Deliberation of the restricted committee no SAN-2020-008 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 the postal and electronic communications code;

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;

Having regard to Ordinance No. 2020-306 of March 25, 2020 relating to the extension of time limits due during the health emergency period;

Given the referrals to our […]

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 companies […], […], […], […] and […];

Having regard to the observations sent to the Commission by the company […] on 5 December 2019;

Having regard to the decision of the President of the National Commission for Computing and Freedoms appointing a rapporteur before the restricted formation, dated December 10, 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 company's board […] received on August 24, 2020;

Having regard to the additional observations received on September 15, 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 […]:

- […];

- […];

- […];

- […];

- […];

- […].

Society […] having had the last word;

The Restricted Committee adopted the following decision:

I. Facts and procedure

1. The company […] (hereinafter "the company") is a subsidiary of the group […] (hereinafter "the group") located […], operating in many areas. Its main activity is mass distribution, but the group has diversified its activities, for example by intervening in the banking and insurance sector, as well as as a travel agency or even a salesperson specializing in e-commerce.

2. In 2019, the group […] employed around 360,000 people, had a turnover of around €80 billion and adjusted net income, group share, of €905 million, up compared to 2018 (804 million euros). The company […] achieved, in 2019, a turnover of around 14 million euros, for a net loss of around 1.6 billion euros.

3. The group […] is notably made up of the parent company […], which owns the company […] at 99.61%. The latter holds the

company […] at 82% and the company […] at 99%. In 2019, […] had a turnover of €14.3 billion and […] had a turnover of €636 million.

4. For the needs of its activity, the company […] publishes in particular the website […] (hereinafter “the site […]”), allowing its customers to create and access a personal space and to order.

5. Between 8 June 2018 and 6 April 2019, the Commission received fifteen complaints from individuals relating to the companies in the group […].

6. Seven of these referrals (our […]) reported commercial prospecting even though the persons concerned had previously expressed their opposition.

7. Four of these referrals (our […]) followed requests to erase data which had not been granted.

8. Three of these referrals (our […]) followed requests for access to data which had not been granted.

9. A referral (no […]) was to an unsubscribe link in a commercial prospecting email.

10. Pursuant to decisions no. 2019-081C of April 24, 2019 and no. 2019-102C of June 6, 2019 of the President of the Commission, five checks were carried out online or at the company's premises:

- an online check, carried out on May 24, 2019, relating to the site […] and the processing carried out from this site;
- an on-site check, carried out on May 28, 2019, relating to the processing implemented by the company […], in particular within the framework of the loyalty program […] (hereinafter "the loyalty program"), as well as the various databases that it used to manage its customers;
- an on-site inspection, carried out on June 11 and 12, 2019, relating to the exercise of rights and the responses provided to several complainants who lodged a complaint against the company with the CNIL;
- an on-site inspection, carried out on June 26 and 27, 2019, relating more particularly to the management of personal data within the framework of the loyalty program;
- an on-site check, carried out on 11 July 2019, relating to the security measures developed by […] to protect the personal data it processes and to the data breaches that have occurred.

11. The purpose of these assignments was to verify compliance by the company with all the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (hereinafter "the Regulation" or " the GDPR") and the modified law no. 78-17 of January 6, 1978 relating to data processing, files and freedoms (hereinafter "the law of January

6, 1978" or "the data-processing law and freedoms").

12. Various exchanges took place by e-mail between the company and the delegation of control. These exchanges concerned the transmission of documents requested during checks. On December 5, 2019, the company notably sent written observations to the delegation of control covering the majority of the points raised during the controls and announcing various actions aimed at bringing it into compliance.

13. For the purposes of investigating these elements, the President of the Commission appointed Mr Éric PÉRÈS as rapporteur, on December 10, 2019, on the basis of Article 22 of the law of January 6, 1978.

14. 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, the Data Protection Act and the Postal Code and electronic communications that he considered constituted in this case.

15. 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, 13, 15, 17, 21, 32 and 33 of the Regulation and Article 82 of the Data Protection Act, accompanied by 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.

16. 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.

17. 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.

18. By e-mail 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 Chairman of the Restricted Committee for an additional period of fifteen days to respond to the company's comments.

19. 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.

20. By letter of the same day, the company was informed of the additional period 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 , one month to respond to the rapporteur's response. The letter also informed him of the postponement of the restricted training session, initially scheduled for April 21, 2020.

21. 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.

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

23. 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 March 25 2020 relating to the extension of the deadlines expired during the period of health emergency.

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

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

26. On August 24, then on September 15, the company produced new observations in response to those of the rapporteur.

27. 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 retain personal data for a period not exceeding that necessary for the purposes for which they are processed

28. Article 5-1 e) of the Regulation provides that personal data must be "kept in a form allowing the identification of the persons concerned for a period not exceeding that necessary with regard to the purposes for which they are processed".

1. The data of customers who are members of the loyalty program and users of the […]

29. On the one hand, the rapporteur criticizes the company for having set retention periods that exceed the periods necessary

for the purposes of the processing. On the other hand, he criticizes the company for having kept personal data for a longer period than those provided for.

30. The company recognizes these points, but recalls that it had decided, before the CNIL inspections, to reduce the retention periods of its inactive customers and that it had started the purge operations necessary to respect these new periods. . It further indicates that it completed all of these operations during the sanction procedure.

31. On the first point, the Restricted Committee recalls that on the day of the checks, the company indicated that the data of "loyalty" customers were kept on an active basis for four years from their last activity (this may be meaning, depending on the situation, such as the last transaction with the passage of the loyalty card at a store checkout, the last online transaction, the last modification of the personal space on the company's website or the last contact with client service).

32. It recalls that the purpose of the loyalty program established by the company is the commercial prospection of its members, as is apparent from the information notices present on the membership form. The Restricted Committee notes that the customers of large retailers, a fortiori those of a "loyalty" program, are customers who usually return to the same stores on a regular basis. Therefore, it considers that a customer who has not traded with the company for several years should no longer be considered an active customer. For illustration, both the former simplified standard no. 48 relating to customer-prospect files and online sales and the recent draft reference document relating to the processing of personal data implemented for the purposes of managing commercial activities recommend that customer data inactive are kept for a period of three years from the last contact with the company. Although this duration is indicative and is not binding as such on data controllers, the Restricted Committee considers that it constitutes a reference allowing an appropriate duration to be assessed. In this case, it notes that this duration is already substantial in the retail sector. If the particularities of the processing implemented by the company […], and in particular the deep interconnection of its databases, can justify that this three-year period is not considered excessive, the Restricted Committee considers that it cannot be extended to the four-year period initially set by the company. Considering this purpose of commercial prospecting of "loyalty" processing, it considers that a retention period of four years was not strictly necessary for the purpose pursued, and therefore excessive.

33. It nevertheless notes that the company, before the start of the control procedures, initiated a plan aimed at reducing this retention period to three years for all of its databases. In view of the interconnection between the company's various databases and the operational need to set an identical retention period for all of its data, the three-year retention period for inactive

customers appears proportionate to the purpose pursued.

