Deliberation SAN-2022-017 of August 3, 2022 National Commission for Computing and Liberties Nature of the deliberation: Sanction Legal status: In force Date of publication on Légifrance: Friday August 19, 2022 Deliberation of the restricted committee no. SAN-2022-017 of 3 August 2022 concerning ACCOR SAThe National Commission for Computing and Liberties, meeting in its restricted formation composed of Mr. Alexandre LINDEN, Chairman, Mr. Philippe-Pierre CABOURDIN, Vice-Chairman, Ms. Christine MAUGÜE, 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 relating to the protection of personal data and 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 concerning the processing of personal data and the protection of privacy in the electronic communications sector ues; Having regard to the postal and electronic communications code; Having regard to law no. 78-17 of January 6, 1978 relating to data processing, files and freedoms, in particular its articles 20 and following; Having regard to decree no. 2019-536 of May 29, 2019 taken for the application of law no. 78-17 of January 6, 1978 relating to data processing, files and freedoms; Having regard to deliberation no. 2013-175 of July 4, 2013 adopting the Commission's internal regulations Commission for Computing and Liberties; Having regard to the referrals to our […]; Having regard to Decision No. 2019-046C of February 18, 2019 of the President of the National Commission for Computing and Liberties to instruct the Secretary General to proceed or to carry out a mission to verify the processing implemented by ACCOR; Having regard to the decision of the President of the National Commission for Computing and Liberties appointing a rapporteur to the restricted committee, dated October 16, 2020; Seen on ra report of Mrs. Sophie LAMBREMON, reporting commissioner, notified to ACCOR on November 24, 2020; Having regard to the written observations submitted by ACCOR on December 22, 2020; Having regard to the other documents in the file; Having regard to decision 01/2022 concerning the dispute relating to the draft decision of the French supervisory authority concerning Accor SA pursuant to Article 65, paragraph 1, point a) of the GDPR; Sophie LAMBREMON, commissioner, heard in her report;As representatives of ACCOR:[…] ACCOR having spoken last;The Restricted Committee adopted the following draft decision:I. Facts and procedure1. ACCOR SA (hereinafter "the company") is a public limited company with a board of directors created in 1960, specializing in the hotel sector. Its head office is located at 82, rue Henri Farman in Issy-les-Moulineaux (92130).2. In 2021, the company achieved a turnover of […]. In the summer of 2020, 5,100 hotels, located in 110 countries, under 39 different brands, were operated under contracts binding their owners to ACCOR (mainly franchise or "management" contracts). The company employs around 1,500 people.3. Between December 2018 and September 2019,

the National Commission for Computing and Liberties (hereinafter "the CNIL" or "the Commission") received five complaints directly (referrals our […]) relating to the absence taking into account the right of opposition to the receipt by e-mail of commercial prospecting messages (advertising e-mails, welcome e-mails to the loyalty program, newsletters) from the company. On September 22, 2019, the CNIL also received a complaint (referral No. […]) relating to the difficulties encountered in exercising the right of access, in particular to banking data collected by the company on the occasion booking 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 processing of complaints received at the against the company, the CNIL informed, on December 12, 2018, all the European supervisory authorities of its competence to act as lead supervisory authority concerning the cross-border processing implemented by the company, competence drawn by the CNIL from the fact that the main establishment of the company is in France.5. Through the exchange platform between European data protection authorities, the CNIL has initiated the procedure allowing the supervisory authorities concerned to declare themselves. Ten authorities have declared themselves concerned by this procedure, within the meaning of Article 4 (22) of the GDPR.6. At the same time, between January 2019 and February 2020, the CNIL received, in its capacity as "lead authority", pursuant to the cooperation mechanisms provided for by the Regulation, five other complaints received respectively by the supervisory authorities of Saarland, Spain, Ireland, Poland and Lower Saxony (referrals nos […]). These complaints also related to requests to oppose the processing of personal data for commercial prospecting purposes by email and the exercise of the right of access to data collected by ACCOR.7. On March 6, 2019, pursuant to decision no. 2019-046C of February 18, 2019 by the President of the CNIL, a questionnaire was sent to ACCOR, to which the latter responded by letter dated April 8 and then by letters May 22, August 1, October 11 and December 27, 2019. The purpose of this document control mission was to verify compliance by ACCOR with all the provisions of the GDPR and Law No. 78-17 of January 6, 1978 relating to data processing, files and freedoms (hereinafter "the amended law of January 6, 1978" or the "Data Processing and Freedoms" law).8. Following this first check, the CNIL, taking into account the response provided by the company to the instruction letter sent to it and its compliance on several points, submitted to its European counterparts, on December 23 2019, in application of article 60 of the GDPR, a draft decision from its president reminding the company of its obligations, in accordance with the provisions of article 58.2.b) of the GDPR.9. This draft decision has been the subject of relevant and reasoned objections from certain authorities concerned within the meaning of Article 60 of the GDPR, requesting that the company not only be the

