Draft decision of the restricted committee No. SAN-2022-017 of 3 August 2022 concerning ACCOR SA

The Commission nationale de l'Informatique et des Libertés (CNIL - French Data Protection Authority), met in its Restricted Committee consisting of Mr. Alexandre LINDEN, Chairman, Mr. Philippe-Pierre CABOURDIN, Vice Chairman, Ms. Christine MAUGÜÉ, Mr. Alain DRU and Mr. Bertrand du MARAIS, members;

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

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

Having regard to the French Post and Electronic Communications Code;

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

Having regard to Decree No. 2019-536 of 29 May 2019 implementing Act No. 78-17 of 6 January 1978 on data protection;

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

Having regard to referrals Nos. […];

Having regard to decision No. 2019-042C of 18 February 2019 of CNIL's Chair to instruct the general secretary to carry out or have a third party carry out an assignment to verify the processing implemented by the company ACCOR;

Having regard to the decision of CNIL's chair appointing a rapporteur before the restricted committee of 16 October 2020;

Having regard to the report of Mrs Sophie LAMBREMON, the commissioner rapporteur, notified to ACCOR on 24 November 2020;

Having regard to the written observations made by ACCOR on 22 December 2020;

Having regard to the other documents in the file;

Having regard to Decision 01/2022 on the dispute arisen on the draft decision of the French Supervisory Authority regarding Accor SA under Article 65(1)(a) GDPR ;

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

- Mrs Sophie LAMBREMON, Commissioner, heard in her report;

In the capacity of representatives of ACCOR:

[…]

ACCOR having last spoken;

The restricted committee adopted the following draft decision:

I. Facts and proceedings

1. ACCOR SA (hereinafter "the Company") is a public limited company with a board of directors established in 1960, specialising in the hospitality sector. Its registered office is located at 82, rue Henri Farman in Issy-les-Moulineaux (92130).

2. In 2021, the Company generated revenue of […] In the summer of 2020, 5,100 hotels, based in 110 countries, under 39 different brands, were operated under contracts between their owners and ACCOR (franchise or management contracts, principally). The Company employs approximately 1500 staff.

3. Between December 2018 and September 2019, the Commission nationale de l'Informatique et des Libertés (hereinafter "the CNIL" or "the Commission") was directly referred five complaints (referral Nos. […]) concerning the failure to take into account the right to object to the receipt by email of marketing messages (advertising emails, welcome emails for the loyalty programme, newsletters) from the Company. On 22 September 2019, the CNIL also received a complaint (referral No. […]) relating to the difficulties encountered in exercising the right of access, in particular to bank data collected by the Company in connection with the reservation of a hotel room.

4. In accordance with Article 56 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the “Regulation” or the “GDPR”), in the context of the handling of complaints received against the Company, on 12 December 2018, the CNIL informed all European supervisory authorities of its competence to act as lead supervisory authority regarding cross-border processing implemented by the Company, a competence derived by CNIL from the fact that the Company's main establishment is located in France.

5. Through the data protection authorities' exchange platform, the CNIL initiated the procedure allowing the supervisory authorities concerned to declare themselves. Ten authorities declared themselves involved in this procedure, within the meaning of Article 4 (22) GDPR.

6. At the same time, between January 2019 and February 2020, the CNIL received as the “leading authority”, in accordance with the cooperation mechanisms provided for by the Regulation, five other complaints from the supervisory authorities of Saarland, Spain, Ireland, Poland and Lower Saxony (referrals Nos. […]). These complaints also concerned requests for opposition to the processing of personal data for the purpose of marketing by e-mail and to the exercise of the right of access to data collected by ACCOR.

7. On 6 March 2019, pursuant to decision No. 2019-046C of 18 February 2019 of the CNIL’s Chair, a questionnaire was sent to ACCOR, to which it replied by letter dated 8 April and then by additional letters dated 22 May, 1 August, 11 October and 27 December 2019. The purpose of this documentary audit was to verify ACCOR's compliance with all the provisions of the

GDPR and Act No. 78-17 of 6 January 1978 relating to data processing, files and freedoms (hereinafter "the Act of 6 January 1978 amended" or the "French Data Protection Act").

