**Deliberation of restricted committee no. SAN-2021-001 of 6 January 2021 concerning [redacted]**

The *Commission nationale de l'Informatique et des Libertés* (CNIL - French Data Protection Authority), met in its restricted committee composed of Alexandre LINDEN, chairman, and Anne DEBET, Sylvie LEMMET and Christine MAUGÜE, members;

Having regard to Council of Europe Convention No. 108 of 28 January 1981 for the protection of persons with regard to the automated processing of personal data;

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

Having regard to amended French Data Protection Act no. 78-17 of 6 January 1978, in particular articles 20 *et seq.*;

Having regard to decree no. 2019-536 of 29 May 2019 implementing law no. 78-17 of 6 January 1978 on data protection;

Having regard to deliberation no. 2013-175 of 4 July 2013 adopting the rules of procedure of the CNIL (French Data Protection Authority);

Having regard to decision no. 2019-42C of 15 February 2019 of CNIL's chair to instruct the general secretary to carry out or have a third party carry out an assignment to verify the processing implemented by that organisation or on behalf of [redacted];

Having regard to the decision of CNIL's chair appointing a rapporteur before the restricted committee of 27 January 2020;

Having regard to referral PL19000723 received by the CNIL on 9 January 2019;

Having regard to the report of [redacted], the commissioner rapporteur, notified to [redacted] on 24 February 2020;

Having regard to the written observations made by [redacted] on 23 March 2020;

Having regard to Order no. 2020-306 of 25 March 2020 on the extension of the deadlines due during the health emergency period;

Having regard to the rapporteur's response to these observations notified on 22 April 2020 to the company's board;

Having regard to the written observations of [redacted] received on 20 August 2020 and the oral observations made at the restricted committee meeting;

Having regard to the other documents in the file;

At the restricted committee meeting of 10 September 2020, which was partially held by videoconference the following were present:

- [redacted], commissioner, heard in his report;

In the capacity of representatives of [redacted]:

- [redacted], lawyer at the Paris Bar;
- [redacted], [redacted]( by video conference);

As a representative of [redacted]:

- [redacted] (by video conference);

[redacted] having last spoken;

The restricted committee adopted the following final decision:

## I- Facts and proceedings

1. [redacted] (hereinafter " the company ") is a simplified joint-stock company founded in France in [redacted], specialising in optical retail trade and whose registered office is located at [redacted]. For this purpose, it has around 100 branches, mostly located on French territory, as well as a network of approximately 450 franchise stores worldwide.

2. In 2017, [redacted] achieved a turnover of [redacted] and more than [redacted] in profits.

3. The company also publishes, for the purposes of its activity, the [redacted] (hereinafter the "company website"), which allows its customers to make online orders. Other variations in this site target consumers in Germany ([redacted]), Spain ([redacted]) and the United Kingdom ([redacted]).

4. On 4 January 2019, the company sent to the French Data Protection Authority (hereinafter the "CNIL" or the "Authority") a notification relating to an "*attack on the Internet sales website of* [redacted] *by a hacker*" which resulted in a "*probable intrusion on the servers hosting the site"*.

5. In a letter supplementing the notification sent to CNIL on 11 January 2019, the company indicated that the intrusion had compromised the personal data of 210,692 customers. After analysis, it was established that the customers of the company concerned are mainly French but also include European nationals and third-country nationals. The personal data displayed on this occasion are the email address, hash of the user account's password, the first and last names, address, telephone number, date of birth of the data subjects and, for 23,000 of them, the social security number.

6. On 19 February 2019, pursuant to CNIL chair's decision no. 2019-42C, a CNIL delegation carried out an audit at the premises of [redacted]. The purpose of this audit was to verify compliance by this 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 law no. 78-17 of 6 January 1978 on data protection (hereinafter "the amended law of 6 January 1978" or "the French Data Protection Act") by examining in particular the circumstances of the aforementioned personal data breach.

7. During this audit, the delegation was informed that the website [redacted] is published by [redacted], but that its development, administration and security had been carried out since 2013 by a provider, [redacted], established in Israel.

8. With regard to the unfolding of the personal data breach, the delegation was informed, in particular, that on 26 December 2018, attackers had exploited a vulnerability affecting the jQuery-File-Upload module that the company is deploying on its website to enable the uploading of its customers' orders to their user account. The exploitation of the vulnerability of this module allowed attackers to place files on the web server containing the tools necessary to extract personal data from this server. On 27 December 2018 and on 2 January 2019, [redacted] detected abnormal files on the web server, which it deleted the same day.

