collected directly from him/her. Such information shall include the identity of the data controller and his/her contact details, the purposes of the processing carried out, its legal basis, the recipients or categories of recipients of the data, and whether the data controller intends to transfer data to a third country. The article also requires the data controller, where it appears necessary to ensure "fair and transparent processing" of personal data in this case, to inform individuals about the period of data retention, the existence of the various rights enjoyed by individuals, the existence of the right to withdraw consent at any time, and the right to lodge a complaint with a supervisory authority.

35. In her report, **the rapporteur** notes in substance that the information provided by the company on the [redacted] website, through its "personal data protection policy" page, was incomplete or imprecise, failing to specify the processing to which the legal bases relate, the recipients or categories of data recipients, the right to lodge a complaint with the CNIL, and the retention periods defined by the company. The rapporteur notes, however, that the company has, since the inspections, engaged in a compliance process, although this does not excuse past failures.

36. **In its defence,** the company disputes the breach; it is of the view that it has merely provided the information inaccurately. It states that since the inspections, it has complied by amending and adding to its personal data protection policy. With regard to the legal bases applicable to processing, the company refers to a clumsy presentation. With regard to the mention of the recipients or categories of recipients, it is of the view that it was not required to provide the identity of all the data recipients.

37. **The Restricted Committee** notes that it emerges from the findings made during the inspection that with regard to the website [redacted], a personal data protection policy was accessible via the bottom of the home page, a document to which the user account creation form also referred. However, it appears that although the legal bases were stated, no explanation was given as to the processing to which they related.

38. In addition, the Restricted Committee notes, as does the rapporteur, that the company gave the name of only one of its processors, [redacted], which is in charge of payments made on the site. Apart from this example, no information was provided with regard to the other recipients or categories of recipients of the personal data. Yet the Restricted Committee notes that the inspection reveals that the company had at least two other processors receiving personal data.

39. Therefore, the Restricted Committee is of the view that the company has failed to comply with the provisions of Article 13 (1) of the GDPR.

40. Secondly, the Restricted Committee notes (a) that this personal data protection policy did not mention the right to lodge a complaint with the CNIL, and (b) that the stated retention periods were inaccurate.

41. The Restricted Committee is of the view that this information is important to ensure fair and transparent processing, since it helps to ensure that users have control over the processing of their data.

42. The Restricted Committee is of the view that the absence of mention of the right to lodge a complaint with the CNIL and the inaccuracy of the information relating to the retention period of user data in the company's privacy policy, constitute a breach of Article 13 (2) of the GDPR.

43. Consequently, **the Restricted Committee** is of the view that the company has committed a breach of Article 13 of the GDPR. It states that the breach under consideration is the one which became apparent at the time of the inspections, and notes that the company has since worked to achieve compliance.

D. Regarding the breach related to the obligation to apply a legal framework to the processing carried out on behalf of the data controller

44. Pursuant to Article 28(3) of the Regulation, the processing operations carried out by a processor on behalf of a controller are governed by a contract or other legal act that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. This contract also provides for the conditions under which the processor undertakes to carry out the processing operations on behalf of the data controller.

45. **The rapporteur** noted that the contractual documents for [redacted], [redacted] and [redacted], the company's processors, did not contain all the information provided for in the aforementioned article.

46. **In its defence**, the company disputes the breach with regard to the contractual relationship with [redacted]. In this respect, it specifies that the latter is governed by a contract which refers to a data processing agreement, which contains the information required by Article 28. With regard to the contract entered into with [redacted], the company states that it entered into an amendment to the contract containing the information provided for in Article 28. Lastly, the company declares that it has terminated the contractual relationship with [redacted].

47. **The Restricted Committee** notes that with regard to the [redacted] contractual documents, the company had provided the CNIL delegation with the only contract entered into on 19 November 2021. Subsequently, in response to the sanction report, it provided the data processing agreement referred to in the contract. The Restricted Committee is of the view that these contractual documents, when read as a whole, contain all the necessary information. A breach has therefore not been established for this contractual relationship.

