Deliberation SAN-2020-018 of December 8, 2020 National Commission for Computing and Liberties Nature of the deliberation: Sanction Legal status: In force Date of publication on Légifrance: Wednesday January 06, 2021 Deliberation of the restricted committee n°SAN-2020-018 of 8 December 2020 concerning the company NESTOR SASThe National Commission for Computing and Liberties, meeting in its restricted formation composed of Mr Philippe-Pierre CABOURDIN, vice-president, Mrs Dominique CASTERA, Mrs Anne DEBET and Mrs Christine MAUGÜE, members; Convention No. 108 of the Council of Europe of January 28, 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 April 27, 2016 relating to the protection of personal data and the free movement of such data; Having regard to law no. 78-17 of 6 January 1978 relating to data processing, files and freedom és modified, in particular its articles 20 and following; Considering the ordinance no. 2020-306 of March 25, 2020 relating to the extension of the periods expired during the period of health emergency; the application of law no. 78-17 of January 6, 1978 relating to data processing, files and freedoms; Considering deliberation no. 2013-175 of July 4, 2013 adopting the internal regulations of the National Commission for Data Processing and freedoms; Having regard to referrals nos […], […], […], […] and […]; Having regard to decision no. 2019-082C of 24 April 2019 of the President of the National Commission for information technology and freedoms to instruct the Secretary General to carry out or have carried out a mission to verify the processing carried out by this organization or on behalf of the company NESTOR; Having regard to the decision of the President of the National Commission for information technology and freedoms appointing a rapporteur before the restricted formation e, dated December 19, 2019; Having regard to the report of Mr. François PELLEGRINI, commissioner rapporteur, notified to NESTOR on February 28, 2020; Having regard to the written observations submitted by NESTOR on August 21, 2020; Having regard to the rapporteur's response to these observations notified on September 18, 2020 to the board of the company; Having regard to the new written observations submitted by the board of the company NESTOR, received on October 16, 2020, as well as the oral observations made during the restricted training session; Having regard to the internal procedure for managing requests to exercise rights submitted by the Board of NESTOR on November 6, 2020; Having regard to the other documents in the file; Were present at the restricted training session of November 5, 2020: Mr. François PELLEGRINI , statutory auditor, heard in his report; As representatives of NESTOR:[…];[…];[…];[…];[…]. The company NESTOR having the floor last;The restricted committee adopted the following decision:I.Facts and procedureThe company NESTOR SAS (hereinafter the company) is a simplified joint stock company

created in February 2015, whose activity is the preparation and delivery of meals for office workers, ordered from the company's website nestorparis.com and a mobile application. Its head office is located at 113, rue Victor Hugo in Levallois-Perret (92300). In 2018, NESTOR SAS generated revenue of around […] euros and a negative net result of around […] euros. In 2019, the company achieved a turnover of approximately […] euros and a negative net result of approximately […] euros. The NESTOR company employs around 74 people. On May 14, 2019, the company listed 169,768 customer accounts created via its site and mobile application. entry of four complaints by people who are not customers of the company, indicating that they have received prospecting emails from the latter without their having given their prior consent (requests n° […], […], […] and […]). These emails contained information relating to commercial offers and menus offered by the company. Some complainants informed the CNIL that the company had told them that it had reconstituted their email address, in order to contact them, based on the format of their company's email address from data disseminated on the company's professional social network […]. In addition, a complainant indicated that she was encountering difficulties in objecting to the processing of her personal data by the company for prospecting purposes by e-mail (request no. […]). Several complainants also indicated that despite their unsubscription from the newsletter received by email, they continued to receive prospecting messages in this way. Finally, two complainants indicated that they had asked the company, in vain, for a copy of their personal data. concerning processed by it, as well as several information relating to the purpose of the processing, the recipients of the data, the retention periods of the data or the source of their data (requests n° […] and […]). On May 3, 2019, pursuant to decision no. society. The purpose of this assignment was to verify compliance by this company with all the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the Regulation or the GDPR) and the law n ° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms (hereinafter the law of January 6, 1978 modified or the Data Protection Act). During this control mission, the delegation followed the registration process of a person on the website as well as on the company's mobile application and created an account in the name of the CNIL. It has thus carried out checks in connection with the data provided by the persons when registering, the information relating to the protection of personal data provided to the persons concerned as well as the security measures put in place by the company with regard to passwords associated with the accounts. On May 14, 2019, a delegation from the CNIL carried out an inspection mission at the company's premises, pursuant to the aforementioned decision no. 2019-082C. During this check, the company told the delegation that it was revamping its website in order to comply with the GDPR, particularly with regard to informing

