Deliberation of the restricted committee no SAN-2020-009 of November 18, 2020 concerning the company [...]

The National Commission for Computing and Liberties, meeting in its restricted formation composed of Messrs Alexandre LINDEN, president, Philippe-Pierre CABOURDIN, vice-president, and Mesdames Sylvie LEMMET and Christine MAUGÜE, members;

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

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

Considering the law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms, in particular its articles 20 and following;

Having regard to decree no. 2019-536 of May 29, 2019 taken for the application of law no. 78-17 of January 6, 1978 relating to data processing, files and freedoms;

Having regard to deliberation no. 2013-175 of July 4, 2013 adopting the internal regulations of the National Commission for Computing and Liberties;

Considering Ordinance No. 2020-306 of March 25, 2020 relating to the extension of the deadlines expired during the period of health emergency;

Having regard to decisions no. 2019-081C of April 24, 2019 and no. 2019-102C of June 6, 2019 of the President of the National Commission for Computing and Liberties to instruct the Secretary General to carry out or have carried out a verification mission processing implemented by this organization or on behalf of the company [...] and its subsidiaries, and in particular the company [...];

Having regard to the decision of the Vice-President of the National Commission for Computing and Freedoms appointing a rapporteur before the restricted formation, dated November 29, 2019;

Having regard to the report of Mr Éric PÉRÈS, commissioner rapporteur, notified to the company [...] on January 10, 2020;

Having regard to the written observations submitted by the board of the company [...] on March 10, 2020;

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

Having regard to the written observations of the board of the company [...] received on August 24, 2020;

Having regard to the oral observations made during the session of the Restricted Committee;

Having regard to the other documents in the file;

Were present at the restricted training session of September 17, 2020:

- Mr Éric PÉRÈS, commissioner, heard in his report;

As representatives of the company [...]:

- [...];

- [...];

- [...];

- [...];

- [...];

- [...];

- [...].

The company [...] having had the floor last;

The Restricted Committee adopted the following decision:

I. Facts and procedure

1. The company [...] is a subsidiary owned 40% by the company [...] and 60% by the company [...], the parent company of the group [...].

2. Created in […], the […] group (hereinafter “the group”), whose registered office is at […], has mass distribution as its main activity. He also works in other areas such as the banking and insurance sector, e-commerce and travel agencies. In 2018, it employed around 360,000 people and had a turnover of 76 billion euros.

3. Based […], the company […] (hereinafter "the company") is a banking establishment whose main activities are consumer credit, portfolio management, insurance brokerage and services of investment. In 2018, it employed around 300 people and had generated net banking income of 308 million euros.

4. As part of its activities, the company publishes the website www. [...] (hereinafter "the site [...]"). It also markets a payment card intended for the group's [...] customers (hereinafter the "card [...]"), which can be linked to the group's loyalty program.

5. Pursuant to decisions no. 2019-081C of April 24, 2019 and no. 2019-102C of June 6, 2019 of the President of the

Commission, the CNIL services carried out an online check, on July 5, 2019, relating to the site [...] and to the processing implemented from this site as well as an on-site inspection at the premises of the company [...], on July 9, 2019, relating to the processing concerning the card [. ..].

6. The purpose of these assignments was to verify, in particular, compliance by the company with all the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (hereinafter "Regulation " or " the RGPD ") and of the modified law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms (hereinafter " the data processing and freedoms law ").

7. Within the framework of the on-site inspection, the representatives of the group [...] specified to the delegation that the company [...] is responsible for processing the two payment programs (debit and credit) of the card [. ..] while the company [...] is responsible for processing the third program allowing the linking of the card [...] to the database " [...] " which implements the loyalty program [. ..].

8. On July 19, 2019, the company transmitted to the delegation of control the documents requested in the context of the on-site inspection of July 9, 2019 and in particular the count of the number of cards [...] attached to the loyalty program [. ..].

9. For the purpose of examining these elements, the Vice-President of the Commission appointed Mr Éric PÉRÈS as rapporteur, on November 29, 2019, on the basis of Article 22 of the "Informatique et Libertés" law.

10. At the end of his investigation, the rapporteur had a bailiff serve on the company [...], on January 10, 2020, a report detailing the breaches of the GDPR and the "IT and Freedoms" law that he considered constituted in this case.