34. On the second point, the Restricted Committee notes, first of all, that the company recognizes a delay in the implementation of its data erasure program but underlines the significant efforts made since the initiation of the procedure to come into compliance. The Restricted Committee notes that the delegation of control noted the presence of data concerning customers who have been inactive for more than four years, and in particular more than twenty-eight million customer members of the loyalty program who have been inactive for five to ten years. With regard to users of the site […], the Restricted Committee points out that the data of more than 750,000 users whose act of purchase dated back five to ten years, and nearly 20,000 users whose last purchase dated back more than ten years.

35. The Restricted Committee therefore considers, in view of these elements, that a breach of Article 5-1-e) of the GDPR has been constituted.

36. The Restricted Committee, however, underlines the very significant resources, both organizational and financial, deployed by the company and notes, on the day of the meeting, the compliance with the Regulations of the company's practices. The latter indeed demonstrates that it has set up an automated system for deleting the data of its customers (both from the loyalty program and from the site […]) who have been inactive for more than three years.

2. Identity documents kept in connection with the exercise of rights

37. The rapporteur criticizes the company for having kept for a period of one to six years the identity documents which were communicated to it by the persons concerned in the context of the exercise of a right. He considers that this period is excessive, the data being kept beyond the period necessary to achieve the purpose for which they are processed.

38. On this point, the company underlines the modification of these practices since the notification of the sanction report, the identity documents being kept only for the duration relating to the processing of the request in question.

39. The Restricted Committee notes that the delegation of control did in fact find that copies of the applicants' national identity cards were kept by the company for a period that could range from one to six years.

40. However, it considers that, once the request has been granted, the company no longer needs to keep a copy of the applicant's identity document. The provision of this document is indeed for the sole purpose of proving the identity of the person from whom the request emanates and it is not necessary to keep it once the identity has been confirmed.

41. The Restricted Committee also considers that, to demonstrate that it has actually granted the request, the company may,

for intermediate archiving for litigation purposes, keep only the favorable response letter, an element whose storage presents, moreover, a lower risk for the data subject.

42. It therefore considers, in view of these elements, that a breach of Article 5-1-e) of the GDPR has been constituted.

43. She nevertheless underlined the changes made upon notification of the report and observed that the company's new practices were, on the day of the meeting, in compliance with the Rules. It has indeed been shown that the identity documents are now deleted as soon as the request has been granted.

B. On the breach relating to the terms and conditions for exercising the rights

44. Article 12 of the Regulation provides, on the one hand, that "the data controller facilitates the exercise of the rights conferred on the data subject under Articles 15 to 22. In the cases referred to in Article 11, paragraph 2, the controller shall not refuse to comply with the data subject's request to exercise the rights conferred on him by Articles 15 to 22, unless the controller demonstrates that he is not able to identify the data subject" and that "where the controller has reasonable doubts as to the identity of the natural person submitting the request referred to in Articles 15 to 21, he may request that he be provided with additional information necessary to confirm the identity of the data subject".

45. It provides, on the other hand, that "the data controller shall provide the data subject with information on the measures taken following a request made pursuant to Articles 15 to 22, as soon as possible and in full state of the case within one month of receipt of the request. If necessary, this period may be extended by two months, taking into account the complexity and the number of requests. The controller informs the data subject of this extension and the reasons for the postponement within one month of receipt of the request."

46. □□Firstly, the rapporteur noted that, except in cases of opposition to the processing of data for commercial prospecting purposes, the company systematically requested proof of identity when exercising a right. .

47. The company underlined, during its exchanges with the rapporteur, that this practice was abandoned as of October 23, 2019.

48. The Restricted Committee notes that the company did not reserve the request for proof of identity only in cases where there was a reasonable doubt about the identity of the person, this request being systematic. It emphasizes that the presence (noted during the checks) of the proof of identity accompanying the requests, such as the letters in response from the company communicated to the CNIL by the complainants, demonstrated the existence of this practice. Indeed, the CNIL was informed of

a request to this effect with regard to Messrs […], […], […], […], […] and […] and Mrs […] without that the company has reasonable doubts as to the identity of the person.

49. The Restricted Committee considers that the systematic nature of the requests for proof of identity, recognized by the company, is sufficient to demonstrate that these requests were not limited to situations where the company had "reasonable doubts as to the identity of the natural person making the request".

50. It therefore considers, in view of these elements, that a breach of Article 12 of the GDPR has been constituted.

51. She nevertheless underlined the changes made by the company and noted that the company's new practices were, on the day of the meeting, in compliance with the Rules. It has in fact been shown that the letters responding to requests to exercise rights no longer systematically require proof of identity.

52. Secondly, the rapporteur criticizes the company for the delay in responding to requests to exercise rights. He points out that the response times vary but can reach nine months, without any information being communicated in the meantime to the persons concerned. He believes that these processing delays are recurrent. By way of illustration, Mrs. […]'s request for deletion and opposition was received on July 4, 2018. The withdrawal of her consent to prospecting advertising was transcribed into the database on April 15, 2019, i.e. more nine months later. Mr. […]'s request for access was received on November 7, 2018 and a response was provided on June 10, 2019, i.e. more than seven months later. Mr. […]'s request for access and opposition has been recorded in the "

53. On this point, the company recognizes, both in its second response to the rapporteur's observations and during the session of the restricted committee, a chronic delay in the processing of requests at the time of the inspection. However, it highlights the particularly significant efforts made since the control operations, the in-depth restructuring of the organization of the teams working on these issues, and the transformation of their working methods, with in particular the development of new ad hoc tools which improve the allocation and processing of requests to exercise rights, reducing their processing time as well as the risk of error.

54. The Restricted Committee observes that the company's organization structurally led to a delay in the processing of requests and notes that the company indicates that this structural failure was caused by a poor appreciation of the consequences of the GDPR. The entry into force of this text has increased the number of requests it has had to deal with, in unexpected proportions (going, before the entry into force of the GDPR, from one to two requests per day to sometimes more

than 75 requests per day after May 25, 2018).

55. The Restricted Committee observes that this lack of anticipation has had direct consequences for people exercising their rights, sometimes forcing them to formalize several reminders in the face of the silence kept by society. The Restricted Committee therefore considers, in view of these elements, that a breach of Article 12 of the GDPR has been constituted.

56. It nevertheless underlines the profound and effective changes made by the company and notes that the new practices of the company are, on the day of the meeting, in compliance with the Regulations. The company now demonstrates an average response time to requests of less than fifteen days, sometimes even less than ten days. It also demonstrates that no response has been sent out of time since the change in its internal processes and the development of new tools.

C. On the breach relating to the information of persons

57. Article 12 of the GDPR provides that "the controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 […] in relation to the processing to the data subject in a concise, transparent, understandable and easily accessible, in clear and simple terms […]". Articles 13 and 14 list the information to be provided to data subjects when personal data is collected directly from them and indirectly.

1. Regarding the accessibility of information

58. Firstly, the rapporteur considers that the information provided was not easily accessible.

59. With regard firstly to the information communicated on the site […], he notes that the multiplicity of pages to be consulted, the links present in the various pages, as well as the redundancy of the information do not make it possible to consider that information relevant to people is easily accessible.

60. With regard to the information communicated to people subscribing online to the loyalty program, the rapporteur considers that the information was not easily accessible since it was inserted within the general conditions of use of the card […].

61. Lastly, with regard to the information provided to people joining the loyalty program using a paper form, the rapporteur notes that the information was not easily accessible either. He notes that the newsletter summarized the essential information and referred for more complete information to the home page of the site […] without further details.