8. Following this initial inspection, the CNIL, taking into account the Company's response to the letter of instruction sent to it and its compliance on several points, submitted to its European counterparts on 23 December 2019, pursuant to Article 60 GDPR, a draft decision of its Chair reminding the Company of its obligations, in accordance with the provisions of Article 58-2-b) GDPR.

9. This draft decision was the subject of relevant and reasoned objections by some of the authorities concerned within the meaning of Article 60 GDPR, requesting that the Company should not only be called to order but also be sanctioned with an administrative fine and pointing out, in particular, the number of breaches, the number of complaints and the size of the Company. In view of these objections and the new complaints received since the first inspection, the CNIL decided to resume its investigations with the Company.

10. On 11 February 2020, the CNIL delegation carried out an inspection at the Company's premises. An online check of the Company's website (www.all.accor.com) was then carried out on 24 February 2020, pursuant to the aforementioned Decision No 2019-046C. Following these investigations, the Company sent the CNIL additional information by letters dated 21 February, 10 March, 19 March and 7 August 2020.

11. In order to examine these items, the chair of the Commission appointed Sophie LAMBREMON as rapporteur on 16 October 2020, on the basis of Article 22 of the amended Act of 6 January 1978.

12. At the end of her investigation, on 24 November 2020, the rapporteur notified the Company of a report detailing the breaches of the provisions of Articles L. 34-5 of the French Post and Electronic Communications Code (hereinafter "CPCE") and 12-1, 12-3, 13, 15-1, 21-2 and 32 GDPR that she considered to have been committed in this case. That report also proposed the restricted committee to impose an administrative fine against the Company and that this decision be made public but that the Company not be identifiable by name upon expiry of a period of two years following its publication.

13. Also attached to the report was a notice to attend the restricted committee meeting on 28 January 2021 indicating to the Company that it had one month to provide its written observations in accordance with Article 40 of Decree No. 2019-536 of 29 May 2019.

14. ACCOR responded to the sanction report with written observations dated 22 December 2020.

15. The Company and the rapporteur presented oral observations at the restricted committee meeting.

II. Reasons for the decision

A. On the European cooperation

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

17. In this case, the restricted committee found, firstly, that the registered office of the Company has been in France since the creation of the Company in 1983 and that the Company has been registered in the trade and companies register in France since its inception.

18. Next, the restricted committee found, that ACCOR group's first hotels were based in France, with the Company starting its business abroad only in a second phase.

19. Lastly, to date, while the hotels in the ACCOR group may be located in 110 countries around the world, more than half of the hotels operated under the "AccorHotels" brand in Europe are located in France (1657 hotels out of the 3051 in the European Union).

20. All of these elements lead to believe that the main establishment of the Company is located in France and that CNIL is competent to act as the lead supervisory authority concerning the cross-border processing carried out by the Company, in accordance with Article 56(1) of the Regulation.

21. The restricted committee noted that, as at the date of this draft decision, the supervisory authorities of the following countries were affected by this procedure: Austria, Belgium, Bulgaria, Croatia, Czech Republic, Denmark, Estonia, Germany, Greece, Ireland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden.

22. Following an adversarial procedure, a draft decision was adopted by the restricted committee and sent to the other European supervisory authorities concerned in accordance with Article 60(3) of the GDPR.

23. On 28 May 2021, the Polish data protection authority expressed three objections, under Article 60(4) of the GDPR.

24. In deliberation no. SAN-2022-001 of 13 January 2022, the restricted committee set out its views on the Polish authority's objections and explained the reasons why it decided not to follow these objections.

25. On 15 June 2022, the European Data Protection Board (hereinafter the "EDPB") adopted Decision 01/2022 on the dispute arisen on the draft decision of the French Supervisory

Authority regarding Accor SA under Article 65(1)(a) GDPR. In its decision, the EDPB decided on the dispute concerning the draft decision, which now concerned only one objection expressed by the Polish authority, regarding the amount of the fine set in the draft decision.