11. This report proposed that the restricted committee of the Commission issue an injunction to bring the processing into compliance with the provisions of Articles 5, 12 and 13 of the Regulations and Article 82 of the "Informatique et Libertés" law, together with a penalty payment, as well as an administrative fine. He also proposed that this decision be made public and no longer allow the company to be identified by name after the expiry of a period of two years from its publication.

12. On January 29, 2020, the company requested a one-month extension of the deadline within which it had to respond to the report, the postponement of the meeting initially scheduled for March 24, 2020 and a meeting with the rapporteur. On February 3, the president of the restricted formation granted the requested extension for a period of one month. On February 6, the secretary general of the CNIL granted the request to postpone the meeting to April 21, 2020. On the same day, the rapporteur refused the meeting requested by the company.

13. On March 10, 2020, through its counsel, the company submitted observations and made a request that the session before the Restricted Committee be held behind closed doors.

14. By email dated March 23, 2020 and on the basis of Article 40, paragraph 4, of Decree No. 2019-536 of May 29, 2019, the rapporteur asked the President of the Restricted Committee for an additional period of fifteen days to respond to the company's comments.

15. By letter dated March 24, 2020, noting in particular the context of the health crisis, the President of the Restricted Committee granted the rapporteur's request.

16. By letter of the same day, the company was informed of the additional time granted to the rapporteur and of the fact that it had, pursuant to paragraph 5 of article 40 of decree no. 2019-536 of May 29 2019, within one month to respond to the rapporteur's response. The letter also informed him of the second postponement of the restricted training session, scheduled for April 21, 2020.

17. By e-mail of April 7, 2020, the rapporteur asked the chairman of the Restricted Committee for a new additional period of fifteen days to respond to the company's observations, which was granted to him on April 8, 2020. The company was informed the same day.

18. The rapporteur responded to the company's observations on April 22, 2020.

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

20. On June 30, 2020, the chairman of the Restricted Committee granted the company's request for a closed session, on the grounds that certain elements included in the debates were protected by business secrecy, as provided for by Article L 151-1 of the Commercial Code.

21. On August 5, 2020, the CNIL services notified the company of a notice to attend the restricted training session of September 17, 2020.

22. On August 24, 2020, the company produced new observations in response to those of the rapporteur.

23. The company and the rapporteur presented oral observations during the session of the Restricted Committee.

II. Reasons for decision

A. On the breach of the obligation to process data fairly

24. According to Article 5, paragraph 1, a) of the GDPR: "Personal data must be: a) processed in a lawful, fair and transparent manner with regard to the data subject (lawfulness, fairness, transparency )".

25. It emerges from the observations made by the delegation of control that when a subscriber to a payment card (card [...]) also wishes to join the loyalty program [...], the company [...] ] made several requests to the company [...] including, in particular, a request to join the loyalty program [...].

26. Indeed, during the online check, the delegation noted that if he wants to join the loyalty program [...], the subscriber to the card [...] must in particular tick the box at the bottom of the page entitled "My loyalty rewarded" in support of which appears the following statement: "I wish to link my Loyalty account [...] to my card [...] (or failing that, create and link it). To do this , I accept that [...] communicate to [...] Fidélité my surname, first name and email. [...] undertake not to transmit any other information to [...] Fidélité ".

27. It appears from the documents submitted to the delegation during the on-site inspection that the company [...] also sends to the company [...], in addition to the surname, first name and email address of the subscriber to the card [. ..] mentioned above, their postal address and their telephone number(s). When it has this information, it also informs the company [...] of the number of children declared by the subscriber.

28. The rapporteur thus considers that the company breached the principle of fairness when it transmitted to the company [...] more personal data concerning card subscribers [...] than those exhaustively listed as part of the online subscription process.

29. The company responds, first of all, that since the concept of loyalty is not defined in the Rules, the rapporteur cannot ask the restricted committee to sanction its violation.

30. It also notes that the principle of fairness can at most be attached to the obligation of transparency, provided for in Article 12 of the Rules. In this case, it claims to have complied with this transparency requirement since the information statement questioned by the rapporteur informs people of the existence of the processing, its purpose and the transfer of this data. to third parties.

31. Finally, it maintains that the practices denounced could be qualified as unfair all the less as they result only from a failure to update its website, due to a communication error between the various departments of the two companies.

32. The Restricted Committee recalls that the principle of loyalty is an autonomous principle provided for in Article 5, paragraph

1, a) of the GDPR, the violation of which by a data controller is likely to give rise to the pronouncement of a corrective measure. from the supervisory authority.