62. On these points, the company argues that a page dedicated to data protection was directly accessible by a hypertext link at the bottom of the page, and that it modified the information notices on its website on November 22, 2019 , or prior to the initiation of the sanction procedure and the notification of the report. These important modifications consisted in particular in

the merger of all the information notices in a single document, the retention of a page dedicated to the exercise of the various rights, and a reformulation of the information communicated in order to make it more readable, more precise and simpler.

63. The Restricted Committee notes that the company has chosen information at several levels, as permitted by the Regulations.

64. In this configuration, the Restricted Committee considers it particularly important that the information remain "easily accessible", as required by Article 12 of the Rules. The presentation of information in several levels increases the risk that the information will be more difficult to find. However, recital 39 of the GDPR emphasizes that "the principle of transparency requires that all information and communication relating to the processing of such personal data be easily accessible, easy to understand, and formulated in clear and simple terms". Recital 58 also provides that "the principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and formulated in clear and simple terms and, in addition, where appropriate, illustrated with visual elements. "

65. In the present case, the Restricted Committee considers, on the one hand, that access to the information notices on the site […] was difficult, since the latter were grouped together in Article 3 of the general conditions of use of the site […] which the user therefore had to browse. The same applies to the information relating to the loyalty program which appeared in Article 10 of the general terms and conditions of use of the card […].

66. However, these two documents were of such length that the user was forced to scroll through a large number of pages and read several dozen paragraphs (about fifteen in the general conditions of use of the site […], more of seventy in the general conditions of use of the card […]) before being able to find the information relating to the protection of his personal data. The Restricted Committee therefore considers that access to this information was not easy and that the user had to demonstrate particular determination to access information on these issues. It recalls that the information must be presented in an effective and succinct way in order to avoid drowning the information to be delivered among other informative content.

67. The difficulty of accessing this information was further reinforced by its redundancy. Indeed, the information relating to the protection of personal data being dispersed and fragmented between several documents (general conditions of use, general conditions of sale, page relating to the protection of "personal data", page dedicated to the exercise rights), some information was present only on certain pages, while others were presented several times.

68. So that the user does not have to search for the relevant information, the Restricted Committee considers that this should

be grouped together in a single document separate from the general conditions of use. It shares here the position developed by the G29 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 considers that "the data subject does not should not have to actively search for the information covered by these sections among other information such as the terms of use of a website".

69. It considers, on the other hand, that when a data controller chooses to communicate to the data subjects information at several levels, it is not only important that the second level of information details all the information relating to the processing but also that the first level of information presents its essential characteristics. This accessibility requirement, as clarified by recital 39 of the GDPR, is recalled in particular in the guidelines on transparency. The G29 recommends in particular that "the first level/first modality includes details of the purpose of the processing, the identity of the controller and a description of the rights of the data subjects".

70. However, the Restricted Committee notes that the first level of information present on the site […], accessible from the "personal data" link, did not provide this essential information but only some general information such as the possibility , for the persons concerned, to "consult the personal data which concern [them]" or to "exercise the various rights" from which they benefit, or one of the purposes of the processing (the presentation of personalized offers).

71. Concerning people joining the loyalty program through the paper form, the Restricted Committee considers that, by referring these people to the site […] without further details, the company did not make the information easily accessible. The company should have, at the very least, specified the page or the URL address at which this information was available. The Restricted Committee notes that this lack of accessibility by a simple reference to the home page of the site was aggravated by the defects previously underlined concerning the site […].

72. Secondly, the rapporteur considers that the information provided was not written in clear and simple terms.

73. It considers that all the information notices (in the general conditions of use of the site […], the paper forms for joining the loyalty program and for joining the same program via the customer area of □□the site […]) used imprecise and unclear terms ar were not easily understandable due to their layout.

74. On this point, the company highlights the significant changes made to the information notices prior to the opening of the sanction procedure. It indicates that, from November 2019, it has put online an information page specific to the protection of personal data, separate from the general conditions of use, accessible directly from the home page by a hypertext link.

75. The Restricted Committee notes that the information notices present on the site […] (both in the general conditions of use and in the process of joining the loyalty program) and on the paper registration forms included, at time of review on May 24, 2019, unclear, ambiguous, or imprecise formulations. The use, almost systematically in particular in the general conditions of use of the site […] and the loyalty program, of terms such as "these processing operations include in particular", "for one or more of the following reasons" or " your data is likely to be used "does not allow the persons concerned to fully understand the processing carried out. Similarly, formulas such as "

76. The general conditions of use of the site […] and of the loyalty program only included, in the majority of cases, only examples relating to the data collected ("we may possibly have data from open Data"), to the operations carried out or the purposes pursued (“your data may be subject to processing for one or more of the following reasons”), or general and evasive formulations. However, the Restricted Committee recalls that recital 39 of the GDPR emphasizes the importance of the principle of transparency, specifying that "natural persons should be informed of the risks, rules, guarantees and rights associated with the processing of personal data and the methods of exercising their rights in relation to such processing.” The Restricted Committee recalls that the information communicated is of capital importance, since its compliance conditions the validity of the person's commitment and his or her willingness to allow the processing of personal data by a specific data controller. The data subject should be able, on reading the information communicated to him, to understand the general scope of the processing, which is not the case here.

77. The formulations used, often unnecessarily complicated, made reading the information notices particularly tedious, even for an informed person. For example, a sentence such as "you can request to exercise your right of opposition for reasons relating to your particular situation, to the processing of personal data concerning you when the processing is based on the legitimate interest of the data controller including profiling" extracted from the general conditions of the site [...] does not allow a lay user to understand neither the existence, nor the scope, nor the conditions for exercising his right of opposition. The same applies to the sentence "your data may be transmitted to all or some of the following recipients: […] partner brands,

78. The Restricted Committee recalls that the information presented was intended for all users of the company's services, who may have very diverse profiles. The company should have adopted a style allowing to be understood by the greatest number. The Restricted Committee considers that this was not the case in this case.

79. In general, the Restricted Committee points out that the information notices must endeavor, as far as possible, to use

simple vocabulary, make short sentences and use a direct style, but also avoid terms legal or technical, abstract or ambiguous terms and formulas such as "we could use your data", "a possible use of your data", "some data concerning you is used", etc.

80. Moreover, the Restricted Committee notes that, despite the very large amount of information communicated, it was neither hierarchical nor orderly. The information took the form of a long list covering the various points of the Rules. It considers that such a presentation does not allow data subjects to easily find the information it is looking for, forcing it to read all the information notices. It therefore considers that the presentation used did not comply with the accessibility requirement laid down in Article 12 of the Regulation, clarified by the guidelines on transparency already cited.

81. The Restricted Committee notes that the combination of Articles 12 and 13 of the Regulation requires the data controller to provide information that is both complete and easily understandable. This balance can be difficult to achieve when, as in this case, the data processed, the purposes pursued and the retention periods are numerous and different. However, it considers that the quality of the information provided is central to the decision of the persons concerned to enter into a commercial relationship. In this respect, the Restricted Committee considers that the company should have paid very particular attention to the information communicated and achieved, even before the checks carried out, a result that was more understandable for people.

2. With regard to the content of the information

82. The rapporteur considers that the information communicated to people is incomplete on several counts.

83. Firstly, it indicates that the data controller is not correctly identified on the site […].

84. Secondly, the rapporteur underlines that the legal basis of the processing is not indicated since the company is content to indicate that the personal data can be processed due to the consent of the user, the execution of the contract or the legitimate interest of the data controller, without further details.