9. On 3 January 2019, after discovering a new intrusion into the servers of the website, [redacted] informed the controller of the situation. In order to permanently cut off the attack, the two companies decided to use [redacted], specialising in information systems security auditing, which sent them its intervention report on 10 January 2019.

10. Following these events,[redacted] and [redacted] took various measures to put an end to the attack and avoid it being repeated. Both companies implemented the recommendations made by [redacted], such as updating the vulnerable module with the latest available version, removing unnecessary or compromised files and folders at the root of the site, changing the SSH key, i.e. the secure communication protocol used to connect to the web server, and strengthening the security measures governing the connection of a customer to its user account.

11. On 29 April 2019, a CNIL delegation carried out an online audit on the [redacted] website, in order to verify the compliance of the processing of personal data implemented by [redacted] and in particular the aforementioned website.

12. On 27 and 28 May 2019, an auditing delegation arrived at the premises of the company's registered office. This second on-site audit, which was part of the investigation of several complaints from customers or prospects of the company received by CNIL, particularly concerned commercial prospecting and the exercise of personal rights.

13. In emails received between March and September 2019, the company sent the CNIL various documents requested by the delegation as part of these three audits, such as the contractual documents binding the company to several of its service providers, including [redacted], as well as the company's exchanges with the customers responsible for the complaints received by the Authority. The company also provided CNIL, by email dated 15 November 2019, with the new "*Personal Data Charter*" posted on its website.

14. In order to examine these items, the chair of the Authority appointed [redacted] as rapporteur, on 27 January 2020, on the basis of Article 22 of the amended law of 6 January 1978.

15. In accordance with Article 56 of the GDPR, on 18 February 2020 the CNIL informed all European supervisory authorities of its competence to act as the lead supervisory authority concerning the cross-border processing carried out by the company and opening the procedure for the declaration to the relevant authorities in this case.

16. At the end of his investigation, the rapporteur had a bailiff notify [redacted], on 24 February 2020, of a report detailing the breaches of the GDPR that he considered constituted in this case.

17. This report proposed to the Authority's restricted committee to pronounce an injunction to bring the processing into line with the provisions of Article 12(2) and Article 32 of the Regulation, accompanied by a penalty at the end of a period of three months following notification of the decision of the restricted committee, as well as an administrative fine.

18. Also attached to the report was a notice to attend the restricted committee meeting on 30 April 2020 indicating to the company that it had one month to provide its written observations in response to the report.

19. On 4 March 2020, the company made a request for the restricted committee meeting to be held behind closed doors.

20. In a letter dated 10 March 2020, the chairman of CNIL's restricted committee responded favourably to this request, on the grounds that certain items submitted to the proceedings were protected by business secrecy, as provided for in Article L 151-1 of the French Commercial Code.

21. On 10 March 2020, the company's counsel sent CNIL's chairman a request to challenge the rapporteur appointed pursuant to Article 39 of Decree no. 2019-536 of 29 May 2019, on the grounds that he would be biased against the company and its representatives.

22. In a letter in response dated 20 April 2020, the CNIL chairman rejected the request after having pointed out in particular that the request was unfounded and that the documents communicated did not establish the existence of bias by the rapporteur against the company and its representatives.

23. On 23 March 2020, the company submitted observations in response to the report.

24. In an email dated 24 March 2020 and on the basis of Article 40, paragraph 4, of Decree no. 2019-536 of 29 May 2019, the rapporteur asked the chairman of the restricted committee for an additional period of fifteen days to respond to the company's observations.

25. In a letter dated 25 March 2020, taking note of the context of the health crisis, the chairman of the restricted committee granted this request.

26. In a letter dated the same day, the company was informed of the additional period granted to the rapporteur and the fact that it had, pursuant to paragraph 5 of article 40 of decree no. 2019-536 of 29 May 2019, a period of one month to respond to the rapporteur's response. The letter also informed it of the postponement of the restricted committee meeting, initially scheduled for 30 April 2020.

27. On 22 April 2020, the rapporteur notified his response to the company's observations.

28. In a letter dated the same day, CNIL's general secretary informed the company that it could submit its observations to the rapporteur's response until 24 August 2020 pursuant to Order no. 2020-306 of 25 March 2020 on the extension of the deadlines due during the health emergency period.