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

1. On the absence of consent by individuals to receive marketing messages from ACCOR

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

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

Direct marketing is the sending of any message intended to promote, directly or indirectly, goods, services or the image of a person selling goods or providing services. For the purposes of this Article, calls and messages whose purpose is to induce the user or subscriber to call a premium rate number or to send a premium rate text message shall also constitute direct marketing.

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

[...]".

Under the terms of paragraph 6 of the same article, *"The CNIL (French Data Protection Authority) shall ensure, with regard to direct marketing using a subscriber's or a natural person's details, that the provisions of this article are complied with, using the powers conferred on it by the aforementioned French Data Protection Act No. 78-17 of 6 January 1978. To this end, it may, in particular, receive, by any means, complaints relating to breaches of the provisions of this Article [...]".*

27. The investigations carried out by the CNIL showed that when a person booked a hotel room directly with the staff of a hotel belonging to one of the ACCOR group's hotel brands (on the spot or by telephone) or on the website of one of the group's hotel brands (Ibis, Novotel, Mercure, Fairmont, Sofitel, Adagio, etc.), he or she was sent emails from the Company containing the newsletter "All–Accor Live Limitless", the box relating to consent to receive the newsletter being pre-ticked by default.

28. The rapporteur considers that, in these cases, the consent of the persons to whom the Company's e-mails containing the newsletter "All – Accor Live Limitless" were sent was not legitimately obtained. In this respect, she notes in particular that the commercial and promotional offers in the newsletter "All–Accor Live Limitless" do not relate solely to services provided by the Company, but also to the services of "partner companies" – such as airlines or car park managers.

29. In these circumstances, the rapporteur considers that the Company cannot avail itself of the exception provided for in Article L. 34-5 paragraph 4 of the CPCE, which provides that an organisation may send direct marketing messages by e-mail without first obtaining the consent of the data subjects when the data have been collected from these persons in connection with a sale or a service and the direct marketing concerns similar products or services provided by the same natural or legal person.

30. The Company maintains that it is indeed the entity that collects the data from the data subjects in all cases because, on the one hand, it publishes and manages all the reservation sites of all the group's brands and, on the other hand, even when they are used by the staff of the group's hotels at the request of customers, the reservation and loyalty programme membership tools are managed by it alone and feed its own database.

31. The restricted committee notes that the Company owns the reservation sites for all the group's brands (Ibis, Novotel, etc.). The restricted committee nevertheless noted that the marketing messages sent by the Company did not relate exclusively to similar products or services provided by that Company, but were likely to contain, for example, promotional offers from partners, such as airlines or car park management companies.

32. In these conditions, the restricted committee considers that the Company was required to obtain the prior, free, specific and informed consent of individuals to receive direct marketing messages by e-mail, in accordance with paragraph 1 of Article L. 34-5 CPCE, which was not possible in this case because a box relating to consent to receive the newsletter was pre-ticked by default. The restricted committee recalls that in its Planet49 decision of 1 October 2019, the Court of Justice of the European Union indicated that a consent collected by means of a pre-ticked box cannot be considered as legitimately given by the user.

33. In the course of the proceeding, the Company justified having taken measures to bring all its tools for collecting the consent of data subjects to receive marketing messages by e-mail into compliance, so that for each of the reservation and programme membership paths this consent is no longer collected by default.

34. The restricted committee therefore considers that the breach of Article L. 34-5 CPCE is established, but that the Company had complied with it by the end of the investigation.

2. <u>On the absence of consent from persons creating a customer space to receive marketing messages</u>

35. In the course of the investigation, the CNIL's supervisory delegation noted that, when a customer area was created, the Company did not obtain the consent of individuals to the processing of their personal data for the purpose of marketing by e-mail. It was noted that personal data used by the Company for marketing purposes could be collected from a form for creating a customer area, independently of a reservation, on which there was a box "pre-ticked" by default concerning consent to receive marketing e-mails.

36. The restricted committee considers that the Company is required to obtain the prior, free, specific and informed consent of persons creating a customer space on its website to receive direct marketing messages by e-mail, in accordance with Article L. 34-5(1) CPCE. Indeed, insofar as the creation of a customer area can take place without prior reservation, the exemption from the collection of consent provided for in Article L. 34-5 when similar services are offered cannot be used in this case.