subject of a reminder to the order but that it be sanctioned by an administrative fine and highlighting, in particular, the number of breaches, the number of complaints and the size of the company. Given these objections and the new complaints received since the first inspection, the CNIL decided to resume its investigations with the company.10. On February 11, 2020, the CNIL delegation carried out an inspection mission at the company's premises. An online check of the company's website (www.all.accor.com) was then carried out on February 24, 2020, pursuant to the aforementioned decision no. 2019-046C. Following these investigations, the company sent additional information to the CNIL by letter dated February 21, March 10, March 19 and August 7, 2020.11. For the purpose of examining these elements, the President of the Commission, on October 16, 2020, appointed Mrs. Sophie LAMBREMON as rapporteur, on the basis of Article 22 of the law of January 6, 1978 as amended.12. At the end of her investigation, the rapporteur notified the company, on November 24, 2020, of a report detailing the breaches of the provisions of Articles L. 34-5 of the Postal and Electronic Communications Code (hereinafter the " CPCE") and 12-1, 12-3, 13, 15-1, 21-2 and 32 of the GDPR which it considered constituted in this case. This report proposed that the restricted committee of the Commission impose an administrative fine on the company and that this decision be made public but no longer allow the company to be identified by name at the end of a two-year period. from its publication.13. Also attached to the report was a convocation to the restricted training session of January 28, 2021 indicating to the company that it had one month to submit its written observations pursuant to the provisions of article 40 of the decree. n° 2019-536 of May 29, 2019.14. ACCOR responded to the sanction report with written observations dated December 22, 2020.15. The company and the rapporteur presented oral observations during the session of the restricted committee.II. Reasons for decisionA. On the European cooperation procedure16. According to Article 56(1) of the Regulation "the supervisory authority of the main establishment or of the sole establishment of the controller or of the processor is competent to act as supervisory authority controller with regard to the cross-border processing carried out by this controller or processor, in accordance with the procedure provided for in Article 60 “.17. In this case, the Restricted Committee notes, first, 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 the origin.18. The Restricted Committee then notes that the first hotels of the ACCOR group were established in France, the company having launched its activity abroad only later.19. Finally, to date, although the hotels of the ACCOR group are established in 110 countries throughout the world, more than half of the hotels operated under the "AccorHotels" brand in Europe are located in France (1,657 hotels out of the 3,051 present in the European Union). 20. All

of these elements combine to consider that the main establishment of the company is in France and that the CNIL is competent to act as the lead supervisory authority concerning the cross-border processing carried out by this company, pursuant to Rule 56(1) of the Rules.21. The Restricted Committee notes that on the date of this draft decision the supervisory authorities of the following countries were concerned by this procedure: Germany, Austria, Belgium, Bulgaria, Croatia, Denmark, Spain, Estonia, Greece, Ireland, Italy, Latvia, Lithuania, Luxembourg, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Sweden and Czech Republic.22. Following an adversarial procedure, a draft decision was adopted by the restricted committee and sent to the other European supervisory authorities concerned pursuant to Article 60(3) of the GDPR.23. On May 28, 2021, the Polish Data Protection Authority filed three objections, in accordance with Article 60(4) of the GDPR.24. By deliberation no. SAN-2022-001 of 13 January 2022, the Restricted Committee set out its point of view on the objections of the Polish authority and explained the reasons for which it decided not to follow these objections.25. On June 15, 2022, the European Data Protection Board (hereinafter "EDPB") adopted decision 01/2022 concerning the dispute relating to the draft decision of the French supervisory authority concerning Accor SA pursuant to the Article 65(1)(a) GDPR. By this decision, the EDPS ruled on the dispute relating to the draft decision, which now only concerned a single objection from the Polish authority, concerning the amount of the fine set in the draft decision.B. On the breach relating to the obligation to obtain the consent of the person concerned by a direct marketing operation by means of an automated electronic communications system pursuant to Article L. 34-5 of the CPCE1. On the lack of consent of individuals to receive commercial prospecting messages from ACCOR26. Article L. 34-5 of the CPCE provides: "Direct canvassing by means of an automated electronic communications system within the meaning of 6° of Article L. 32, a fax machine or e-mails using the contact details is prohibited. of a natural person, subscriber or user, who has not previously expressed his consent to receive direct prospecting by this means. For the purposes of this article, consent means any expression of free will, specific and informed by which a person accepts that personal data concerning him be used for the purpose of direct prospecting Constitutes direct prospecting 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 intended to encourage the user or subscriber to call a surt focused or to send a surcharged text message also fall under direct prospecting. However, direct prospecting by e-mail is authorized if the recipient's contact details 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, on the occasion of a sale or the provision of services, if the