29. On 11 August 2020, CNIL services notified the company of a notice to attend the restricted committee meeting on 10 September 2020.

30. On 20 August 2020, the company submitted further observations in response to those of the rapporteur.

31. The company and the rapporteur presented oral observations at the restricted committee meeting.

## II- Reasons for the final decision

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

33. In this case, the restricted committee firstly stated that [redacted] was founded in France in [redacted] and that since that date it has had a registered office in Paris.

34. The restricted committee then noted that this head office, which employs approximately 50 employees, is organised into seven divisions, including a marketing division, a sales division, as well as an IT and development division.

35. Lastly, although the company has several franchise stores worldwide as well as around 100 branches, three of which are located in Spain, the restricted committee noted that these different establishments are only distribution points of the company's products.

36. As a result, [redacted] is the sole establishment of the company in the European Union and that CNIL is competent to act as the lead supervisory authority concerning the cross-border processing carried out by this company, in accordance with Article 56(1) of the Regulation.

37. In accordance with the cooperation and consistency mechanism provided for in Chapter VII of the GPDR, the supervisory authorities of the following countries declared themselves affected by this procedure: Germany (Rhineland-Palatinate, Lower Saxony, Berlin, Bavaria), Belgium, United Kingdom, Spain and Luxembourg.

38. The draft decision adopted by the restricted committee was sent to these supervisory authorities on 3 December 2020, pursuant to Article 60(4) of the GDPR.

39. The restricted committee notes that on 1st January 2021, none of the supervisory authorities concerned had raised any relevant and reasoned objection to the draft decision submitted to them, so that they are deemed to have approved it, in accordance with Article 60(6) of the GDPR.

### A. Failure to comply with the arrangements for the exercise of the rights of persons (Article 12(2) of the GDPR)

40. According to Article 12(2) of the Regulation, "*the controller facilitates the exercise of the rights conferred on the data subject under Articles 15 to 22 of the Regulation*".

41. **Firstly**, it appears from referral no. [redacted] that, on 6 November 2018, a prospect of the company attempted to exercise his right to object to the latter by using the email addresses intended to exercise rights, indicated on the "*Personal Data Charter*" page of the company's website. The defective nature of these addresses was actually noted by the CNIL delegation during the online audit of 29 April 2019. This malfunction was definitively repaired by the company in May 2019, as was noted during the on-site inspection of 27 and 28 May.

42. The rapporteur argued that, in general, the defective nature of these email addresses has hindered the exercise of the rights of persons. In addition, he noted, in particular, that the company has never granted the request for opposition made by the complainant at the origin of referral no. [redacted].

43. In defence, the company argued that this malfunction is due to a simple technical error. It also recalled that after having noted that the electronic addresses had been incorrectly transcribed on its site - the addresses mentioned with a first level domain name in "*.fr*" instead of "*.com*" - it restored the correct version on 13 November 2018. It pointed out in this respect that it was only in a second step, upon receipt of the online inspection report of 29 April 2019, that it became aware that this first correction was not sufficient. In fact, the "*mailto*" field of the hyperlink which allows, when clicking on it, to generate an email directly with the address of the pre-filled recipient, continued to generate emails for "*personaldata.fr*" instead of

"*personaldata.com*". For this reason, the actual recovery of these addresses did not occur until May 2019.

44. The company indicated that, in any event, before that date the data subjects could always exercise their rights through the other channels made available to them, for example by sending a letter to the registered office or using the online form dedicated to the exercise of rights.

45. The restricted committee acknowledged that the succession of technical errors made by the company makes it possible to explain in part its delay in restoring the email addresses intended to exercise rights, but it pointed out, firstly, that these explanations do not justify the company's negligence in this matter, more than six months having elapsed between the finding of the defective nature of these addresses and their full repair. Furthermore, the restricted committee again noted that the company only corrected these addresses following the intervention of CNIL delegations.

46. The restricted committee then noted that although, for these six months, the data subjects could always exercise their "data protection" rights through other channels, the simple fact of providing people with a channel that proves to be defective necessarily complicated the exercise of these rights, especially if this channel were supposed to be the simplest to use. In this case, in order to be able to exercise their rights and ensure that their request had been sent, the data subjects had to undertake a new procedure using one of the other channels made available to them by the company when they received an error message informing them of the failure to provide their email, due to the defective "mailto" field.