85. Thirdly, the rapporteur considers that the information relating to the countries where the data can be transferred is not complete, the guarantees surrounding the transfer not being specified, as well as the means of obtaining a copy of these guarantees.

86. Fourthly, he considers that individuals are not informed, for all of their data, of the duration for which they may be kept.

87. On all of these points, the company indicated that it had made changes before and after the notification of the report and aimed at bringing it into compliance. It argues that it provided, on the day of the checks, complete information on several

points, and in particular the contact details of its data protection officer, the recipients of the data, the existence of rights. On the points where it acknowledges the insufficiency of the information it provided, it indicates that it has modified its information notices in accordance with the requests of the rapporteur during the procedure, in particular as regards the identity of the data controller, the purposes and legal bases for the processing carried out, the retention periods and the transfer of personal data outside the European Union.

88. On the first point, it appears from the findings of the delegation of control that the company […] was indicated as being responsible for the processing implemented through the site […]. The companies […], […], […], […] and […] were designated in the information notices as joint controllers for the loyalty program.

89. The Restricted Committee considers, on the first point, that the responsibility for the processing implemented from the site […] lies with the company […], which alone determines the marketing policy common to all store formats in France . This interpretation is in line with the analysis of the company […], which also considers itself data controller as it indicated to the delegation of control on May 28, 2019.

90. Consequently, the Restricted Committee considers that the statements made on the site […] and in the general conditions of use of the card […] were incorrect.

91. On the second point, the Restricted Committee recalls that data subjects must be informed of the legal basis of the processing(s) implemented. This requirement cannot be satisfied by the sole reference made to the existing legal bases when several processing operations are implemented. In this case, people are not informed of the legal basis applicable to each of the processing operations carried out.

92. The Restricted Committee considers that the indication of the legal basis applicable to each processing operation is of particular importance. On the one hand, it allows the person concerned to have an overall assessment of the processing carried out, in particular its origin. It must therefore be able to know whether the data processed is on the basis of the consent it has given (and which it could therefore withdraw), or under the terms of a contract it has entered into with the data controller. processing, a legal obligation of the latter or its legitimate interest. On the other hand, and above all, the applicable legal basis can have direct consequences on the rights of individuals. For example, Article 20 of the GDPR provides that the right to data portability applies when the processing is based on consent.

93. Due to the absence of such details, the Restricted Committee considers that the information given on the site […] was

incomplete.

94. On the third point, the Restricted Committee emphasizes that Article 13 of the Regulation requires, in its point 1.f), that the data controller informs the data subject of "the existence or absence of a decision of adequacy issued by the Commission or, in the case of transfers referred to in Article 46 or 47, or in the second subparagraph of Article 49(1), the reference to the appropriate or suitable guarantees and the means of obtaining them a copy or the place where they have been made available".

95. The Restricted Committee finds that this information was not communicated to the persons concerned at the time of the findings made by the supervisory delegation. The Restricted Committee considers that the information given on the site […] was incomplete.

96. On the fourth point, the Restricted Committee notes that Article 13-2-a) of the Regulation requires that individuals be informed of "the retention period of personal data or, where this is not possible, the criteria used to determine this duration". The Transparency Guidelines, which shed light on the provisions of Article 13, specify that “the retention period (or the criteria for determining it) […] should be formulated in such a way that the data subject can assess […] ] what will be the retention period in the case of specific data or in the event of specific purposes". The Restricted Committee notes that the information notices did not indicate the retention periods (or the criteria used to establish it) in a systematic way for all the data or purposes, in particular browsing data or data relating to purchases made. As a result, people could not estimate, for a lot of data, the retention periods established by the data controller.

97. Due to the absence of such details, the Restricted Committee considers that the information given on the site […] was incomplete.

98. It emerges from all of these elements that the information communicated to people through the site […] and through the paper membership forms for the loyalty program was not easily accessible and was incomplete. The Restricted Committee therefore considers that a breach of Articles 12 and 13 of the GDPR has been constituted.

99. It nevertheless underlines the important compliance work carried out by the company with regard to the information notices present on its website and on its paper bulletins. It notes that the company's new practices are, on the day of the meeting, in compliance with the Regulations. The company now demonstrates clear, transparent, easily accessible and complete information on all of its media.

D. On the breach relating to the right of access

100. Article 15 of the GDPR provides that data subjects have the right to obtain from the controller confirmation that personal data concerning them are being processed as well as a certain amount of information, including any information available as to at the origin of the data, when these are not collected directly by the data controller (article 15-1-g).

101. In referral no x of January 21, 2019, Mr […] explained that he had received an electronic prospecting letter on November 8, 2018 without having communicated his contact details to the […] group in the past. He indicated that he had asked the same day for the origin of the personal data concerning him held by the company. On November 15, 2018, the company replied to him in order to obtain a copy of the complainant's identity document, which was communicated to the data controller on November 21. Mr […] explained that, despite several reminders on January 4 and 18, 2019, no response was given to his request, only his opposition to receiving prospecting having been taken into account.

102. It appears from the findings made on 12 June 2019 that this complainant was a former customer of the company […], whose site was subsequently integrated into the site […].

103. The company […] acknowledges that it did not initially inform the complainant of the origin of the data it held concerning him, considering that it was processing this personal data in the context of direct collection, and not indirect, and that the origin of the data is among the information to be communicated on the basis of Article 15 of the Regulation only in the event of indirect collection of personal data.

104. On this point, the Restricted Committee notes that the complainant had previously created an account on the website […]. It was on this occasion that the personal data concerning him had been collected by the company […]. The Restricted Committee considers that the subsequent merger between the website […] and the site […] does not give the company […] the status of primary collector of personal data. Indeed, the personal data were transmitted to the company […] by the company […], which corresponds to the case of an indirect collection, the data not having been collected by […] from the concerned person. Therefore, the Restricted Committee considers that […] was required to inform the complainant of the origin of the data as part of his request for access, in accordance with Article 15-1-g) of the GDPR.

105. The Restricted Committee recalls that the fact that the complainant was informed of the merger between the site […] and the site […] prior to his request to the company did not exempt the data controller from his obligation to inform on the origin of the data, formulated by the plaintiff within the framework of the exercise of his rights.

106. It follows from these elements that a breach of Article 15 of the Rules has been established.

107. The Restricted Committee nevertheless points out that the company granted the complainant's request on June 19, 2019, after the inspection was carried out but before the initiation of the sanction procedure, and that the breach was therefore no longer constituted on the day of the session.

E. On the breach relating to the right to erasure

108. Article 17 of the Regulation defines the conditions under which data subjects have the right to the erasure of their personal data. Article 17-1-c), in particular, offers this right when the data is no longer necessary with regard to the purposes of the processing or when the person opposes the processing implemented for prospecting purposes.

109. The Commission has received several complaints relating to the difficulties encountered in the exercise of this right.

110. By referral No. X of June 8, 2018, Mr. […] seized the CNIL, explaining that he had requested the erasure of his data without obtaining a favorable response to his request, which related in particular to the erasure of his email address. email, used by the company for commercial prospecting purposes.

111. The findings made during the inspection of June 12, 2019 revealed the presence of the complainant's email address in the company's databases.