37. In response, the Company explained that it had modified its form for creating a customer area so that the consent of the data subjects to receive marketing messages was no longer required by default.

38. In these circumstances, the restricted committee considered that the breach of Article L. 34-5 of the CPCE was established, but that the Company had complied by the end of the investigation.

C. On the failure to comply with the obligation to inform individuals pursuant to Articles 12 and 13 GDPR

39. According to Article 12(1) GDPR: *"The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language [...]".*

40. Article 13 GDPR requires the data controller to provide, at the time the data is collected, information on its identity and contact details, the purposes and its legal basis of the processing, the recipients or categories of recipients of the personal data, transfers of personal data where applicable, the retention period of the personal data, the rights of individuals and the right to lodge a complaint with a supervisory authority.

41. Firstly, with regard to the accessibility of information, the delegation noted during the online inspection of 24 February 2020 that the forms for creating a customer account or joining the ACCOR group's loyalty programme did not contain the information required by Article 13 GDPR. Nor were individuals invited to take any steps to find out the information provided under Article 13 GDPR, for example by accessing the Company's "*Personal Data Protection Charter"* via a hyperlink.

42. The restricted committee recalls that in order to consider that a controller meets its transparency obligation, it is necessary, in particular, for the information provided to be "*easily accessible*" for the data subjects within the meaning of Article 12 of the Regulation.

43. In addition, it points out that this provision must be interpreted in the light of Recital 61 of the Regulation, according to which: *"The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject".* In this sense, it shares the position of the G29 presented in the guidelines on transparency under the Regulation, adopted in their revised version on 11 April 2018 and endorsed on 25 May 2018 by the European Data Protection Board (EDPB), which recalls that which recalls that "*the data subject should not have to search for the information but should be able to access it immediately*".

44. The restricted committee considered that in the case in point, the information provided to the data subjects was not "easily accessible" for the latter, in that, when an account was created, access to the Company's "*Personal Data Protection Charter*" was only organised via a hypertext link available at the very bottom of the website's pages, which required the Internet user to scroll down the entire page and search for the information, in disregard of Article 12 GDPR.

45. In the course of the investigation, the Company indicated that it had made corrections in order to provide information in accordance with the requirements of the GDPR. Through an informal verification, it was observed that the informational wording on the processing of personal data would be completed on the account creation and loyalty programme membership forms and that the "*Client Data Protection Charter*" would henceforth be directly accessible from a link inserted on these forms.

46. Secondly, the delegation noted that the "*Customer Personal Data Protection Charter"* specifies that the legal basis for the processing of personal data in connection with the sending of marketing messages is "legitimate interest" or "performance of a contract".

47. However, the rapporteur maintains that, in the aforementioned cases, when sending marketing messages relating to the products or services of third parties, the Company cannot dispense with the need to obtain the consent of the data subjects to receive marketing messages.

48. In response, the Company indicated that, even if the consent of the data subjects must be obtained under the provisions of Article L. 34-5 CPCE, the legal basis for the processing carried out for the purposes of marketing is legitimate interest.

49. As previously stated, the restricted committee considers that in certain cases the Company is required to obtain the prior, free, specific and informed consent of the data subjects to receive direct marketing messages by electronic mail, in accordance with the provisions of Article L. 34-5(1) CPCE.

50. The restricted committee considers that, when the consent of the data subject is required for the processing of his or her personal data for a determined purpose (and not only for a given operation), the legal basis for the processing thus carried out is consent.

51. Consequently, the restricted committee noted that, by not mentioning consent as the legal basis for processing, for marketing to promote the products or services of third parties, the Company had failed to fulfil its obligation under Article 13 GDPR.

52. The restricted committee therefore considers that all these facts constitute breaches of Articles 12 and 13 GDPR.

D. On the failure to comply with the obligation to respect the right of access of individuals under Article 15 GDPR

53. Article 15.1 GDPR provides for a data subject's right of access to his or her personal data in these terms: "*The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data (...)*".