47. As a result, the restricted committee held that the prolonged defect in these email addresses did not facilitate the exercise of the rights of persons.

48. Lastly, the restricted committee noted that at the date of the hearing, the company had not provided any evidence that it had granted the request for opposition made by the plaintiff at the origin of referral no. [redacted].

49. **Secondly**, the restricted committee noted that the checks carried out on 27 and 28 May 2019 were, in particular, intended to investigate several complaints from prospects of the company arguing that they were unable to validly exercise their right of access.

50. The declarations made by the company's representatives in the framework of these audits revealed that, in order to promote its business, the latter conducts, each year, between five and six commercial prospecting campaigns by post and that each of these campaigns represents an approximate volume of 9 million envelopes sent. For each of these campaigns, the company prepares specifications to define, over a period of one to two months, the very concrete terms of the upcoming campaign. These specifications are sent to various service providers of the company, including [redacted], which provides the file of persons to be prospected.

51. Therefore, since it determines the purpose and means of the prospecting processing by post, [redacted] has the capacity of controller for this processing, while [redacted], which acts in this respect on behalf of the former, has the capacity of processor, within the meaning of the Regulation.

52. The findings have made it possible to establish that, when a person who has been the subject of one of these commercial prospecting campaigns by post attempts to exercise his right of access to the "*store customer service*" of [redacted], the latter simply informs it that it does not process its personal data and sends them to [redacted] as follows: "*we use a mailing company without having access to personal data, we do not have any more information about you. If you wish to have more details about this, you can write to* [redacted]".

53. The rapporteur argued that the terms of the right of access procedure described above do not facilitate the exercise of the rights of data subjects contrary to the provisions of Article 12 of the GDPR.

54. In defence, the company first argued that it fully complies with the requirements of section 12 of the Regulation by ensuring the effective implementation of the rights of persons. It has therefore deployed numerous information media to ensure that all data subjects are informed of their rights and can exercise them through the procedures it has implemented, such as the procedure for requesting the deletion of accounts and/or personal data or the "stop pub" service that its customer service did not hesitate to highlight.

55. The company then argued that it is not responsible for managing a prospect's file belonging to its processor, [redacted]. It pointed out that it does not have the means to act on this file, it cannot ensure the effectiveness of the rights of persons in the name and on behalf of that company.

56. The restricted committee noted, first of all, that although [redacted] uses a processor in the context of its prospecting operations, it is responsible for the processing carried out and, as such, remains accountable for the obligations associated with this status, particularly those related to compliance with the rights of the data subjects.

57. It then pointed out that the access right procedure implemented for prospects by post necessarily forces prospects who have made a request for a right of access to it to initiate a second step with [redacted] to exercise their right. Thus, even if the prospect's right of access request is ultimately successful, this two-step process necessarily extends the processing time. This operational choice has a structural effect that can affect a considerable number of people, with [redacted] sending on average over forty-five million mail solicitations for [redacted] campaigns.

58. Consequently, the restricted committee considered that in view of the constraints that the right of access procedure places on prospective customers who receive solicitations by post, and

independently of the various information media and procedures put forward by the company, the company does not facilitate the exercise of these people's rights.

59. **Thirdly**, the company claimed to have been the subject of only five complaints.

60. The restricted committee recalled, first of all, in general, that any person encountering difficulties in exercising their rights does not refer the matter to the CNIL, so that the number of complainants cannot be fully representative of the number of people affected by a breach.

61. It then noted that while the number of complaints to CNIL concerning the difficulties encountered in exercising rights with the company is low, the findings made have demonstrated that the actions denounced by the complainants were structural, both as regards the defective nature of the email addresses intended for the exercise of the rights of persons and the excessive complexity of the right of access procedure reserved for prospects receiving solicitations by post.

62. Therefore, and although the company indicated, during the meeting, that it had satisfied 11,633 requests to exercise its customers' rights, the number of persons concerned by the breach of Article 12 of the Regulation, i.e. potentially all of the company's customers, given the systemic nature of the malfunctions, far exceeds the number of complainants who reported this negligence to CNIL.

63. In view of all these facts, the restricted committee considered that the company breached the obligation laid down in Article 12(2) of the Regulation to facilitate the exercise of the rights conferred on the data subjects.