33. It notes, in this regard, that this provision must be interpreted in the light of recital 60 of the Regulation, according to which: "the principle of fair and transparent processing requires that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any other information necessary to ensure fair and transparent processing, taking into account the particular circumstances and the context in which the personal data is processed".

34. In this case, the Restricted Committee considers that the information provided in this statement was both imprecise and misleading.

35. First of all, the Restricted Committee notes that the company [...] mentions "[...] Fidélité" as the recipient of the data communicated even though this service, attached to the company [...], does not had, before this mention, never been presented to subscribers of the card [...]. Thus, the persons concerned could not understand for themselves that their personal data were in fact communicated to a third company, the company [...].

36. Next, the Restricted Committee considers that the information provided to the persons concerned was misleading and unfair since the company had expressly indicated, in this same information notice, that it "undertake[d] not to transmit no other [...] Loyalty information" than the surnames, first names and e-mail address of card subscribers [...] even though such was precisely not the case.

37. The Restricted Committee therefore considers that a breach of Article 5, paragraph 1, a) of the GDPR was constituted.

38. It notes, however, that on the day of the meeting, the company had completely overhauled the online à la carte subscription process [...] and, in particular, rewritten the disputed information notice. Card subscribers wishing to be part of the loyalty program [...] are now informed of the fact that personal data concerning them are transmitted to the company and [...] are also informed about the exact nature of the data actually transmitted.

B. On the breach relating to the information of persons

39. Article 12 of the Regulation provides that: "the controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 […] with regard to the processing to the data subject in a concise, transparent manner , comprehensible and easily accessible, in clear and simple terms […]".

40. Article 13 of the same Regulation lists the information to be communicated to data subjects when personal data is collected from them.

1. Regarding the accessibility of information

41. Firstly, the rapporteur considers that, as evidenced by the observations made by the delegation during the online check, the information made available to users of the site [...] through various channels, was not readily available within the meaning of Rule 12 of the Rules.

42. To read the information provided on the processing of his personal data, the user could first click on the "Protection of banking data" tab appearing at the bottom of the page of the site. Alternatively, he could also click on the "Legal notices" link appearing at the bottom of the page of the site, reach point 3 of these notices, entitled "3 - Protection and confidentiality of personal data processed by [...]" and, finally , click on the link "To find out more about our personal data protection policy, see our dedicated page", which referred to the company's privacy policy entitled "Protection and confidentiality of personal data processed by [...]" ,

43. The company maintains that it was perfectly justified in inserting a link to its privacy policy in its legal notices and that in any event, this information was provided directly via the "Banking data protection" tab appearing in the footer of the site.

44. The Restricted Committee recalls that in order to consider that a data controller meets his obligation of transparency, the information provided must in particular be "easily accessible" for the persons concerned within the meaning of Article 12 of the Regulation.

45. It notes, in this regard, that this provision must be interpreted in the light of recital 61 of the Regulation, according to which: "information on the processing of personal data relating to the data subject should be provided to him at the time where these data are collected from it".

46. □□In this sense, it shares the position of the G29 presented in the guidelines on transparency within the meaning of the Regulation, adopted in their revised version on 11 April 2018 (hereinafter "the guidelines on transparency"), which recalls that "the data subject should not have to search for the information but should be able to access it immediately".

47. To illustrate how it is possible to meet this accessibility criterion, these same guidelines specify, with regard to an online environment, that "each company with a website should publish a statement or notice statement on its website. A direct link to this privacy statement or notice should be clearly visible on every page of this website under a commonly used term (such as

"Privacy", " Privacy Policy" or "Privacy Notice". Texts or links whose layout or choice of color makes them less visible or difficult to find on a web page are not considered easily accessible" .

48. In the present case, the Restricted Committee considers, firstly, that the vagueness of the title of the "Protection of bank data" tab appearing at the foot of the page of the site, referring to bank data and not the data of a personal nature, could not allow the persons concerned to easily understand that by clicking on this link they would be redirected to the privacy policy of the site, containing information relating to the processing of their personal data. Indeed, for the general public, a large part of the data processed (address, number of children, etc.) does not come under "banking data".