direct prospecting 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 manner, the use of his contact details at the when they are collected and each time a prospecting e-mail is sent to him in the event that he has not refused such use from the outset. […] ". Under the terms of paragraph 6 of the same article, "The National Commission for Computing and Liberties ensures, with regard to direct prospecting using the contact details of a subscriber or a natural person, compliance with the provisions of this article by using the skills recognized by law n° 78-17 of January 6, 1978 mentioned above. To this end, it may in particular receive, by any means, complaints relating to breaches of the provisions of this article [...]". directly with the staff of a hotel of one of the hotel brands of the ACCOR group (on site or by telephone) or on the site of one of the hotel brands of the group (Ibis, Novotel, Mercure, Fairmont, Sofitel, Adagio etc. ), she was made the recipient of emails from the company containing the “All – Accor Live Limitless” newsletter, 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 recipients of the company's emails containing the "All – Accor Live Limitless" newsletter was not validly obtained. It notes in particular in this respect that the commercial and promotional offers present in the "All – Accor Live Limitless" newsletter do not relate solely to services provided by the company but also relate to the services of "partner" companies - such as, for example, airlines or car park management companies.29. Under these conditions, the rapporteur considers that the company cannot take advantage of the exception provided for in Article L. 34-5 paragraph 4 of the CPCE, which provides that an organization may send commercial prospecting messages by e-mail. without first obtaining the consent of the persons concerned when the data has been collected from these persons on the occasion of a sale or the provision of services and that the commercial prospecting concerns similar products or services provided by the same natural person or moral.30. The company maintains that it is indeed the company that collects the data from the persons concerned in all cases because, on the one hand, it publishes and manages all the reservation sites of all the brands of the group and, on the other hand, even when they are used by the staff of the group's hotels at the request of customers, the tools for booking and joining the loyalty program are managed by it alone and feed its own database.31. The Restricted Committee notes that the company owns the reservation sites of all the group's brands (Ibis, Novotel, etc.). The Restricted Committee nevertheless notes that the commercial prospecting messages sent by the company do not relate exclusively to similar products or services provided by this company but that they are likely to contain, for example, promotional offers from partners,

such as airlines or car park management companies.32. Under these conditions, the Restricted Committee considers that the company was required to obtain the prior, free, specific and informed consent of persons to receive direct prospecting messages by e-mail, in accordance with paragraph 1 of Article L. 34 -5 of the CPCE, which was not allowed by the existence, in this case, of a box relating to consent to receive the newsletter pre-ticked by default. The Restricted Committee recalls that in its Planet49 judgment of October 1, 2019 (case C-673/19), the Court of Justice of the European Union indicated that consent obtained by means of a pre-ticked box cannot be considered as validly given by the user.33. As part of the procedure, the company has justified having taken measures to bring all of its tools for collecting the consent of the persons concerned to receive commercial prospecting messages by e-mail into compliance, so that for each of the reservation and membership of the program this consent is no longer collected by default.34. The Restricted Committee therefore considers that the breach of Article L. 34-5 of the CPCE has been established, but that the company has complied on the closing date of the investigation.2. On the lack of consent of persons creating a customer space, upon receipt of commercial prospecting messages35. As part of the investigation, the CNIL's delegation of control noted that, when creating a customer space, the company did not obtain the consent of individuals for the processing of their personal data for the purposes commercial prospecting by e-mail. Indeed, it was noted that the personal data used by the company for commercial prospecting purposes could be collected from a form for creating a customer area, independently of a reservation, on which appeared a box "pre - checked " by default relating to the consent to receive commercial prospecting.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 prospecting messages by e-mail, in accordance with paragraph 1 of the article L. 34-5 of the CPCE. Indeed, insofar as the creation of a customer area can occur without prior reservation, the exemption from obtaining consent provided for in Article L. 34-5 when similar services are offered cannot be mobilized in this scenario.37. In response, the company justified having modified its form for creating a customer area, so that the consent of the persons concerned to receive prospecting messages is no longer collected by default.38. Under these conditions, the Restricted Committee considers that the breach of Article L. 34-5 of the CPCE has been established, but that the company has complied on the closing date of the investigation.C. On the breach relating to the obligation to inform individuals pursuant to Articles 12 and 13 of the GDPR39. Under the terms of paragraph 1 of Article 12 of the GDPR: "The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 as well as to carry out any communication under Articles 15 to 22 and