48. With regard to the contract entered into with [redacted], the Restricted Committee notes that the amendment produced by the company in response to the sanction report was entered into on 7 September 2023. The Restricted Committee notes that this amendment contains all the required information, but is of the view that evidence of the breach has been shown for the past

with regard to the date of signature of the said amendment. Indeed, the restricted committee considers that the retroactive nature of the amendment relied on by the company cannot cover the past breach insofar as, at the time of the investigations, the contract concluded did not contain the required information.

49. Finally, with regard to the contract concluded with company [redacted], the restricted committee considers that, in view of the documents produced, it has not been established that this company processed personal data on behalf of the company [redacted] and was a processor within the meaning of the GDPR. Accordingly, the breach of Article 28 cannot be established.

50. For these reasons, the Restricted Committee is of the view that evidence of the breach of Article 28(3) of the GDPR has been established for past actions with regard to the contract governing relations with [redacted].

E. On the breaches of the obligation to ensure data security

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

a) the pseudonymisation and encryption of personal data;
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
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."*

1. <u>Regarding passwords and private references</u>

52. **The rapporteur** noted that, firstly, during the online inspection, the delegation had noted that when creating a user account on the company's website, passwords of a single character (one number or one letter) were accepted and that no access restriction in the event of authentication failure was implemented. In addition, the rapporteur noted that, during the inspections, each password was both stored in plain text and hashed using the Bcrypt hash algorithm.

53. Secondly, the rapporteur noted that, during the on-site inspection, the delegation was informed that users without accounts who submitted advertisements were provided with a clear private reference consisting of ten alphanumeric characters, the first seven of which were public in that they matched the characters contained in the advertisement reference filed on the website. This private reference could not be changed by the advertiser. This reference on its own was sufficient for the user to directly access the advertisement and the associated space on the site after entering it in the corresponding field. Furthermore, this private reference, which works like a password, was stored in plain text in the database.

54. **In its defence,** the company does not contest the substance of the breaches, but states that it has taken corrective actions. First of all, it announces that it has changed its password policy by

requiring passwords of a length of eight characters consisting of at least one upper case letter, one lower case letter, one number and one special character. It points out that passwords are now hashed using the Bcrypt algorithm, and that passwords that had been stored in plain-text form have been deleted. The company goes on to state that it no longer provides private references to users requiring the creation of an account on the site, and that it has implemented a system for locking the proprietary space after ten unsuccessful login attempts.

55. **Firstly, the Restricted Committee** points out that it follows from the provisions of Article 32 of the GDPR that the data controller is required to ensure that the automated data processing it implements is sufficiently secure. The sufficiency of the security measures is assessed (a) with regard to the characteristics of the processing and the risks it entails, and (b) with consideration of the state of knowledge and the cost of the measures.

56. The Restricted Committee is of the view, firstly, that excessively permissive password complexity rules, which enable the use of insufficiently robust passwords, may lead to attacks by unauthorised third parties, such as "brute force" or "dictionary" attacks, which consist of successively and systematically testing many passwords and thus lead to a compromise of the associated accounts and the personal data they contain.

57. It notes, in this respect, that the need for a strong password is recommended both by the French National Agency for Information Systems Security (ANSSI) and by the Commission in its deliberation no. 2017-012 of 19 January 2017 adopting a recommendation relating to passwords, a requirement that it confirmed in its deliberation no. 2022-100 of 21 July 2022.

58. By way of illustration, the Restricted Committee points out that the Commission, in its deliberation no. 2017-012 of 19 January 2017 – which, while it does not have the power to compel, does provide relevant clarification on the measures to be taken in terms of security – is of the view that, in order to ensure a sufficient level of security and confidentiality, in the event that authentication is based solely on a username and a password, the password must be composed of at least twelve characters including upper case letters, lower case letters, numbers and special characters.