49. Next, with regard to the second channel of information, users of the site [...] could not guess for themselves that the link to the site's privacy policy was inserted in the site's legal notices . Thus, to reach this privacy policy, users must, in a certain number of cases, first take several actions, such as, for example, clicking on the "Accessibility" or "General conditions of sale" links also appearing in foot of the home page, before finally clicking on the "Legal notices" link.

50. As a result, the information provided to users of the site [...] was not "easily accessible".

51. Secondly, the rapporteur considers that the information relating to the card [...] provided as part of the online subscription process on the site [...] and as noted during the online check no. nor was it "easily accessible" since the subscribers of this card did not have complete information relating to the processing of their data on the presentation page of the subscription process and they were not, no more, invited to read more complete information, for example by means of a hypertext link to additional information.

52. The company argues that such a link already existed through the "Banking data protection" tab at the bottom of the site page.

53. The Restricted Committee emphasizes that according to the principle of transparency, as recalled in particular in recital 61 of the GDPR, information must be communicated to individuals at the time the data is collected.

54. As an example, the G29 Transparency Guidelines mention that, in an online context, "a link to the privacy statement or notice should be provided at the point collection of personal data, or that this information is available on the same page where the personal data is collected".

55. In this case, it is apparent from the findings that the company has chosen to adopt information at several levels.

56. In this respect, if the company did indeed provide, on the presentation page of the card subscription process [...] the

information expected as first-level information, namely the identity of the person in charge of processing, the main purposes of the processing and the description of the "Computing and Freedoms" rights, the restricted committee notes, on the other hand, that the company had neglected to complete these mentions by allowing people to read complete information by inserting, for example , a hypertext link to second-level information, in this case, to the company's privacy policy, which is supposed to detail all the information required by article 13 of the Regulation.

[...] and recalls that in any event its title would not have allowed the persons concerned to easily understand that by clicking on this link they were going to be redirected to the company's privacy policy.

58. As a result, data subjects were not informed, at the time of collection of their personal data, of all the information relating to the processing. As a result, not all of the information provided to card subscribers [...] on the site was "easily accessible".

59. The Restricted Committee therefore considers that the company disregarded the provisions of Article 12 of the Regulation.

60. It notes, however, that on the day of the meeting, the company had completely overhauled its website and that the information now provided both to users of the site and to card subscribers satisfies [...] now meet the requirements of section 12 of the Regulations.

2. With regard to the content of the information

61. The rapporteur considers that the company's confidentiality policy, entitled "Protection and confidentiality of personal data processed by [...]" and accessible according to the methods mentioned above, was both imprecise and incomplete as regards statements relating to retention periods. Thus, on the one hand, the information policy contained too vague formulations, not making it possible to identify defined durations and, on the other hand, the company did not give any information concerning certain data which it nevertheless indicated to collect, such as behavior data, habits and online consumption preferences collected by cookies placed on users' terminals from its website. Otherwise,

62. The company contests the imprecise nature of its information notices relating to retention periods and argues that the information relating to cookies was available in another development of its "Legal notices".

63. The Restricted Committee recalls that under the terms of Article 13, paragraph 2, a) of the Regulation, the controller provides the data subject with information relating to "the retention period of personal data or, when it is not possible, the criteria used to determine this duration ".

64. By way of clarification, the aforementioned guidelines on transparency recommend that "the retention period [be]

formulated in such a way that the data subject can assess, depending on the situation in which he finds himself, what the in the case of specific data or in the case of specific purposes. The controller cannot simply state in general terms that the personal data will be kept for as long as the legitimate purpose of the processing requires. where appropriate, different storage periods should be mentioned for different categories of personal data and/or different processing purposes, in particular periods for archival purposes".

65. In the present case, the Restricted Committee points out, first of all, that the use of vague and undefined formulas such as "the applicable legal limitation periods" or "the retention of your data by [...] varies according to the applicable regulations and laws" or even the expressions "by way of example" or the adverb "in particular" necessarily made it confusing for the persons concerned to understand the extent and nature of the data stored as well as the retention periods applied to this data.

66. It then adds that the information was also incomplete insofar as the company neglected to specify the retention periods applicable to all the data processed or did not specify the criteria used to determine these periods. Thus, the company did not specify that it archived the contractual data for five years, the duration of the applicable legal prescription, in the event of litigation. Moreover, it did not specify the retention periods for the data collected by cookies, since if the "Legal notices" of the site did include a paragraph relating to cookies, the latter did not specify the retention periods for the data collected by these cookies.