112. In defence, the company explained that the electronic address serves as the entry key to the database in question and that it cannot therefore be deleted. She further indicated that the situation did not entail any prejudice for the complainant, his opposition to prospecting having been taken into account.

113. The Restricted Committee emphasizes first of all that Mr. […]'s request for erasure of May 28, 2018 was broad and explicit: "I ask you to delete all the data that you may have on me. This data will be attached at […]@[…].com."

114. The Restricted Committee observes that the company has chosen to use as the entry key to its database the electronic address of individuals, therefore personal data. This purely practical decision, without the retention of the data in question being justified by any legitimate purpose with regard to the elements of the file, cannot allow it to be exempted from its obligations in terms of exercising rights. The Restricted Committee considers that Mr […] could legitimately, on the basis of Article 17-1 c) of the Regulation, demand the erasure of his data used for commercial prospecting purposes and it was therefore up to the company to to grant this request and to set up a system for organizing its database which did not infringe this right. In this case,

115. The Restricted Committee nevertheless observes that the company modified the architecture of its databases after the notification of the sanction report. The new mode of operation no longer uses personal data as the entry key to the database, and Mr […]'s request has been granted.

116. By referral no x of July 7, 2018, Mrs […] contacted the CNIL, explaining that she had asked the company to erase all personal data concerning her without obtaining a favorable response to her request.

117. The findings made during the inspection revealed the presence of the complainant's surname, first name, date of birth and mobile telephone number in the company's databases.

118. In defence, the company explained that the presence of this data was the result of a one-time error and that it had no consequences for the complainant, her opposition to receiving commercial prospecting having been taken into account.

119. The Restricted Committee considers that Mrs […] could legitimately, on the basis of Article 17-1 c) of the Regulation, demand the erasure of her data used for commercial prospecting purposes. A breach of section 17 of the Regulations is therefore constituted.

120. The Restricted Committee nevertheless notes that the company granted Ms. […]'s request on May 12, 2020.

121. By referral No. X of January 19, 2019, Mr […] contacted the CNIL, explaining that he had twice requested the erasure of his data and nevertheless continued to receive commercial prospecting.

122. The observations made during the inspection revealed the presence of the complainant's surname, first name, date of birth and postal and electronic addresses in the company's databases.

123. The company explains that the data recorded was not integrated into a database used for commercial prospecting. It argues that, in the event of an opposition to prospecting, it grants this request but does not erase the data from the databases that are not dedicated to prospecting.

124. The Restricted Committee notes that Mr. […]'s request, relating to the cessation of commercial prospecting and the deletion of data, was devoid of any ambiguity. In a first email sent to the company, the complainant explained "I wishes to obtain the closing of my account thus in accordance with articles 38 and following of the law "computing and freedoms" of January 6, 1978 modified, I thank you for deleting all of my personal data attached to this account ". In a second letter, he specified "" Thus, I reiterate my request: in application of articles 21.1 and 17.1.c of the General Data Protection Regulations (GDPR), thank you for deleting the personal data concerning me on the sites following: […] and […]". Mr. […] being entitled to

request such deletion on the basis of Article 17-1 c), it was up to the company, unless the latter justified its keeping the data for a legitimate purpose, to grant this request. . A violation of section 17 of the Regulations is therefore constituted.

125. The Restricted Committee nevertheless notes that, while contesting the rapporteur's assessment, the company granted Mr. […]'s request by deleting all the data concerning him.

126. By referral No. X of April 6, 2019, Mr. […] seized the CNIL, explaining that he had asked the company to erase his postal address without obtaining a favorable response to his request.

127. The observations made during the inspection revealed the presence of the complainant's surname, first name, date of birth, fixed and mobile telephone numbers and postal and electronic addresses in the company's databases.

128. The company explains that the presence of the complainant's postal address resulted from a one-off error and had no consequences, his opposition to receiving commercial prospecting having been taken into account.

129. The Restricted Committee considers that Mr […] could legitimately, on the basis of Article 17-1 c) of the Regulation, demand the erasure of his data. A breach of section 17 of the Regulations is therefore constituted.

130. The Restricted Committee nevertheless notes that the company rectified its error as soon as it was informed of it, following the inspection carried out on June 11, 2019.

131. In conclusion on these shortcomings, the Restricted Committee considers that if, after a request for erasure, certain personal data of customers may be retained, in particular under legal obligations or for evidentiary purposes or when the company has a compelling legitimate reason, personal data not necessary for compliance with these other obligations or purposes must be deleted after the exercise of this right as soon as the conditions set out in Article 17 of the GDPR are met. It notes in this regard that such was the case for the processing for the purpose of canvassing and that it does not appear from the elements of the procedure that the retention of the data in question was legitimate on another basis.

132. Moreover, the Restricted Committee recalls that the data controller has an obligation to approach the data subject when he considers that the requests he receives do not include all the elements allowing him to carry out the operations which he are requested (article 142 of 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, formerly article 94 of decree no. 2005 -1309 of October 20, 2005). Therefore, the Restricted Committee considers that, if the company […] considered that the deletion requests were too broad and that it could not grant them on the basis of a higher legitimate interest or because the deletion was not possible on the

basis of Article 17 of the GDPR,

133. Consequently, in each of the aforementioned cases, the company has not complied with its obligations resulting from article 17 of the Regulation and that a breach has been established.

F. On the breach relating to the right of opposition to the processing of personal data for commercial prospecting purposes

134. The second paragraph of Article 21 of the Regulation provides that "when personal data is processed for prospecting purposes, the data subject has the right to object at any time to the processing of personal data. regarding for such prospecting purposes".

135. By referral No. X of October 1, 2018, Mr. […] seized the CNIL, explaining that he had continued to receive advertising SMS from the company despite a previously expressed opposition to the processing of his personal data for the purposes of business development.

136. The findings made during the inspection of June 11, 2019 revealed that the complainant's opposition had not been transcribed into the company's databases, thus not allowing it to be effectively taken into account.

137. The company explains that this one-off error is due to a shortcoming on the part of its service provider, who had not sent it the opposition in question.

138. The Restricted Committee notes that it is clear from the findings made during the inspection, such as the documents communicated by the company, that the service provider […] communicates to the company the objections expressed by the people “as it happens”. These transmissions are also compiled during a monthly sending, only taken into account by the company to transcribe the objections in the database, as it indicated in the context of the procedure. It appears from the documents communicated by the company during the procedure that Mr. […]'s opposition had not been transmitted in a compiled dispatch on the day of the inspection, June 11, 2019. However, the Restricted Committee underlines that the company had received this opposition within the framework of the transmission "over the water" and that it should therefore have ceased all commercial prospecting towards the plaintiff. In any event, the delegation noted that this objection had not been taken into account on the day of the inspection.

139. Consequently, a breach of Article 21 of the Rules is established.

140. The Restricted Committee nevertheless notes that this error was corrected by the company during the inspection carried out on June 11, 2019. It emphasizes above all that the company has deployed significant resources to thoroughly review the

impact of the objections expressed by SMS in its databases in this procedure. It notes that objections are now directly received, processed and transcribed into the database, ensuring better respect for rights.

141. By referral No. X of November 22, 2018, Mr. […] seized the CNIL, explaining that he had continued to receive advertising SMS from the company despite several objections previously expressed.