Article 34 with regard to the processing to the data subject in a concise, transparent, understandable and easily accessible manner, in clear and simple terms […] ".40. Article 13 of the GDPR requires the data controller to provide, at the time the data is collected, information relating to his identity and contact details, the purposes of the processing and its legal basis, the recipients or categories of recipients personal data, where applicable the transfers of personal data, the retention period of personal data, the rights enjoyed by individuals and the right to lodge a complaint with a supervisory authority. 41. Firstly, with regard to the accessible nature of the information, the delegation noted during the online check of February 24, 2020 that the forms allowing the creation of a customer account or membership of the ACCOR group's loyalty program did not include the information required by Article 13 of the GDPR. People were also not invited to take any steps to read the information provided under Article 13 of the GDPR, for example by accessing the "data protection charter" via a hypertext link. personal data" of the company.42. The Restricted Committee recalls that in order to consider that a data controller meets his obligation of transparency, the information provided must in particular be "easily accessible" for the persons concerned within the meaning of Article 12 of the Regulation.43. It notes, in this respect, that this provision must be interpreted in the light of recital 61 of the Regulation, according to which: "information on the processing of personal data relating to the data subject should be provided to him at the time when these data is collected from it". In this sense, it shares the position of the G29 presented in the guidelines on transparency within the meaning of the Regulation, adopted in their revised version on April 11, 2018 and endorsed on May 25, 2018 by the European Data Protection Board (EDPB), 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 considers that in this case the information notices of the persons concerned were not "easily accessible" for the latter, in that, when creating an account, access to the "charter protection of personal data" of the company was only organized via a hypertext link available at the very bottom of the pages of the website, which required the Internet user to scroll through the page in its entirety and search for information, in ignorance of article 12 of the GDPR.45. As part of the investigation, the company indicated that it had made corrections, in order to provide information that complies with the requirements of the GDPR. Through an informal check, it was found that the information relating to the processing of personal data had been completed on the forms for creating an account and joining the loyalty program and that the "data protection charter customers' personal data" was now directly accessible from a link inserted on these forms.46. Secondly, the delegation of control noted that the company's "customer personal data protection charter" specifies that the legal basis for the processing of personal data in connection with