59. Failing this, the Commission is of the view that a sufficient level of security and privacy is also provided by authentication based on a password with a minimum length of eight characters, consisting of three different categories of characters but accompanied by an additional measure such as, for example, the time-out of access to the account after several failures (temporary prevention of access, the duration of which increases as attempts are made), the establishment of a mechanism to protect against automated intensive submissions of attempts (e.g. "captcha") and/or the locking of the account after several (up to ten) unsuccessful authentication attempts.

60. The Restricted Committee emphasises that it has, on several occasions, implemented financial penalties in cases where its finding of a breach of Article 32 of the GDPR has been the result of insufficient measures to guarantee the security of the data processed. Deliberations no. SAN-2019-006 of 13 June 2019, no. SAN-2019-007 of 18 July 2019 and no. SAN-2022-018 of 8 September 2022 focused in particular on insufficiently robust passwords.

61. **The Restricted Committee** notes that in this case, firstly, the passwords of users of the website [redacted] were, at the time of the inspections, required to be composed of a single character, without any additional security measures. It emerges from the company's observations that the

required passwords are now 8 characters long and consisting of at least one upper case letter, one lower case letter, one number and one special character without any access restriction being provided. Secondly, the private references – equivalent to passwords within the meaning of the definition of deliberation no. 2022-100 of 21 July 2022, according to which the term "password" refers to any knowledge-based factor, namely any set of revocable information, known only to the person concerned and enabling or contributing to the authentication of that person – consisted of ten alphanumeric characters, the first seven of which were public, in that they corresponded to the reference code for the advertisement on the website, with only the last three characters private. In addition, these references were sent in plain text and could not be modified by the user, and thus constituted a permanent means of authentication.

62. The Restricted Committee is of the view that such constructions do not ensure the security of the data or prevent unauthorised third parties from having access to it.

63. With regard to the passwords required when creating an account, it pointed out, as did the rapporteur, that on the day of the on-site inspection, the company was processing the data associated with nearly five million user accounts, including surname, first name and email address. This means that these passwords, associated with their usernames, provide access to all the personal data contained in their [redacted] accounts. They were not robust enough, with regard to the personal data in question and the state of the art.

64. With regard to the private reference, the Restricted Committee is of the view that the use of this reference alone, which consisted of ten alphanumeric characters, did not meet the criterion of sufficient complexity. Indeed, it appears that the initial part of this reference – the first seven alphanumeric characters representing the advertisement reference number – is effectively a public identifier. As for the second part of the reference – comprising the last three alphanumeric characters, which is similar to a password – it does not meet the robustness criteria as described above.

65. In addition, as the rapporteur pointed out, this private reference provides access to the personal data in the owner space associated with the person who published the advertisement, making it possible to modify that data, and also to modify the advertisement. In addition, access to this space enables access to the interactions between the owner and the individuals interested in the advertisement, during which a large amount of personal information may be transmitted (family, professional, financial situations).

66. Also, authentication that is based on the use of (a) a password, which was previously short and lacking any additional security measures, and is still insufficiently robust in the absence of additional security measures, and (b) a non-modifiable private reference, transmitted in plain text and lacking sufficient complexity, can lead to attacks by unauthorised third parties and thus to a compromise of user accounts and "proprietary spaces" and the large amount of personal data they contain.

67. For this reason, the Restricted Committee is of the view that the implemented password or private reference policy was, and remains, insufficiently robust to guarantee the security of the data being processed, which is a breach of Article 32 of the GDPR.

68. **Secondly**, the Restricted Committee points out that the secure retention of passwords constitutes an elementary precaution in the protection of personal data. In 2013, the ANSSI issued an alert and reminder of good practices regarding the retention of passwords, stating that

they must "be stored in a form that has been transformed by a one-way cryptographic function (hash function) and is slow to calculate, such as PBKDF2" and that "the transformation of passwords must involve a random salt to prevent an attack using precomputed tables" (ANSSI, "Bulletin d'actualité CERTA-2013-ACT-046", 15 November 2013, https://www.cert.ssi.gouv.fr/actualite/CERTA-2013-ACT-046/).