142. The observations made during the inspection revealed that the complainant's opposition had not been transcribed into the company's databases.

143. The company explains that this absence of transcription results from an internal human error.

144. The Restricted Committee therefore considers that the company had not complied with its obligations resulting from Article 21 of the Regulation.

145. It nevertheless notes that the complainant's opposition was taken into account and transcribed into the database during the check carried out on June 11, 2019.

146. In conclusion on these breaches, the Restricted Committee considers that in each of the aforementioned cases, the company did not comply with its obligations resulting from Article 21 of the Rules and that a breach was characterized on the day of the inspection when , although it had offered data subjects a means of exercising their right to object, this was not systematically taken into account. However, it points out that all of the complaints were handled by the company during the course of the procedure, either immediately during the checks or following its discussions with the rapporteur.

G. On the breach relating to the right of opposition to prospecting by electronic means

147. The first paragraph of Article L34-5 of the Postal and Electronic Communications Code provides that "direct prospecting by means of an automated electronic communications system within the meaning of 6° of Article L. 32 is prohibited, a fax or e-mails using the contact details of a natural person, subscriber or user, who has not previously expressed his consent to receive direct prospecting by this means." The fourth paragraph of the same article, however, makes an exception to this principle of prohibition "if the contact details of the recipient have been collected from him, in compliance with the provisions of law no. 78-17 of 6 January 1978 relating to data processing, files and freedoms, to the occasion of a sale ora provision of services, if the direct marketing concerns similar products or services provided by the same natural or legal person, and if the recipient is offered, in an express and unambiguous manner, the possibility of opposing, free of charge , except those linked to the transmission of the refusal, and in a simple way, to the use of his contact details at the time they are collected and each

time a prospecting e-mail is sent to him in the event that he would not have refused from the outset such exploitation".apart from those related to the transmission of the refusal, and in a simple way, to the use of his contact details at the time they are collected and each time a prospecting e-mail is sent to him in the event that he would not have refused to immediately such exploitation".apart from those related to the transmission of the refusal, and in a simple way, to the use of his contact details at the time they are collected and each time a prospecting e-mail is sent to him in the event that he would not have refused to immediately such exploitation".

148. By referral No. X of January 4, 2019, Mr. […] seized the CNIL, explaining that he had received commercial prospecting without the email allowing him to oppose it. Indeed, the unsubscribe link from the mailing list sent him, to be able to object, to a page for connecting to a customer account. However, the complainant did not have such an account, and therefore could not object to commercial prospecting.

149. The rapporteur considers that the company failed in its obligations arising from article L34-5 of the postal and electronic communications code since it did not systematically offer the recipients of its prospecting emails a simple means and effective unsubscribe in the emails in question.

150. The company acknowledges this error but considers that a breach cannot be characterized from this single occurrence.

151. It appears from the explanations provided by the company during the inspection carried out on July 11, 2019 that such an error actually occurred in a prospecting email sent to more than 350,000 people. The company indicates that the unsubscribe link included in the prospecting e-mail referred to the personal space of the site […] allowing people with a customer account to unsubscribe. By mistake, people without a customer account were targeted by this prospecting campaign. When these people clicked on the unsubscribe link, they were asked, in order to be able to unsubscribe, to log into a customer account which they did not have.

152. The company explains that it immediately spotted the error because it received a large number of complaints from customers who could not properly exercise their rights. She therefore asserts that this error only occurred once, since she did not receive any other similar complaints.

153. The Restricted Committee considers that people who do not have a customer account could not simply object to the use of their personal data for commercial prospecting purposes. Consequently, a breach of article L34-5 of the postal and electronic communications code is established when no means of opposing prospecting by electronic means has been offered

to these persons.

154. The Restricted Committee nevertheless notes that the company has set up a unique unsubscribe link that does not require going through the customer account to unsubscribe. Therefore, it considers that the company has implemented the necessary measures to ensure that the rights of individuals are respected in the future.

H. On the breach relating to the security of personal data

155. Article 32 of the GDPR provides that "the controller and the processor shall implement appropriate technical and organizational measures to guarantee a level of security appropriate to the risk".

156. The rapporteur criticizes the company for not having put in place the necessary measures to protect the personal data it processes after becoming aware of the existence of a vulnerability on its website.

157. It appears from the company's statements made during the inspection of July 11, 2019 that, during a purchase on the site […], an invoice is made available to the customer on his personal space after the delivery of the order or in-store pickup. This invoice is accessible via a fixed URL address. Anyone with this address can access the invoice issued without having to authenticate and connect to their customer area.

158. The company identified this technical vulnerability on November 16, 2018, recorded in the security incident log under number 415342. To mitigate this vulnerability, the company decided to develop two measures: the addition of a chain of random characters and a mandatory pre-authentication mechanism. The first measure was to, by increasing the number of potential URL addresses, reduce the risk of an incremental deduction of the address allowing access to the invoices. The second measure completely prevented access to the invoices by anyone other than the data subject.

159. The first measure was implemented very quickly by the company. On the day of the inspection, ie almost eight months after the discovery of the vulnerability, the second measure had still not been deployed, and access to an invoice remained possible for anyone with its URL address.

160. On this point, the company indicates that it had already deployed, on the day of the inspection, a sufficient first measure significantly reducing the risk of access to the documents, and that the second measure was in the process of being deployed.

161. The Restricted Committee considers that the addition of a random character string is not sufficient, on its own, to prevent improper access to the personal data of third parties. This measure makes it possible to reduce the risk but does not make it disappear, access remaining possible. It recalls that the National Information Systems Security Agency (ANSSI) has been

warning since 2013 about this vulnerability linked to URL addresses, even "in the case of URLs composed of several dozen perfectly random characters" (Recommendations for the Securing Websites, August 13, 2013, p. 16). The Restricted Committee points out that the company had identified the appropriate measure to be put in place in November 2018 since it had planned, from that date, the deployment of mandatory prior authentication.

162. Consequently, the Restricted Committee considers that the lack of implementation of the mandatory prior authentication following the discovery of the vulnerability – whereas this measure had been identified and is the only measure allowing completely preventing the risk – constitutes a breach of section 32 of the Regulations.

163. The Restricted Committee notes, however, that the company implemented mandatory authentication on July 17, 2019.

I. On the failure to notify personal data breaches

164. Article 33 of the Regulation provides that "in the event of a breach of personal data, the controller shall notify the breach in question to the competent supervisory authority in accordance with Article 55, as soon as possible and, if possible, 72 hours at the latest after becoming aware of it, unless the violation in question is not likely to create a risk for the rights and freedoms of natural persons".

165. The rapporteur considers that the company failed in its obligation to notify personal data breaches, this obligation being apparent from the circumstances of the breach and the data concerned.

166. It appears from the findings made during the inspection of July 11, 2019 that the company identified and recorded a computer attack of which it had been the victim on July 1, 2019. This attack, using the authentication service of the group's mobile application , took the form of 800,000 login attempts from 10,000 IP addresses. It resulted in 4,000 successful authentications and 275 effective accesses to customer accounts. This violation was not notified to the CNIL.

167. In defence, the company indicated that the violation was unlikely to pose a risk to the rights and freedoms of individuals. It also specifies that the persons concerned did not suffer any financial loss since no loyalty points were subtracted. It emphasizes that in any event, the general conditions of use of the card […] provide for the reimbursement of the kitties of the persons concerned in the event of an attack by third parties.