67. The Restricted Committee therefore considers that a violation of Article 13 of the Rules was established.

68. It notes, however, that on the day of the meeting, the company had completed its information notices and that its confidentiality policy now meets the requirements of Article 13 of the Rules.

C. On the breach relating to cookies

69. Article 82 of the "Informatique et Libertés" law (Article 32.II in the same wording on the day of the findings) requires that users be informed and that their consent be obtained before any access or registration operation. to information already stored in their equipment. Any deposit of cookie or other tracer must therefore be preceded by the information and consent of the users. This requirement does not apply to cookies whose "exclusive purpose is to enable or facilitate communication by electronic means" or which are "strictly necessary for the provision of an online communication service at the express request of the user".

70. The rapporteur considers that the company did not comply with these provisions since it was noted during the online check

that when arriving on the website [...], several cookies did not fit in the two cases mentioned above were deposited on the user's terminal upon connection to the site's home page and before any action on his part.

71. The company does not contest these elements.

72. The Restricted Committee notes, in this case, that the deposit of thirty-one cookies was automatic upon arrival on the home page of the site and before any action by the user.

73. The Restricted Committee observes that five of these cookies (the "MUIDB", "GPS" and "gid", "_ga" and "_gat_trackerBanque" cookies) had neither the exclusive purpose of allowing or facilitating communication by electronic, nor were they strictly necessary for the provision of a service expressly requested by the user.

74. With regard, firstly, to the three "gid", "_ga" and "_gat_trackerBanque" cookies, known as Google analytics, the Restricted Committee stresses that it is not in dispute that the data collected by these cookies can be cross-checked with data resulting from other processing to pursue different purposes than those restrictively provided for by article 82 of the law “Informatique et Libertés”, in particular to carry out personalized advertising. Indeed, it appears from the practical guide "Association of Analytics and Google Ads accounts", posted on one of the sites of the Google company, that "the integration of Google Analytics into Google Ads (…) allows [advertisers] to know precisely how well [their] ads result in conversions, then quickly adjust creatives and bids accordingly. [Advertisers can] also combine products to identify [their] most valuable segments and then engage those users with personalized messaging.”

75. With regard, then, to the "MUIDB" and "GPS" cookies, the Restricted Committee notes that these two cookies are tracking cookies, the first making it possible to follow a user visiting different domain names belonging to the company Microsoft, the second registering an identifier on the user's terminal in order to geolocate it. Therefore, the deposit of these five cookies should have required the company to obtain the user's consent beforehand.

76. The Restricted Committee therefore considers that a breach of Article 82 of the “Informatique et Libertés” law was constituted.

77. It notes, however, that on the day of the meeting, the company had completely overhauled its cookie policy. These modifications led, in particular, to the stopping of the automatic deposit of cookies on arrival on the home page of the site since March 4, 2020.

III. On corrective measures and publicity

78. Under the terms of III of article 20 of the law “Informatique et Libertés”:

"When the data controller or its subcontractor does not comply with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or from this law, the President of the National Commission for Computing and Liberties may also , if necessary after having sent him the warning provided for in I of this article or, if necessary in addition to a formal notice provided for in II, seize the restricted formation of the commission with a view to the pronouncement, after adversarial procedure, one or more of the following measures: […]

7° With the exception of cases where the processing is implemented by the State, an administrative fine not exceeding 10 million euros or, in the case of a company, 2% of the annual worldwide turnover total for the previous year, whichever is higher. In the cases mentioned in 5 and 6 of Article 83 of Regulation (EU) 2016/679 of April 27, 2016, these ceilings are increased, respectively, to 20 million euros and 4% of said turnover. The restricted formation takes into account, in determining the amount of the fine, the criteria specified in the same article 83. "

79. Article 83 of the GDPR provides:

1. Each supervisory authority shall ensure that administrative fines imposed under this Article for breaches 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 points (a) to (h) and (j) of Article 58(2). In deciding whether to impose an administrative fine and in deciding the amount of the administrative fine, due account shall be taken in each individual case of the following:

a) the nature, gravity and duration of the breach, taking into account the nature, scope or purpose of the processing concerned, as well as the number of data subjects affected and the level of damage they have suffered;

b) whether the breach was committed willfully or negligently;

c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

d) the degree of responsibility of the controller or processor, taking into account the technical and organizational 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 with a view to remedying the breach and mitigating its possible negative effects;

g) the categories of personal data affected by the breach;

h) how the supervisory authority became aware of the breach, including whether and to what extent the controller or processor 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 pursuant to Article 40 or certification mechanisms approved pursuant to Article 42; and

k) any other aggravating or mitigating circumstances applicable to the circumstances of the case, such as the financial advantages obtained or the losses avoided, directly or indirectly, as a result of the violation. "

80. Firstly, concerning the proposed sanction, the company argues that since the breaches of loyalty and information would not be identified, the imposition of an administrative fine does not appear necessary.