## B. Breach of the obligation to ensure the security of personal data (Article 32 of the GDPR)

### 1. Vulnerability behind the personal data breach suffered by the company

#### *a. Characterisation of the breach*

64. According to Article 32( 1) of the Regulation, "*the controller shall implement appropriate technical and organisational measures to ensure a level of safety appropriate to the risk*".

65. Furthermore, d) of the same paragraph 1 provides that "*as appropriate*", i.e. depending on in particular "*the scope, of the context and purposes of the processing and of the risks*" for the data subjects, the controller shall implement "*a procedure to test, analyse and evaluate the effectiveness of the technical and organisational measures taken to ensure the security of the processing*".

The rapporteur argued that the vulnerability resulting from the breach of personal data suffered by the company resulted in particular from a lack of vigilance by the controller regarding the measures implemented by its data processor responsible for securing its website.

66. In defence, the company first argued that the security obligation resulting from Article 32 of the Regulation is an obligation to provide the means and not to produce a result, so that the finding of a personal data breach does not necessarily involve a breach of this article. It also argued that the rapporteur did not take into account the security measures implemented prior to this breach, which consisted of strengthening the security measures applied to the processing, such as the implementation of two separate servers for the operation of the site or the securing of the entry doors to the servers, as well as strengthening the control of the measures implemented by its processor, in particular through regular exchanges between the company's data protection officer and the latter.

67. The restricted committee recalled that the IT attack leading to the compromise of the personal data of the company's customers was made possible by the exploitation of a vulnerability affecting a module implemented on the company's website, the version of which was obsolete at the time of the attack.

68. First of all, it noted that as of 13 October 2018, it had been posted on the GitHub platform used to make the jQuery-File-Upload module available at the origin of the breach, an update of this module incorporating a patch whose timely installation on the company's website would have made the attack impossible. It further noted that, due to the criticality of this obsolete version of the module, the National Information Systems Security Agency (hereinafter the "ANSSI") had also communicated on this vulnerability and referred to the patch of the module in a publication on its website on 19 October 2018. Thus, on 27 December 2018, the date of the attack on the company's server, the update of the jQuery-File-Upload module incorporating the patch that would have made this attack impossible was put online for more than two months on the GitHub platform and had been relayed by the ANSSI.

69. In this case, the restricted committee pointed out that although the responsibility for the failure to update in due time lies with [redacted], which was responsible for securing the company's website, the controller failed to determine the nature of the measures incumbent on its processor, as well as the monitoring of their proper performance by the latter.

70. In this respect, the restricted committee pointed out that it appears from a combined reading of Article 32(1) (d) and Article 28(3) of the Regulation that controllers are required to continue to monitor regularly the effectiveness of the technical and organisational measures implemented to ensure the security of the processing, including the effectiveness of the measures taken by their processor. If, as the company argues, this security obligation is indeed an obligation to provide the means and not to produce a result, it is required throughout the subcontracting relationship and not only at the time of the choice of the latter and the contractualisation of the service.

71. The restricted committee noted that the monthly security reports by which [redacted] reports to [redacted] on the technical and organisational measures implemented to ensure the security of the website were far from complying with latest industry standards since they did not specify, in particular, whether [redacted] regularly carries out a security watch on the site, including the identification and maintenance of its various software components.

72. The restricted committee pointed out, in this respect, that in order to remove this unknown and to draw up a more general assessment of the practices of its processor in terms of IT security, [redacted] could have carried out checks or audits of [redacted], which the company in question has not proven, despite the fact that the two companies have been in a business relationship since 2013.

73. The restricted committee noted that the responsibility for such shortcomings is all the more attributable to a data controller such as [redacted], which, by its scale, had all the material and financial resources sufficient to ensure the security of the data it processes.

74. Consequently, the restricted committee considered that [redacted] did not exercise a satisfactory and regular audit of the technical and organisational measures implemented by [redacted] to ensure the security of the personal data processed.

75. Moreover, the restricted committee recalled that following a first breach of personal data, [redacted] has already been penalised by SAN decision no. 2015-379 of 5 November 2015, certainly concerning different facts, but by which it was sanctioned for not ensuring the security of the personal data for which it was responsible and for not having guaranteed the security of the personal data managed by one of its former processors. Furthermore, following a new breach of personal data that affected its website, the company was again sanctioned by a decision no. SAN-2018-002 of 7 May 2018 for a breach of the security of personal data. After appeal against these decisions, the Council of State confirmed the materiality of these breaches (EC, 19 June 2017, appeal no. 396050 and 17 March 2019, appeal no. 422575)

76. In this respect, the restricted committee noted that [redacted] was involved in the facts causing several of the breaches sanctioned in these decisions, so that [redacted] should have, in light of these precedents, been particularly alerted as to the defective nature of the guarantees presented by its processor in terms of IT security and, therefore, should have been particularly vigilant.