the sending of commercial prospecting is "the legitimate interest " or " performance of a contract ".47. However, the rapporteur maintains that, in the hypotheses mentioned above, for the sending of prospecting messages relating to the products or services of third parties, the company cannot dispense with obtaining the consent of the persons concerned to receive commercial prospecting messages. 48. In response, the company indicates that, even if the consent of the persons concerned must be obtained by virtue of the provisions of Article L. 34-5 of the CPCE, the processing operations implemented for the purposes of commercial prospecting have the legal basis legitimate interest.49. As previously explained, the Restricted Committee considers that in certain cases the company is required to obtain the prior, free, specific and informed consent of the persons concerned to receive direct prospecting messages by e-mail, in accordance with the provisions of paragraph 1 of article L. 34-5 of the CPCE.50. The Restricted Committee considers that when obtaining the data subject's consent is necessary for the processing of their personal data for a specific purpose (and not only for a given operation), the legal basis for the processing thus implemented is consent.51. Consequently, the Restricted Committee notes that by not mentioning consent as the legal basis for processing, for prospecting to promote the products or services of third parties, the company has failed to comply with its obligation under Article 13 of the GDPR. 52. The Restricted Committee therefore considers that all of these facts constitute breaches of Articles 12 and 13 of the GDPR.D. On the breach relating to the obligation to respect the right of access of individuals pursuant to Article 15 of the GDPR53. Article 15.1 of the GDPR provides a right of access for the data subject to his personal data in these terms: "The data subject has the right to obtain from the controller confirmation that personal data concerning him are or are not processed and, when they are, access to said personal data (…)".54. Article 12.3 of the GDPR further specifies that "the 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 any cause within one month of receipt of the request ".55. During the investigation of complaint No. […] received by the CNIL, it appeared that the company failed in its obligation to provide the complainant, within the time limit set by the GDPR, with a copy of her personal data. personnel it held in its database.56. The rapporteur notes that the author of the complaint made a request for the right of access on 1 August 2019, the date on which her customer account had been suspended following detection of a fraudulent connection. However, while the complainant had provided proof of her identity on January 10, 2020, thus allowing the company to reopen her customer account, no response had yet been provided to her request for the right of access on the date of the control of the CNIL delegation, February 11, 2020. The company granted the complainant's request on February 24, 2020.57. The Restricted

Committee considers that, in the event that a customer's account has been detected as a fraudulent connection, the company may certainly have a reasonable doubt about the identity of the applicant wishing to exercise his right to access, justifying that an identity document is requested from the person concerned.58. The Restricted Committee considers, however, that, once the doubt is removed as to the identity of the person, the request for the right of access must be honored by the controller.59. Under these conditions, the Restricted Committee considers that the breach of Article 15 of the GDPR is constituted with regard to complaint No. […], although it does not appear from the file that beyond this specific complaint the failure was of a structural nature.E. On the breach relating to the obligation to respect the right of opposition of individuals pursuant to Article 21 of the GDPR60. Under Article 21.2 of the GDPR: "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 concerning him or her for such purposes. prospecting purposes, including profiling insofar as it is related to such prospecting".61. Firstly, the rapporteur noted that the author of complaint no. […] objected to the receipt of prospecting messages from the company on his two email addresses on December 11, 2018.62. The rapporteur considered that the company had not responded satisfactorily to the complainant's request for opposition, since his request for opposition was only taken into account on January 11, 2020 and for only one of the two email addresses concerned.63. In response, the company indicated that it had found no trace of this objection request in its systems. It also indicates that it has not found in its database either the first email address referred to by the complainant in his request and specifies, with regard to the second email address, that it is the author of the complaint himself. even who unsubscribed from newsletters on January 11, 2020.64. The Restricted Committee considers that, with regard to this first complaint, the elements of the debate do not allow it to conclude that there has been a breach committed by the company.65. Secondly, the investigation of complaints no. […] received by the CNIL revealed the existence of malfunctions in the unsubscribe link appearing at the bottom of the prospecting emails sent by the company, resulting from two types of technical problem affecting the any of the steps in the unsubscribe process.66. First, between November 11, 2018 and January 21, 2019, malfunctions occurred in the transmission of information relating to unsubscriptions between the tool used to manage the sending of newsletters and the customer repository, which records the information whether or not a customer subscribes to newsletters. Thus, during this period, the newsletter management tool was not informed by the customer repository of creations or updates of contacts and unsubscriptions to associated newsletters made every Sunday between midnight and 8 p.m. From then on, until January 21, 2019, the author of complaint n°[…] continued to receive commercial prospecting