168. The Restricted Committee recalls that in the event of a breach of personal data, the principle is that of notification to the supervisory authority. The absence of notification is only possible by exception, when the violation is not likely to create a risk for the rights and freedoms of individuals. In the present case, the Restricted Committee considers that the analysis of the risks

linked to this violation does not lead to the application of this exception to the notification obligation. Indeed, the seriousness of the breach stems from the obviously malicious origin of this attack,

169. The Restricted Committee notes that the 4,000 accounts for which no effective access was observed but which were the subject of successful authentication must be regarded as participating in the risk assessment. Indeed, the Restricted Committee recalls that many people use an identical combination of email address and password on a very large number of websites. There was therefore a serious risk that attackers having identified a "valid" email address/password pair would try to reuse it on other websites (a technique called credential stuffing). There was also a risk that, now having more information on the persons concerned and their relations with the companies of the group […], attackers attempt to impersonate one of these companies in malicious and misleading emails (phishing). These accounts must therefore be considered to be affected by the breach.

170. Consequently, the Restricted Committee considers that a breach of Article 33 of the GDPR has been constituted.

171. It nevertheless underlines that, despite a difference of assessment with the rapporteur and with the aim of compliance, the company notified the violation to the CNIL on July 19, 2020 and was thus in compliance on the day of the meeting.

J. On the breach relating to cookies

172. Article 82 of the Data Protection Act (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 for information already stored in his equipment. Any deposit of cookies or other tracers must therefore be preceded by the information and consent of the persons. 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".

173. The rapporteur considers that the company did not comply with these provisions since it appears from the online check of 24 May 2019 that on arriving at the website […] several cookies not falling into the two cases mentioned above were deposited on the user's terminal as soon as they connect to the site's home page and before any action on their part.

174. The company does not contest these elements.

175. The Restricted Committee notes that in this case, the deposit of thirty-nine cookies was automatic upon arrival on the home page of the site, and before any action by the user. Of these thirty-nine cookies, three belonged to the Google Analytics

solution (“_gid”, “_ga” and “_gat_gtag_UA_3928615_46” cookies).

176. With regard to these three cookies, known as Google analytics, the Restricted Committee stresses that it is not in dispute that the data collected by these cookies may be cross-checked with data from other processing operations to pursue different purposes than those limitedly provided for by article 82 of the law "computing and freedoms", 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 are translating into conversions, then quickly adjust creatives and bids accordingly.

177. Consequently, these cookies are not exclusively intended to allow or facilitate communication by electronic means and are not strictly necessary for the provision of the service. Their filing should therefore have required the company to first obtain the consent of users.

178. The Restricted Committee therefore considers that a breach of Article 82 of Law No. 78-17 of 6 January 1978 has been constituted. It also considers that this failure affected a large number of people, namely all visitors to the site […].

179. The Restricted Committee nevertheless points out that the company made significant changes to its website during the sanction procedure. These modifications led, in particular, to the stopping of the automatic deposit of cookies on arrival on the home page of the site since February 5, 2020.

III. On corrective measures and publicity

180. Under the terms of III of article 20 of the law of January 6, 1978:

"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. "

181. 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. "

182. On injunctions and compliance, the Restricted Committee stresses that the company corrected all of the shortcomings noted in the sanction report during the procedure. Its compliance having been demonstrated to date, the Restricted Committee considers that no injunction is justified.

183. On the imposition of a fine and its amount, the Restricted Committee considers that, in the present case, the aforementioned breaches justify the imposition of an administrative fine against the company.

184. With regard to the fine proposed by the rapporteur, the company first argues that the amount of the proposed fine is excessive, several breaches being, in its view, not established. On this point, the Restricted Committee considers that all of the shortcomings noted by the rapporteur are specific to the present case, as it detailed previously in the reasons for the decision.

185. The company then argues that the mitigating factors set out in Article 83 of the Rules should lead to a reduction in the amount proposed by the rapporteur and that the significant compliance work carried out should be taken into account.

186. The Restricted Committee analyzes the criteria established by Article 83 as follows.

187. With regard to the nature, gravity and duration of the violation, it considers that this criterion is particularly characterized for several breaches, in particular those relating to the retention periods of personal data, the procedures for exercising and the deposit of cookies. With regard to the breach relating to the right to erasure and opposition to canvassing, the Restricted Committee notes the residual nature of these cases in view of the large number of erasure requests that the data controller has faced since the entry into force of the GDPR. She stresses that the number of complaints received by the Commission is limited and results, each time, from isolated failings. It recognizes the changes made by the company to comply on this point as well as to internalize the consideration of the opposition of people and improve the processing of requests and respect for rights. With regard to the breach relating to data security, the Restricted Committee considers that the seriousness of this breach is mitigated by the rapid implementation of measures partially limiting the occurrence of the risk. Finally, with regard to the opposition to prospecting by electronic means, the Restricted Committee notes that the incident was occasional. Regarding the number of people concerned, this criterion is particularly aggravating for the breach relating to the duration of data retention, which concerned several million people, for information, since each person who joined the loyalty program or created an account on the site […] was concerned, and for the breach relating to cookies, since cookies were placed without consent on the terminal of the 1.7 million unique visitors of the site. This criterion is, on the other hand, attenuated with regard to the difficulties encountered when exercising the right of access (three persons concerned), the right to erasure of data (four

persons concerned), the right of opposition (two data subjects) and opposition to electronic prospecting (350 data subjects out of the 350,000 people targeted by the campaign). Of all the breaches, the Restricted Committee considers the level of damage suffered as insignificant. and for the breach relating to cookies, since cookies were placed without consent on the terminal of the 1.7 million unique visitors to the site. This criterion is, on the other hand, attenuated with regard to the difficulties encountered when exercising the right of access (three persons concerned), the right to erasure of data (four persons concerned), the right of opposition (two data subjects) and opposition to electronic prospecting (350 data subjects out of the 350,000 people targeted by the campaign). Of all the breaches, the Restricted Committee considers the level of damage suffered as insignificant. and for the breach relating to cookies, since cookies were placed without consent on the terminal of the 1.7 million unique visitors to the site. This criterion is, on the other hand, attenuated with regard to the difficulties encountered when exercising the right of access (three persons concerned), the right to erasure of data (four persons concerned), the right of opposition (two data subjects) and opposition to electronic prospecting (350 data subjects out of the 350,000 people targeted by the campaign). Of all the breaches, the Restricted Committee considers the level of damage suffered as insignificant. on the other hand mitigating with regard to the difficulties encountered when exercising the right of access (three persons concerned), the right to erasure of data (four persons concerned), the right of opposition (two persons concerned) and opposition to electronic canvassing (350 people concerned out of the 350,000 people targeted by the campaign). Of all the breaches, the Restricted Committee considers the level of damage suffered as insignificant. on the other hand mitigating with regard to the difficulties encountered when exercising the right of access (three persons concerned), the right to erasure of data (four persons concerned), the right of opposition (two persons concerned) and opposition to electronic canvassing (350 people concerned out of the 350,000 people targeted by the campaign). Of all the breaches, the Restricted Committee considers the level of damage suffered as insignificant.

188. The Restricted Committee notes that most breaches result from negligence, occasional errors or a lack of anticipation of the consequences of the entry into application of the Regulation.