77. Consequently, the restricted committee held that in light of these previous decisions, [redacted] could not be unaware of the importance to be given to IT security issues.

*b. Scope of the breach*

78. The company argues that the breach did not cause any harm to the customers concerned by the personal data breach, since none of these persons notified them of the fraudulent use of their personal data.

79. The restricted committee noted that it is apparent from the notification sent to CNIL on 11 January 2019 that the personal data breach compromised the personal data of nearly 200,000 European nationals: 189,707 French, 3,326 Belgians, 1,149 Germans, 786 Spanish and 332 British.

80. UK nationals are included as a whole when the United Kingdom was a member of the European Union at the time of the events in question, therefore the GDPR is applicable. Furthermore, under the Trade and Cooperation Agreement concluded on December 24, 2020 between the European Union and the United Kingdom, it appears that despite the United Kingdom's exit from the European Union on January 1, 2021, the GDPR will continue to apply on a transitional basis in the United Kingdom for a maximum additional period of six months from that date.

81. The restricted committee also recalled that the email address, the hash of the user account password, the surname and first names were compromised, address, telephone number, date of birth of customers and, for 23,000 of them, the social security number.

82. It pointed out in this respect that, in view of the nature of these personal data, and in particular the email address/hash pair of the password, the persons affected by the breach are exposed to the risk of reuse of their personal data by attackers, in particular to carry out targeted phishing campaigns or identity usurpations.

83. The restricted committee therefore considers that the company breached the provisions of Article 32 of the Regulation.

2. Lack of security for user account access passwords

84. According to Article 32(1) of the Regulation, "*the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including among others, as required: (...) B) means to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.*"

85. The controller must therefore, in accordance with Article 32(2) of the GDPR, take into account the risks posed by the processing, resulting in particular from the destruction, loss, alteration, unauthorised disclosure of personal data transmitted, stored or otherwise processed, or the unauthorised access to such data, accidentally or unlawfully.

86. The CNIL delegation noted, during the online check-up of 29 April 2019, that when creating a user account on the company's website, individuals can use a password of at least eight characters and consisting of only capital letters and figures. In its letter dated 17 September 2019, the company stated that in addition to authentication by login and password, a restriction of access to the account was also implemented, with user accounts being blocked after ten unsuccessful login attempts.

87. The rapporteur argued that the passwords accepted by the company do not ensure the security of the personal data processed in that they are not sufficiently robust and thus do not prevent "brute force" attacks, which consist in the systematic testing of many passwords and which could lead to a compromise of the associated accounts and the personal data they contain.

88. In defence, the company recalled that the rules for creating its passwords had however been redefined in mid-2018. It is surprised by the rapporteur's additional requirements in this regard, noting that for authentication to user accounts of online banks, passwords of a minimum length of five characters are allowed.

89. In its latest submissions, however, it stated that it has reinforced its password policy by requiring that its customers' passwords also contain a special character, but it does not specify whether this reinforcement has also been passed on to customers already having a user account.

90. 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, which states that "*a good password is above all a strong password, which is difficult to find even using automated tools. The strength of a password depends on its length and the number of possibilities available for each character. In fact, a password consisting of lower cases, capital letters, special characters and numbers is technically more difficult to discover than a password consisting solely of lower cases*".

91. For the sake of clarity, the restricted committee recalled that in order to ensure a sufficient level of security and satisfy the requirements for robustness of passwords, when authentication relies solely on an identifier and password, the CNIL recommends, in its deliberations no. 2017-012 of 19 January 2017, that the password has at least 12 characters - containing at least one capital letter, a lower-case letter, a digit and a 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.: "Captcha") and/or blocking the account after several unsuccessful authentication attempts.

92. In this case, the restricted committee considers, first of all, that in light of the weak rules governing their composition, the robustness of the passwords accepted by the society was weak, which put them more at the risk of a brute force attack perpetrated by a hacker.