messages from the company, despite his request to unsubscribe made on Sunday November 18, 2018 in the afternoon.67. Then, another anomaly, also affecting the synchronization of unsubscriptions between the customer repository and the tool that manages the sending of newsletters, was identified by the company on February 8, 2019. This anomaly explains that the author of the complaint n ° […] continued to receive the ACCOR newsletter between January 2, 2019 and February 8, 2019, despite the deletion of its data from the customer repository as of January 1, 2019.68. The Restricted Committee considers that these two anomalies, which recurred for several weeks, are likely to have prevented a significant number of people from effectively opposing the receipt of prospecting messages. It notes in this regard that it appears from the documents in the file that in 2019, […] million people received at least one of the ACCOR group newsletters on a valid email 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 consideration of opposition requests.70. The Restricted Committee takes note of the compliance measures adopted by the company, but considers that the company has in the past disregarded its obligations under the provisions of Article 21.2 of the GDPR, since the aforementioned anomalies have defeated the taking into account within a reasonable time of requests to object to receiving commercial prospecting messages from the persons concerned. F. On the breach relating to the obligation to ensure the security of personal data pursuant to Article 32 of the GDPR71. Article 32 of the Regulation provides: "1. Taking into account the state of knowledge, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risks, the degree of which probability and severity varies, for the rights and freedoms of natural persons, the controller and the processor implement the appropriate technical and organizational measures to guarantee a level of security appropriate to the risk, including, among other things, as required:a) pseudonymization and encryption of personal data;b) means to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;c) means to to restore the availability of personal data and access to them within an appropriate period of time in the event of a physical or technical incident; d) a procedure aimed at testing, analyzing and evaluating regularly monitor the effectiveness of the technical and organizational measures to ensure the security of the processing […]".72. Firstly, the rapporteur notes that, during the on-the-spot check of 11 February 2020, the delegation noted that the use of a password made up of eight characters containing only two types of characters (seven capital letters and one character special) provided access to the management tool for sending communications to clients.73. The rapporteur considers that, given in particular the volume of personal data processed by the "Adobe Campaign" tool, the requirements put

in place by the company in terms of the robustness of passwords are insufficient and do not make it possible to ensure the security of personal data. 74. In response, the company argues that, given the existence of an additional security measure – namely 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 missing for the password noted by the delegation to meet the recommendations of the CNIL. The company also justifies having reinforced the complexity rules for the password for accessing the "Adobe Campaign" software, which must now include 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 notes in this regard that the need for a strong password is also emphasized by the National Information Systems Security Agency.76. By way of clarification, the Restricted Committee recalls that to ensure a sufficient level of security and meet the robustness requirements of passwords, when authentication is based solely on an identifier and a password, the CNIL recommends, in its deliberation no. 2017-012 of January 19, 2017, that the password has at least twelve characters - containing at least one uppercase letter, one lowercase letter, one number and one special character - or has at least eight characters - containing three of these four categories of characteristics - if it is accompanied by an additional measure such as, for example, the delay of access to the account after several failures (temporary suspension of access, the duration of which increases as attempts are made), the implementation of a mechanism to guard against automated and intensive submissions of attempts (such as a "captcha") and/or blocking of the account after several authentication attempts unsuccessful ification.77. In this case, the Restricted Committee considers that with regard to 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. The Restricted Committee notes, however, that the company justifies having increased the level of complexity of the passwords for connecting to the "Adobe Campaign" software.79. Consequently, the Restricted Committee considers that the breach relating to the obligation to ensure the security of personal data has been established, but that the company has complied on this point before the close of the investigation.80 . Secondly, the rapporteur indicated that when a customer's account is suspended due to a suspicion of fraudulent connection, customer service invites the person concerned to send a copy of their identity document as an attachment to an email.81. The rapporteur notes that the conditions under which the copy of the identity document of customers whose account has been suspended is transmitted do not provide protection against its interception by a third party.82. The Restricted Committee

considers that the practice consisting in the transmission of unencrypted data by e-mail generates a significant risk for 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 the encryption of data before their recording on a physical medium or their transmission by e-mail. It also recommends keeping the decryption password confidential by transmitting it through another channel.84. In view of all of these elements, the Restricted Committee considers that the aforementioned facts constitute a breach of Article 32 of the GDPR.III. On corrective measures and their publicity85. Under the terms of III of article 20 of the modified 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 April 27, 2016 or from the 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, 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 not to exceed 10 million euros or, in the case of a company, 2% of the total worldwide annual turnover of the previous financial year, whichever is higher. 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 committee takes into account, in determining the amount of the fine, the criteria specified in the same article 83".86. Article 83 of the GDPR provides that "Each supervisory authority shall ensure that the administrative fines imposed in under this Article for breaches of this Regulation referred to in paragraphs 4, 5 and 6 are, in each case, effective, proportionate and dissuasive", before specifying the elements to be taken into account in deciding whether to impose an administrative fine and to decide on the amount of this fine.87 In defence, the company argues that a sanction is not necessary given all the measures it has taken to remedy the breaches observed and Considers, in any event, that the amount of the administrative fine proposed by the rapporteur is disproportionate in view, in particular, of the low seriousness of the breaches, of the measures taken to remedy them, of her cooperation with the CNIL services and its financial situation, which has deteriorated significantly due to the current health crisis. The company also maintains that 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 is accused: carrying out massive prospecting campaigns by e-mail without the consent of the persons,