69. Similarly, in its deliberation no. 2017-012 of 19 January 2017, the CNIL had already stated that it "recommends [that the password] be transformed by means of a non-reversible and secure cryptographic function (i.e. using a known-strong public algorithm whose software implementation is free from any known vulnerability), incorporating the use of a salt or a key". Indeed, non-robust hash functions present known vulnerabilities that do not guarantee the integrity and confidentiality of passwords in the event of a brute force attack once the servers that host them have been compromised.

70. **In this case,** the Restricted Committee notes that the plain-text storage of (a) user passwords, associated with their identifiers and email addresses, and (b) private references, associated with a personal space, is not sufficient to guarantee their security. This retention method implies that anyone with access to the company's customer database – whether an administrator of the company's information systems or an attacker in the event of a compromise – can view, collect, modify or sell them.

71. For this reason, the Restricted Committee is of the view that the procedures for storing passwords and private references did not, as of the date of the findings, guarantee the security and privacy of the personal data of the holders of user accounts, which is in breach of Article 32 of the GDPR.

72. **Consequently**, the Restricted Committee is of the view that the aforementioned actions, which are not disputed by the company, constitute breaches of the obligations under Article 32 of the GDPR. It notes that since the inspections, the company has partially remedied the breaches observed by implementing a password policy that offers an adequate level of security, and by encrypting all passwords.

2. <u>On the retention of data in an active database</u>

73. **The rapporteur** noted that during the inspections, the delegation was informed that all data relating to inactive customers was kept for ten years, and data relating to inactive user accounts for five years, in an active database without intermediate archiving.

74. **In its defence**, the company disputes that any breach occurred. First, it argues that this active database retention of the data of customers and users who have become inactive is justified for anti-fraud reasons, requiring daily checks. Secondly, it states that only persons who have an interest in processing the data due to their functions can access the personal data; that is to say, customer service advisors, employees of the IT departments, and members of management staff. In this respect, it adds that these employees are subject to a confidentiality clause and a confidentiality undertaking, and that each of them has a personal password.

75. **The Restricted Committee points out** that in order to ensure data security, it is necessary for this data to be sorted once it is no longer necessary for the purpose for which it was

collected. This means that it must be deleted, or be archived on an intermediary basis; this process involves a physical or logical separation.

76. In this case, the Restricted Committee notes that it emerged from the explanations provided by the company that while the purpose of combating fraud may justify data retention, the methods of data retention in the active database as defined by the company do not ensure data security. On the one hand, the Restricted Committee notes the large number of categories of employees with access to the database, insofar as customer service advisors, IT department employees and members of the management team are all authorised to access the database. Secondly, it noted the absence of any sorting of the data stored, even though it appears that storing data such as the advert and billing address is not necessary to achieve the objective of combating fraud. Indeed, the company confirmed during the session that the data used to identify fraudsters was the e-mail address.

77. **Consequently**, the Restricted Committee is of the view that a breach is established.

F. Regarding the breach of the obligation to provide information and the right to object to commercial prospecting by email for similar products or services

78. Article L. 34-5 of the French Post and Electronic Communications Code (CPCE) provides that *"Direct prospecting by means of an automated electronic communications system […], a fax machine or emails, using the contact details of a natural person […] who has not previously expressed his/her consent to receive direct prospecting by this means, is prohibited.*
Direct prospecting is the sending of any message that is directly or indirectly intended to promote goods, services or the image of a person selling goods or providing services. For the purposes of this article, calls and messages whose purpose is to encourage users or subscribers to call a premium rate number or to send premium rate text messages also fall within the scope of direct marketing.
However, direct prospecting by e-mail is permitted if the contact details of the recipient have been collected from them, in compliance with the provisions of Act no. 78-17 of 6 January 1978 relating to data processing, files and freedoms, at the time of a sale or provision of services, if the direct prospecting action concerns similar products or services provided by the same natural or legal person, and if the recipient is expressly and unambiguously offered the option to object, free of charge, other than charges related to the sending of the objection, and in a simple manner, to the use of his/her contact details at the time they are collected and each time a prospecting email is sent to him/her in the event that he/she has not refused such exploitation from the outset."