It then pointed out that this weakness is all the more reprehensible since the user accounts to which these passwords give access contain much personal data concerning the company's customers (email address, surname and first names, postal address, telephone number, date of birth). Some user accounts even contain data of a highly personal nature, such as the social security number, or even within the category of "*special*" data within the meaning of Article 9 of the GDPR, such as medical prescriptions uploaded by customers.

93. Lastly, while online banks can simply offer their customers passwords of a minimum length of five characters, it is because, in addition to the password, authentication to these online accounts also includes additional information, secret, imposed on the user, communicated on its own and with a size of at least seven characters, which most often takes the form of a service ID (customer number or other). Furthermore, for this type of authentication, the requirements for access restrictions are also reinforced (for example, blocking the account after five unsuccessful attempts).

94. Consequently, the restricted committee considers that the passwords put in place by the company to access the user accounts of its website were not sufficiently robust at the time of the findings made by the auditing delegation and that the elements put forward by the company in its last entries do not establish whether the strengthening of its passwords applies to all customers with a user account. Therefore, the company's requirements for the robustness of passwords do not ensure the security of the personal data processed and prevent unauthorised third parties from having access to such data, in breach of Article 32 of the GDPR.

95. In light of all of these elements, the restricted committee considers that the company breached the obligation set out in Article 32 of the Regulation to ensure the security of the personal data it processes.

## III. Corrective measures

96. Under the terms of Article 20 III of the law of 6 January 1978 amended:

"*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 to comply, provided for in II, contact the restricted committee of the authority 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 not exceeding €100,000 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.*"

97. Article 83 of the GDPR stipulates that:

"*1. Each supervisory authority shall ensure that the administrative fines imposed under this Article for infringements of this Regulation referred to in paragraphs 4, 5 and 6 are, in each case, effective, proportionate and dissuasive.*
*2. Depending on the specific characteristics of each case, administrative fines shall be imposed in addition to or instead of the measures referred to in Article 58(2)(a) to (h) and (j). In deciding whether to impose an administrative fine and to decide on the amount of the administrative fine, the following shall be taken into account in each case:*
*a) the nature, seriousness and duration of the breach, taking into account the nature, scope or purpose of the processing concerned, the number of data subjects affected and the level of damage they have suffered;*
*b) whether the breach was committed deliberately or due to negligence;*
*c) any action taken by the controller or processor to mitigate the damage suffered by the data subjects;*
*d) the degree of responsibility of the controller or processor, taking into account the technical and organisational measures they have implemented pursuant to Articles 25 and 32;*
*e) any relevant breach previously committed by the controller or processor;*
*f) the degree of cooperation established with the supervisory authority to remedy the breach and mitigate any adverse effects;*
*g) the categories of personal data concerned by the breach;*
*h) how the supervisory authority has become aware of the breach, in particular whether, and to what extent, the controller or processor has notified the breach;*
*i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned for the same purpose, compliance with those measures;*
*j) the application of codes of conduct approved under section 40 or certification mechanisms approved pursuant to section 42; and*
*k) any other aggravating or mitigating circumstances applicable to the circumstances of the case, such as financial benefits obtained or losses avoided, directly or indirectly, as a result of the breach.*"

98. **Firstly**, concerning the imposition of an administrative fine, the company argued that the CNIL chair should first have sent it an order to comply instead of directly contacting the restricted committee.

99. It added that the amount of any fine imposed should be reduced in view of its cooperation with CNIL's services since the notification of the breach, the non-intentional nature of the breaches alleged against it and the absence of any profits or benefits derived from them.

100. The restricted committee recalled, first of all, that in accordance with Article 20 of the French Data Protection Act, the chair of the CNIL is not required to send an order to comply to the organisation before initiating sanction proceedings against it.

101. Furthermore, if it is established that the company has taken steps to quickly end the personal data breach since the vulnerability was discovered, that it has actively cooperated with CNIL's

services since the notification of the personal data breach and that it has not intentionally committed the breaches of which it is accused, the restricted committee pointed out that the imposition of an administrative fine is no less justified in accordance with the relevant criteria laid down in Article 83(2) of the Regulation.

102. Firstly, the restricted committee recalled that the company has breached two basic IT security obligations, concerning the timely installation of the published critical updates relating to the software it uses and concerning the regular evaluation of the measures taken to ensure the security of the personal data processed, and in particular monitoring of the effectiveness of the technical and organisational measures implemented by its processor.