54. Article 12.3 GDPR further states that "*The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request*".

55. During the investigation of complaint No. […] received by the CNIL, it appeared that the Company had failed to provide the complainant with a copy of her personal data held in its database within the time limit set by the GDPR.

56. The rapporteur notes that the complainant made a request for access on 1 August 2019, when her customer account was suspended following the detection of a fraudulent connection. However, while the complainant had provided proof of her identity on 10 January 2020, allowing the Company to reopen her customer account, no response had yet been provided to her request for access rights at the time of the CNIL delegation's inspection on 11 February 2020. The Company granted the complainant's request on 24 February 2020.

57. The restricted committee considers that, in the event that a fraudulent login has been detected on a customer's account, the Company may certainly have reasonable doubts about the identity of the applicant wishing to exercise his or her right of access, justifying that an identity document should be requested from the data subject.

58. The restricted committee points out, however, that if doubt is raised over the identity of the person, the request for a right of access must be honoured by the controller.

59. In these circumstances, the restricted committee considers that the breach of Article 15 GDPR is established with regard to complaint No. […], although it does not appear from the file that, beyond this specific complaint, the breach was of a structural nature.

E. On the failure to comply with the obligation to respect the right to object of individuals under Article 21 GDPR

60. According to Article 21.2 GDPR: "*Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing*".

61. Firstly, the rapporteur notes that the complainant of complaint No. […] objected to the receipt of marketing messages from ACCOR at their two email accounts on 11 December 2018.

62. The rapporteur considered that the Company had not responded satisfactorily to the complainant's request for an objection, since the objection request was only taken into account on 11 January 2020 and for only one of the two e-mail addresses concerned.

63. In response, the Company stated that it had not found any record of this objection in its systems. It also stated that it had not been able to find the first e-mail address referred to by the complainant in their application in its database and that, as regards the second e-mail address, it was the complainant himself who had unsubscribed from the newsletters on 11 January 2020.

64. The restricted committee considers that, with regard to this first complaint, the elements of the debate do not make it possible to conclude that the Company committed a breach.

65. Secondly, the investigation of complaints No. […] received by the CNIL revealed the existence of malfunctions in the unsubscribe link at the bottom of the marketing emails sent by the Company, resulting from two types of technical problems affecting either of the stages of the unsubscribe process.

66. First, between 11 November 2018 and 21 January 2019, there were malfunctions in the transmission of unsubscribe information between the tool used to manage the sending of newsletters and the customer repository, which records information on whether or not a customer has subscribed to newsletters. Thus, during this period, the newsletter management tool was not informed by the customer repository of the creation or updating of contacts and the unsubscribing of associated newsletters every Sunday between 0:00 and 20:00. Consequently, until 21 January 2019, the author of complaint No. […] continued to receive marketing messages from the Company, despite their unsubscribe request made on Sunday 18 November 2018 in the afternoon.

67. Then, another anomaly, also affecting the synchronisation of unsubscriptions between the customer repository and the tool that manages the sending of newsletters, was identified by the Company on 8 February 2019. This anomaly would explain why the author of claim No. […] continued to receive the newsletter from ACCOR between 2 January 2019 and 8 February 2019, despite the deletion of their data from the customer repository as of 1 January 2019.

68. The restricted committee considers that these two anomalies, which recurred over several weeks, are likely to have prevented a significant number of persons from effectively objecting to the receipt of the marketing messages. In this regard, it recalls that it is clear from the evidence that in 2019, […] million people received at least one of the ACCOR group's newsletters at a valid e-mail address.

69. In response, the Company states that it has taken measures to improve the management of requests to exercise rights and to prevent anomalies in the processing of objection requests.

70. However, the restricted committee acknowledges the Company's efforts to come into compliance, but considers that in the past the Company disregarded its obligations under Article 21.2 GDPR since the above-mentioned anomalies have failed to take into account within a reasonable period of time data subjects' objection requests to receiving direct marketing messages.

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

71. Article 32 of the Regulation states:

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

a) the pseudonymisation and encryption of personal data;

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

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing […]".