81. It argues that it would in any event be appropriate to reduce the amount of the fine proposed, insofar as the alleged breaches are devoid of seriousness and that it has operated, since the beginning of the sanction procedure, major compliance work.

82. In view of the relevant criteria provided for in Article 83 of the Rules, the Restricted Committee considers, on the contrary, that the imposition of an administrative fine is necessary.

83. In the present case, with regard, firstly, to the nature, gravity and duration of the violation, the Restricted Committee notes that this criterion is characterized for the breach linked to loyalty when the company has provided its customers with information contrary to the reality of the processing carried out.

84. Secondly, with regard to the number of persons concerned, the Restricted Committee emphasizes that the infringement relating to cookies concerned a large number of persons since the cookies made it possible to follow in the same way, without distinction, the online behavior card subscribers [...] and potential prospects of the company, but also all Internet users likely to browse its website.

85. In addition, the breaches of loyalty and information also concerned all of the subscribers of the card [...] attached or not to the loyalty program [...] which, according to the elements noted by the delegation of control, amount to at least […] people.

86. Thirdly, with regard to the measures taken by the controller to mitigate the damage suffered by the data subjects and the

degree of cooperation with the supervisory authority, the Restricted Committee notes the perfect cooperation of the company throughout the sanction procedure and the very significant efforts made to achieve full compliance on the day of the session. It notes that the three shortcomings have been corrected to date.

87. With regard to the amount of the administrative fine, the Restricted Committee recalls that in 2018 the company generated net banking income of €308 million and that, pursuant to the provisions of Article 83, paragraph 5 , it incurs a financial penalty of a maximum amount of 20 million euros.

88. Therefore, with regard to the financial capacities of the company and the relevant criteria of Article 83, paragraph 2, of the Rules mentioned above, the Restricted Committee considers that the imposition of a fine of €800,000, which would therefore represent only 0.25% of this net banking income, appears to be effective, proportionate and dissuasive, in accordance with the requirements of Article 83, paragraph 1, of this Regulation.

89. Secondly, concerning the issuance of an injunction, the company maintains that insofar as it has remedied all of the breaches of which it is accused, the requests made under the injunction proposed under penalty lose all foundation.

90. The Restricted Committee notes that, once the company has corrected all of the shortcomings noted in the sanction report, the issuance of an injunction is no longer justified.

91. Thirdly, regarding the publicity of this decision, the company maintains that such a measure would not respect the constitutional principle of the necessity of the penalties since it would have already been part of an approach consisting in reinforcing the conformity of his situation to the requirements of the data protection regulations. It adds that publicity would have particularly harmful consequences in that it would risk affecting its reputation in a lasting manner.

92. The Restricted Committee considers that the publication of this decision is justified in view of the seriousness of the breaches sanctioned and the number of people concerned.

93. It considers that this measure will make it possible to inform all of the company's potential customers and prospects of the existence of various breaches sanctioned and in particular breaches of disloyalty and cookies.

94. Finally, the measure is not disproportionate since the decision will no longer identify the company by name at the end of a period of two years from its publication.

95. It follows from all of the above and from taking into account the criteria set out in Article 83 of the Rules that an administrative fine of 800,000 euros as well as an additional sanction of publication for a period of two years are justified and

proportionate.

FOR THESE REASONS

The CNIL Restricted Committee, after having deliberated, decides to:

• impose an administrative fine on the company [...] in the amount of 800,000 (eight hundred thousand) euros for breaches of Articles 5, paragraph 1, a), 12 and 13 of the GDPR and article 82 of the law "data-processing and freedoms";

• make public, on the CNIL website and on the Légifrance website, its deliberation, which will no longer identify the company by name at the end of a period of two years from its publication.

President

Alexander LINDEN

This decision may be subject to appeal before the Council of State within two months of its notification.