79. These provisions transpose into French law the rules governing the use of automated call and communication systems without human intervention (automated call systems), fax machines or electronic mail systems for direct marketing purposes set out in Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on the processing of personal data and the protection of privacy in the electronic communications sector (known as the "ePrivacy" directive), as amended by Directive 2009/136/EC of 25 November 2009.

80. **The rapporteur** noted that when a user subscribes to an alert with regard to real estate, they are likely to receive emails for similar goods or services by the company, having neither

been notified nor being given the opportunity to object to this, at the time when the alert was created.

81. **In its defence,** the company disputes the breach by asserting that the disputed emails do not constitute commercial prospecting since their purpose is not to promote goods or services. Furthermore, it points out the low volume of this type of message and specifies that users have the option of unsubscribing via an unsubscribe link that is found in each new communication.

82. **The Restricted Committee** points out that within the meaning of Article 34-5 of the CPCE, firstly, direct commercial prospecting is defined as *"any message intended for the direct or indirect promotion of goods, services or the image of a person selling goods or providing services"*. Secondly, similar products and services, offered at the time of a sale or provision of services, must be understood as promoting goods or services of the same natural or legal person without any requirement for the promotion to result in a financial transaction with the person.

83. The Restricted Committee considers that the emails sent by the company to users, such as the ones containing information concerning an advertisement or anonymous surveys on [redacted] are a direct result of subscribing to a property alert and are not intended to promote other goods or services offered by the company. Therefore, these e-mails do not constitute commercial canvassing within the meaning of article L.34-5 of the CPCE.

84. In these circumstances, the restricted committee considers that the breach of Article L.34-5 of the CPCE is not established.

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

85. Pursuant to Article 20(III) of the Act of 6 January 1978 as amended:

"*In cases where the data controller or its processor fails to comply with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or from this Act, the Chairman of the French Data Protection Authority may also, where applicable after having sent it the warning provided for in section I of this article or, where applicable in addition to a formal notice provided for in section II, refer the matter to the Restricted Committee of the authority with a view to issuing, after adversarial proceedings, one or more of the following sanctions: […] 7° With the exception of cases where the processing is implemented by the State, an administrative fine of not more than €10 million or, in the case of a company, 2% of the total global annual turnover of the previous financial year, whichever is higher. In the cases mentioned in sections 5 and 6 of Article 83 of Regulation (EU) 2016/679 of 27 April 2016, these ceilings are increased, respectively, to €20 million and 4% of said turnover. The Restricted Committee shall, in determining the amount of the fine, take into account the criteria specified in the same Article 83."*

86. Article 83 of the GDPR provides that "*Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article […] shall in each individual case be effective, proportionate and dissuasive*", before specifying the elements to be taken into account in deciding whether an administrative fine should be imposed and in deciding the amount of this fine.

A. Regarding the imposition of an administrative fine and its value

1. Regarding the imposition of an administrative fine

87. **In its defence**, the company maintains that the proposed administrative fine is disproportionate to the alleged breaches and its conduct since it implemented several corrective measures before the end of the investigation, including a change to its confidentiality policy in order to provide the required information, the use of processors governed by a legal act containing all the required information, the implementation of a password policy and storage with an adequate level of security. In addition, it stresses that it has fully cooperated with the CNIL. It adds that it did not derive any financial benefit from the alleged breaches. It argues that its turnover is stagnating, and that the highly competitive [redacted] sector is in crisis. Lastly, it is of the view that the fine of €250,000 proposed by the rapporteur is equivalent to [redacted]% of its 2023 turnover, and is therefore excessive.