72. Firstly, the rapporteur indicates that during the on-site inspection of 11 February 2020, the delegation noted that the use of a password consisting of 8 characters containing only two types of characters (seven upper case letters and one special character) enabled access to the tool used to send messages to customers.

73. The rapporteur therefore considers that, in view of the volume of data processed by the “Adobe Campaign” tool, the requirements put in place by the Company with regard to the robustness of passwords are insufficient and do not guarantee the security of personal data.

74. In response, the Company argued that, given the existence of an additional security measure – in that access to the "Adobe Campaign" software is only possible from a terminal connected to the ACCOR network – only one level of complexity (lower case or number) was needed for the password found by the delegation to comply with the recommendations by CNIL. The Company also explains that it has tightened the complexity rules for the password to access the "Adobe Campaign" software, which must now contain a minimum of nine characters and four levels of complexity.

75. The restricted committee considers that the length and complexity of a password remain basic criteria for assessing its strength. It noted in this respect that the need for a strong password is also highlighted by ANSSI (French National Cybersecurity Agency).

76. For the sake of clarity, the restricted committee recalled that in order to ensure a sufficient level of security and satisfy the requirements for robustness of passwords, when authentication relies solely on an identifier and password, the CNIL recommends, in its deliberations No. 2017-012 of 19 January 2017, that the password has at least 12 characters - containing at least one capital letter, a lower-case letter, a digit and a special character - or at least eight characters - containing three of these four characters - if it is accompanied by an additional measure such as, for example, the timing of access to the account after several failures (temporary suspension of access, the duration of which increases as attempts are made), setting up a mechanism to guard against automated and intensive attempts (e.g.: a “captcha”) and/or locking the account after several failed login attempts.

77. In this case, the restricted committee considered that, in view of the rules governing their composition, the robustness of the passwords accepted by the Company for access to the "Adobe Campaign" software was too weak, leading to a risk of compromise of the personal data it contains.

78. However, the restricted committee notes that the Company has provided evidence of having increased the level of complexity of the connection passwords to the "Adobe Campaign" software.

79. As a result, the restricted committee considered that the breach of the obligation to ensure the security of personal data was established, but that the Company had come into compliance on this point before the end of the investigation.

80. Secondly, the rapporteur was informed that when a customer's account is suspended due to a suspected fraudulent login, the customer service department asks the data subject to provide a copy of his/her identity document in an email attachment.

81. The rapporteur notes that the conditions in which the copy of the identity document of customers whose account has been suspended is transmitted do not prevent its interception by a third party.

82. The restricted committee believes that the practice of transmitting unencrypted data by e-mail creates a significant risk to the confidentiality of the data transmitted.

83. In this respect, the restricted committee recalls that, in its guide on "the security of personal data", the CNIL recommends as an elementary security precaution, encryption of data before it is recorded on a physical medium or e-mail transmission. It also recommends that the confidentiality of the decryption password be ensured by transmitting it through another channel.

84. In view of the above, the restricted committee considers that the aforementioned facts constitute a breach of Article 32 GDPR.

III. On corrective measures and their publication

85. Under the terms of Article 20(III) of the Act of 6 January 1978 amended:

"*When the controller or his processor fails to comply with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or this law, the chair of the CNIL may also, if applicable, after sending the warning provided for in point I of this article or, where applicable, in addition to an order provided for in II, contact the restricted committee of the commission with a view to the announcement, after adversarial procedure, of one or more of the following measures: [...]*

7. With the exception of cases where the processing is implemented by the State, an administrative fine may not exceed 10 million euros or, in the case of a company, 2% of the total annual global turnover of the previous financial year, whichever is the greater. In the cases mentioned in 5 and 6 of Article 83 of Regulation (EU) 2016/679 of 27 April 2016, these upper limits shall be increased, respectively, to 20 million euros and 4% of the said turnover. In determining the amount of the fine, the restricted committee shall take into account the criteria specified in the same Article 83."

86. Article 83 GDPR further states that "Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive", before specifying the elements to be taken into account when deciding whether to impose an administrative fine and to decide on the amount of that fine.