189. With regard to the measures taken by the controller to mitigate the damage suffered by the persons concerned, 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 all of the shortcomings have been corrected to date.

190. With regard to the degree of cooperation with the supervisory authority, the restricted committee notes the perfect cooperation of the company, both in facilitating the CNIL's investigations and in taking into account, even before the committee's decision limited, of the rapporteur's observations. It also notes that the company complied with the rapporteur's legal analysis of all the shortcomings noted, even in cases where a difference of opinion remained.

191. With regard to the categories of personal data concerned, the Restricted Committee notes that no sensitive data was concerned by the processing.

192. With regard to the manner in which the supervisory authority became aware of the violation, the Restricted Committee notes that complaints are, for a number of shortcomings, at the origin of its action.

193. With regard to the benefits derived from the breaches, the Restricted Committee considers that the company did not derive any financial benefit from them. It demonstrated in particular that, even when the data retention periods were exceeded, they could not be used for prospecting purposes. It has also committed substantial financial resources to ensure compliance during the sanction procedure.

194. In conclusion, the Restricted Committee notes the number and seriousness of breaches of certain essential obligations of a data controller, such as information or respect for the rights of individuals. It also notes that certain shortcomings were structural. This was the case, for example, of the under-sizing of the means employed to respond to requests for the exercise of rights, resulting in a recurring manner in abnormally long response times without the persons being informed of the processing of their request, or the delay caught in the purging of personal data whose retention period had expired. On these points, the restricted committee also underlines the particularly large number of people concerned with regard to the several tens of millions of customers whose personal data appear in the company's databases. Finally, the Restricted Committee notes that the shortcomings were brought to its attention due to a large number of complaints received by the CNIL concerning this data controller. This large volume of complaints is also at the origin of the decision to initiate an inspection against this company.

195. Consequently, the Restricted Committee considers that a fine should be imposed.

196. On the basis of the fine, the company also disputes the method of calculating the basis of the penalty.

197. On this point, the Restricted Committee recalls that Article 83-5 of the Regulation provides that the amount of the fines pronounced for the breaches found may amount "in the case of a company, up to 4% of the turnover total global annual

revenue for the previous fiscal year". It points out that recital 150 of the Regulation specifies that "when administrative fines are imposed on an undertaking, this term must, for this purpose, be understood as an undertaking in accordance with Articles 101 and 102 of the Treaty on the Functioning of the European Union ". The Restricted Committee therefore considers that the Regulation makes a direct and explicit reference, in the specific context of determining the amount of fines, competition law covered by Articles 101 and 102 of the Treaty on the Functioning of the European Union (hereinafter "the TFEU"). The Restricted Committee recalls that the guidelines on the application and setting of administrative fines for the purposes of Regulation 2016/679, adopted on 3 October 2017 by the G29, specify in this regard that "in order to impose effective, proportionate and dissuasive fines , the supervisory authorities will rely on the definition of the concept of business provided by the CJEU for the purposes of applying Articles 101 and 102 of the FEU Treaty, namely that the concept of business must be understood as an economic unit which may be formed by the parent company and all the subsidiaries concerned In accordance with Union law and case law, an enterprise should be understood as the economic unit engaged in commercial or economic activities, regardless of the legal person involved (recital 150). "

198. The Restricted Committee considers that the subsidiaries owned by the company […] and benefiting from the processing must be considered to be concerned within the meaning of the aforementioned guidelines. Indeed, in the context of competition law to which recital 150 of the Regulation refers directly, an undertaking "must be understood as designating an economic unit even if, from a legal point of view, this economic unit is made up of several natural persons or morals" (judgment of 12 July 1984, Hydrotherm, 170/83, Rec. p. 2999, point 11, repeated in the judgment Confederación Española de Empresarios de Estaciones de Servicio, ECLI:EU:C:2006:784, point 40).

199. The Restricted Committee also recalls that the fines imposed must be dissuasive. With regard to this requirement, it has been held that "attribution of liability to the economic successor is justified for the purposes of the effective implementation of the competition rules. Indeed, if the Commission did not have such , it would be easy for companies to be able to escape sanctions by restructuring, transfers or other legal or organizational changes.The objective of repressing behavior contrary to the rules of competition and preventing its renewal by of dissuasive sanctions would thus be compromised" (judgment of the Trib. UE, 29 February 2016, Schenker v European Commission, case T-265/12, point 193).

200. The Restricted Committee considers that the legal organization of the group, and in particular of the company […] and its subsidiaries, would de facto render ineffective any fine imposed solely on the turnover of the company […] . The Restricted

Committee recalls that the company […] achieved, in 2019, a turnover of approximately 14 million euros and a net loss of 1.6 billion euros. These figures were of the same order in 2018 (turnover of around 25 million euros and net loss of 1.4 billion euros). […] however belongs to a group whose economic activity is of a completely different order of magnitude, presenting a turnover of approximately 80 billion euros (approximately 40 billion euros in France) for a result net adjusted, group share, profit of approximately 900 million euros in 2019. Certain subsidiaries of the company […] achieve a particularly high turnover. For example, the company […] (81.73% owned by the company […]) achieved a turnover of 14.3 billion euros in 2019 and the company […] (99% owned by the company […]) achieved a turnover of 636 million euros in 2019.

201. Consequently, the Restricted Committee considers that, in order to assess the notion of undertaking in accordance with Articles 101 and 102 of the TFEU, account should be taken of the turnover achieved by the company […] and by the subsidiaries which it she holds and who have benefited from the treatments. It appears from the company's statements during the inspection carried out on May 28, 2019 that the companies […] and […] benefit from the data pooling program. The Marketing France department of the company […] processes the pooled data of the customers of these companies (surname, first name, physical and electronic address, telephone number, purchase history) in order to send them personalized advertisements for the products sold in these stores.

202. In conclusion, the Restricted Committee holds that the company's turnover, in the sense of economic unit, serving as the basis for calculating the basis of the fine amounts to 14.9 billion euros. euros in 2019.

203. The Restricted Committee nevertheless considers that the determination of the amount of the fine must take into account the specificity of the economic model of the sector concerned, that of large-scale distribution, characterized by a particularly high turnover with regard to the net results generated by activity, which is distinguished by extremely high volumes and low margins.

204. Consequently, it considers that a fine of €2,250,000 is justified and proportionate to the breaches noted and to the situation of the company […].

205. On the publicity of the decision, the company considers that the publicity of the sanction is not justified.

206. The Restricted Committee considers, firstly, that the seriousness of certain breaches justifies, in itself, the publication of this decision.

207. The Restricted Committee recalls, secondly, that the breaches relating to the retention period of data, the procedures for

exercising rights or the information provided concerned a very large number of people. It considers that publicizing its decision is the best way to inform people of the past existence of these breaches. It notes that people can only be aware of certain shortcomings (such as the one relating to the retention period) thanks to this publicity of its decision.

208. It follows from all of the foregoing and from consideration of the criteria set out in Article 83 of the Regulation that an administrative fine of €2,250,000 as well as an additional penalty 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 against the company […] an administrative fine in the amount of 2,250,000 (two million two hundred and fifty thousand) euros for breaches of articles 5-1 e), 12, 13, 15, 17 , 21, 32 and 33 of the GDPR, in Article L34-5 of the Post and Electronic Communications Code and in Article 82 (formerly 32.II) of the Data Protection Act;

• 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.