103. Secondly, it pointed out that the number of persons affected is significant, with the breach of personal data compromising the personal data of nearly 200,000 European nationals. Furthermore, with regard to the procedure for exercising rights, the systemic nature of the malfunctions causing the breach associated with the significant volume of solicitations sent by the company for commercial prospecting purposes, implies that at least hundreds of thousands of prospects or customers of the company are or have been likely to be affected by the two-stage right of access procedure implemented by the company and the defective email addresses indicated for the exercise of rights.

104. Thirdly, it noted that the categories of data exposed by the breach are numerous and reveal personal information, some highly personal, of the lives of individuals, such as their email address, surname and first names, address, telephone number, date of birth and, for 23,000 of them, their social security number. These personal data are also likely to be reused by attackers to carry out phishing campaigns with the data subjects.

105. Lastly, over the past five years, the restricted committee has already twice penalised the company for breaches of personal data security as well as for a breach of subcontracting in the context of previous data breaches.

106. Therefore, since the breaches of Articles 12(2) and 32 of the Regulation are characterised, the restricted committee considers that an administrative fine should be imposed.

107. With regard to the amount of the administrative fine, the restricted committee noted that in 2017 the company achieved a turnover of [redacted] and made a profit of [redacted] and that pursuant to the provisions of Article 83(5) of the GDPR, it incurs a financial penalty of a maximum amount of €20 million.

108. Therefore, in light of the company's financial capacity and the relevant criteria of Article 83(2) of the Regulation referred to above, the restricted committee considers that imposing a fine of €250,000, which would therefore only represent [redacted] of that turnover, appears to be both effective, proportionate and dissuasive, in accordance with the requirements of Article 83(1) of that Regulation.

109. **Secondly**, with regard to the need to issue an injunction, the restricted committee noted that, with regard to the breach of the exercise of rights, the company has not provided any information since the start of the proceedings which would allow it to be considered that it now facilitates requests for access from persons who have been subject to commercial prospecting by post and that it has followed up on the request for opposition from the applicant at the origin of referral no. [redacted].

110. Furthermore, with regard to the breach of the security of personal data, the company did not provide any evidence that the strengthening of its password policy was passed on to all its customers, particularly to customers already having a user account.

111. Consequently, if the company fails to comply with the breaches of Article 12(2) and Article 32 of the Regulation, the restricted committee considers that an injunction should be issued.

112. It follows from all of the above and from taking into account the criteria laid down in Article 83 of the GDPR that an administrative fine of €250,000 and an injunction with a penalty are justified and proportionate.

**FOR THESE REASONS**

**The CNIL's restricted committee, after having deliberated, decides to:**

- for breaches of Articles 12 and 32 of Regulation no. 2016/679 of 27 April 2016 on the protection of personal data, order [redacted] to pay an administrative fine of €250,000 (two hundred and fifty thousand euros);

- rule against [redacted] an injunction to bring the processing into compliance with the obligations resulting from Articles 12 and 32 of Regulation no.2016 /679 of 27 April 2016 on the protection of personal data, and in particular:
  - with regard to the failure to exercise the rights of persons, facilitate all requests addressed to it, in accordance with the provisions of Article 12( 2) GDPR, and in particular:
    - facilitate requests for access rights from persons subject to commercial prospecting by post, for example by implementing a mechanism to redirect these requests to its processor effectively and to ensure their follow-up and proper consideration by the processor;
    - provide an exhaustive response to the applicant's request for a right of opposition at the origin of referral no. 19000723;

  - with regard to the breach of the obligation to ensure the security of personal data, take all measures to preserve the security of such data and prevent unauthorised third parties from accessing them pursuant to Article 32 of the GDPR, and in particular:
    - implement a robust and binding password management policy for all user accounts, for example, under one of the following methods:

- passwords shall consist of at least 12 characters, containing at least one letter, a lower case, one digit and a special character;
- passwords are composed of at least eight characters, containing three of the four character categories (upper case letters, lower case letters, digits and special characters) and are accompanied by a complementary measure such as the timing of access to the account after several failures (temporary access suspension whose duration increases as attempts are made), the establishment of a mechanism to guard against automated and intensive submission of attempts (for example: "captcha") and/or blocking the account after several unsuccessful authentication attempts (maximum ten).

- attach to the injunction a penalty payment 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.

The Chairman

Alexandre LINDEN