87. In its defence, the Company argued that a penalty was not necessary in view of all the measures it had taken to remedy the shortcomings observed and considered, in any event, that the amount of the administrative fine proposed by the rapporteur was disproportionate in view of, in

particular, the low seriousness of the breaches, the measures taken to remedy them, its cooperation with the CNIL, and its financial position, which had deteriorated significantly as a result of the current health crisis. The Company also maintains that the publication of the restricted committee's sanction decision would have manifestly disproportionate consequences for it.

88. With regard to the nature and seriousness of the violation, the restricted committee first notes the number of breaches of which the Company was accused: carrying out massive e-mail marketing campaigns without the consent of individuals, lack of easily accessible and complete information on the processing carried out, difficulties encountered in the exercise of their rights by complainants and data security defects. It stresses that these failures concern several fundamental principles of the applicable legislation on the protection of personal data and that they constitute a substantial infringement of the rights of the data subjects.

89. The restricted committee then noted the particularly large number of people affected by these breaches, since in 2019, […] million people received at least one of the ACCOR group 's newsletters at a valid e-mail address.

90. The restricted committee finally recalls that these breaches had direct consequences for the data subjects, as evidenced by the fact that the CNIL received eleven complaints relating in particular to the right to object to marketing messages.

91. Consequently, the restricted committee considers that an administrative fine should be imposed in view of the breaches established.

92. With regard to the amount of the fine concerning breaches of the GDPR, the restricted committee recalls that Article 83(3) of the Regulation provides that in the event of multiple breaches, as in the case in point, the total amount of the fine may not exceed the amount set for the most serious breach. Insofar as the Company is alleged to be in breach of Articles 12.1, 12.3, 13, 15.1, 21.2 and 32 of the Regulation, the maximum fine that can be imposed is €20 million or 4% of annual worldwide turnover, whichever is higher.

93. The restricted committee notes that the company's turnover amounted to […] in 2021

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

95. In assessing the proportionality of the fine, the restricted committee took into account the fact that the Company had complied with all the breaches identified and that some of them, in relation to the exercise of individuals' rights, were not of a structural nature. It also notes that the Company fully cooperated with the CNIL.

96. In determining the amount of the fine imposed, the restricted committee also takes into account the financial situation of the company. In this respect, the company's turnover decreased in 2020 and 2021 compared to 2019. Indeed, the company's turnover amounted to […] in 2019, […]in 2020 and […] in 2021.

97. Finally, the restricted committee duly notes the decision no 01/2022 of the EDPB on the dispute concerning the French supervisory authority's draft decision about Accor SA, under Article 65(1)(a) of the GDPR. In particular, it notes that the EDPB has ordered the CNIL to reconsider the factors on the basis of which it calculated the amount of the fine, in order to ensure that the fine meets the criterion of dissuasive effect laid down in Article 83(1) of the GDPR.

98. Therefore, in view of the economic context caused by the Covid-19 health crisis, its consequences on the Company's financial situation and the relevant criteria of Article 83(2) GDPR mentioned above, the restricted committee considers that the imposition of an administrative fine of €600,000 appears justified

99. Finally, the restricted committee considers that the publication of its decision to impose a sanction for a period of two years is justified in view of the number of breaches identified, their seriousness, and the number of persons concerned.

100. The restricted committee specifies that the administrative fine of €600,000 envisaged for ACCOR applies as follows: €100,000 for the breach of the provisions of Article L. 34-5 of the CPCE and €500,000 for the Company's breaches of Articles 12.1, 12.3, 13, 15.1, 21.2 and 32 of the Regulation.

FOR THESE REASONS

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

- **impose an administrative fine on ACCOR SA in the amount of €600,000** for all the breaches found, which breaks down as follows:
    - **€100,000 (one hundred thousand euros)** for the Company's failure to comply with Article L. 34-5 of the French Post and Electronic Communications Code;
    - **€500,000 (five hundred thousand euros)** for the Company's failure to comply with Articles 12.1, 12.3, 13, 15.1, 21.2 and 32 of **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016**.
- **make public**, on the CNIL website and on the Légifrance website, its decision, which will no longer identify the Company at the end of a period of two years following its publication.

The Chairman

Alexandre LINDEN

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