absence of easily accessible information and complete on the processing carried out, difficulties encountered in the exercise of their rights by the complainants and data security defects. It stresses that these breaches relate to 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 persons concerned. 89. The Restricted Committee then notes the particularly large number of people affected by these breaches, since in 2019, […] million people received at least one of the ACCOR group newsletters on a valid email address.90. The Restricted Committee holds, finally, that these breaches had direct consequences for the persons concerned, as evidenced in particular by the fact that the CNIL was seized of eleven complaints relating in particular to the right of opposition to receive prospecting messages commercial.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 for breaches of the GDPR, the Restricted Committee recalls that paragraph 3 of Article 83 of the Rules provides that in the event of multiple breaches, as is the case here, the total amount of the fine cannot exceed the amount set for the most serious violation. Insofar as the company is accused of a breach of Articles 12.1, 12.3, 13, 15.1, 21.2 and 32 of the Regulations, the maximum amount of the fine that can be withheld is 20 million euros or 4% of worldwide annual turnover, whichever is higher.93. The Restricted Committee notes that the company's turnover amounted to […] euros in 2021.94. With regard to the amount of the fine relating to the breach of Article L.34-5 of the 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 of the CPCE which transposes the "ePrivacy" directive into domestic law, article 20, paragraph III, of the "IT and Freedoms" law gives it jurisdiction to pronounce various sanctions, in particular an administrative fine, the maximum amount of which may be equivalent to 2% of the total worldwide annual turnover of the previous financial year achieved by the data controller. In addition, the determination of the amount of this fine is also assessed with regard to the criteria specified by Article 83 of the GDPR.95. To assess the proportionality of the fine, the restricted committee took into account that the company had complied with all of the breaches noted and that some of them, in connection with the exercise of rights of individuals, were not of a structural nature. It further notes that the company cooperated fully with the CNIL.96. The restricted committee also takes into account, in determining the amount of the fine imposed, the financial situation of the company. In this regard, the company reports a decrease in its turnover in 2020 and 2021 compared to 2019. Indeed, the turnover of the company amounted to […] in 2019, [… ] in 2020 and […] in 2021. 97. Finally, the Restricted Committee takes note of EDPS decision No. 01/2022 concerning the dispute relating to

the draft decision of the French supervisory authority concerning Accor SA pursuant to Article 65(1)(a) GDPR. In particular, it notes that the EDPS instructed the CNIL to re-examine the elements on which it relied to calculate the amount of the fine, in order to ensure that the said fine meets the deterrent effect criterion provided for by the 83(1) GDPR.98. Therefore, in view of the economic context caused by the Covid-19 health crisis, its consequences on the financial situation of the company and the relevant criteria of Article 83, paragraph 2, of the GDPR mentioned above, the Restricted Committee considers that the imposition of an administrative fine of 600,000 euros appears justified.99. Finally, the Restricted Committee considers that the publication of its sanction decision for a period of two years is justified in view of the plurality of breaches noted, their seriousness and the number of people concerned. 100. The Restricted Committee specifies that the administrative fine of 600,000 euros against the company ACCOR applies up to 100,000 euros for the breach of the provisions of Article L. 34-5 of the CPCE and up to €500,000 for the company's breaches of the provisions of Articles 12.1, 12.3, 13, 15.1, 21.2 and 32 of the Regulations. FOR THESE REASONSThe Restricted Committee of the CNIL, after having deliberated, decides to: pronounce against the company ACCOR SA an administrative fine of 600,000 euros for all the breaches observed, which breaks down as follows: follows: 100,000 (one hundred thousand) euros for the company's breach of Article L. 34-5 of the Post and Electronic Communications Code; 500,000 (five hundred thousand) euros for breaches by the company of 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 April 27, 2016. make public, on the CNIL site and on the Légifrance site, its deliberation, which will no longer identify the company by name at the end of a period of two years from its publication. Chairman Alexandre LINDEN This decision is likely to the subject of an appeal before the Council of State within two months of its notification.