88. **The Restricted Committee points out** that, for the imposition of an administrative fine, it must take into account the criteria specified in Article 83 of the GDPR, such as the nature, severity and duration of the breach, the scope or purpose of the processing concerned, the number of persons affected, the measures taken by the controller to mitigate the damage suffered by the data subjects, the fact that the breach was committed by negligence, the degree of cooperation with the supervisory authority and, in certain cases, the level of damage suffered by the persons concerned.

89. The Restricted Committee notes, firstly, that the alleged breaches by the company infringe fundamental principles provided for by the GDPR and relate to many people.

90. With regard to the breach of the principle of limiting the retention period for personal data, the company was negligent (a) by not adequately defining a retention period for data of customers who entered into a contract of less than €120, and (b) by not applying the retention period that it had specified for data relating to users on the day of the inspections. The Restricted Committee notes that this breach relates to a significant number of people, with the company counting 2,394,538 users whose last login to their account was between 5 and 10 years previously as of the date of the inspections.

91. With regard to the breach of the obligation to inform data subjects and of transparency, the Restricted Committee notes that the company failed to comply with the requirement to provide complete and transparent information to data subjects, which is an essential prerequisite for any processing of personal data.

92. With regard to the breach of the obligation to regulate the processing carried out on behalf of the data controller by means of a formalised legal act, the Restricted Committee notes that the company failed to ensure that it subscribed to contractual document containing the information required by Article 28 of the GDPR, thus depriving the data subjects of full protection of their personal data.

93. With regard to the breach of the obligation to ensure the security of personal data, the Restricted Committee points out the number of observed breaches of basic security obligations; namely, the use of an insufficiently robust password and private reference for

customer or user accounts, the unencrypted transmission of the private reference, and the unencrypted storage of passwords and private references. The Restricted Committee is of the view that the accumulation of these security flaws denied individuals the benefit of the full protection provided for by the GDPR with regard to the use of their data.

94. Finally, while taking account of the fact that the company has put in place measures following the notification of the sanction report, the Restricted Committee notes that these actions do not exempt the company from its liability for breaches which occurred in the past.

95. **Consequently,** the Restricted Committee is of the view that an administrative fine should be imposed for breaches of Articles 5-1-e), 13, 28 and 32 of the GDPR.

2. Regarding the amount of the administrative fine

96. The Restricted Committee first notes that breaches of Articles 5-1-e) and 13 of the GDPR constitute breaches of key principles of the GDPR that may be subject, under Article 83 of the GDPR, to an administrative fine of up to €20,000,000 or up to 4% of annual turnover, whichever is higher.

97. Next, the Restricted Committee points out that in 2022, the company generated revenue of approximately €[redacted] million and net income of €[redacted].

98. **Therefore**, with regard to the company's liability, its financial capacity and the relevant criteria of Article 83 of the Regulation, the Restricted Committee is of the view that an administrative fine of a total amount of 100,000 (a hundred thousand) euros, for breaches of Articles 5-1-e), 13, 28 and 32 of the GDPR appears justified.

B. Regarding publication

99. The Restricted Committee is of the view that the publication of this decision is justified in view of the seriousness of the breaches in question and the number of persons involved. It is also of the view that the publication of the sanction will, for example, make it possible to inform all the persons concerned by the breaches.

100. Finally, the measure is proportionate given that the decision will cease to identify the company by name upon expiry of a period of two years from its publication.

CONSEQUENTLY

The Restricted Committee of the CNIL, after deliberation, decided to:

- **impose an administrative fine on [redacted] to the value of:**
- **a hundred thousand (100,000) euros for breaches of Articles 5-1-e), 13, 28 and 32 of Regulation (EU) no. 2016/679 of 27 April 2016 on data protection;**

- **make public, on the CNIL website and on the Légifrance website, its deliberation, which will cease to identify the company by name upon expiry of a period of two years from its publication.**

The Chair

[redacted]

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