people and the means of opposing the receipt of the newsletter. The company also explained to the delegation how it builds its prospect database. Verifications were finally carried out with regard to the follow-up to the complaints referred to the CNIL, with regard to the rights of access and opposition of individuals. In response to a request of June 21, 2019, the company provided the CNIL delegation of control, by email of the following July 3, with information relating to the source of the personal data contained in its prospect database. Finally, by email of September 11, 2019, the company provided the CNIL with information relating to the legal basis of the processing implemented for commercial prospecting purposes, the right of opposition as well as the retention periods for the data of the prospects and customers. For the purpose of examining these elements, the President of the Commission appointed Mr François PELLEGRINI as rapporteur, on December 19, 2019, on the basis of article 22 of the law of January 6, 1978 amended in its version applicable on the day of designation. On February 20, 2020, in order to update the findings already made, a delegation from the CNIL carried out a new online inspection mission of the nestorparis.com site and the mobile application of the society. The delegation again created an account in the name of the Commission, on the website and the mobile application, and carried out checks relating to the transparency of the information provided to individuals and the robustness of the passwords associated with the accounts.Following his investigation, the rapporteur had NESTOR SAS notified, on February 28, 2020, of a report detailing the breaches of the GDPR that he considered constituted in this case.This report proposed to the restricted committee of the Commission to issue an injunction to bring the processing into compliance with the provisions of Articles L. 34-5 of the Postal and Electronic Communications Code (hereinafter the CPCE) and 12, 13, 15 and 32 of the Regulation, together with a fine of five hundred euros per day of delay at the end of a period of three months following the notification of the deliberation of the restricted formation, as well as an administrative fine. It 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. of May 7, 2020 indicating to the company that it had one month to submit its written observations pursuant to the provisions of Article 40 of Decree No. 2019-536 of May 29, 2019. March 11, 2020 , through its counsel, the NESTOR company sought, by reasoned letter, a period to produce its observations. By email of March 18, 2020, the chairman of the Restricted Committee informed NESTOR that it could produce its observations in defense until April 20, 2020. On April 8, 2020, pursuant to Order No. 2020-306 of March 25, 2020 relating to the extension of the deadlines expired during the health emergency period and the adaptation of procedures during this same period, taken pursuant to emergency law n ° 2020-290 of March 23, 2020 to make faced with the Covid-19 epidemic, the

chairman of the restricted committee informed the company that it had additional time to submit its observations to the rapporteur's report, until August 24, 2020. On August 21, 2020, through its counsel, the company filed submissions. The rapporteur responded to it on September 18, 2020. On September 10, 2020, the Commission's departments sent the company a notice to attend the restricted training session of November 5, 2020. By email dated August 25, 2020, on the basis of article 40, paragraph 4, of decree no. 2019-536 of May 29, 2019 taken for the application of the Data Protection Act (hereinafter the decree of May 19, 2019), the rapporteur asked the president to the restricted committee an additional period of fifteen days to respond to the company's observations, which was granted to it on August 27, 2020. The company was informed of this on the same day. On October 16, the company produced new observations in response to those of the rapporteur. The company and the rapporteur presented oral observations during the restricted committee meeting of November 5, 2020. II. Grounds for the decision A. On the regularity of the procedure1. On the grievance based on the lack of powers of the restricted committeeThe company considers that the restricted committee only has the power to order the measures referred to in Article 20 III of the Data Protection Act in the presence of persistent breaches. first, it argues that this analysis stems from the interpretation of the terms of the law, Article 20 III of the Data Protection Act providing for the possibility for the restricted formation to have recourse to the measures provided for in the aforementioned article 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 rapporteur maintains that the interpretation of article 20 III of the Data Protection Act presented by the company cannot be followed. The legislator intended to allow the restricted formation of the CNIL to pronounce a sanction, in particular pecuniary, including in the event of a breach duly noted but for which a formal notice would be without object, the breach having ceased and no longer calling for correction. .The Restricted Committee considers that the measures taken by a data controller to put an end to a breach observed, if they justify that no formal notice or injunction should be addressed to it for the future, do not deprive it of the possibility of order a corrective measure, and in particular an administrative fine, insofar as bringing the controller into compliance does not have the effect of eliminating the existence of past breaches. It emphasizes that this interpretation of Article 20 of the Data Protection Act is in line with the GDPR in that this article aims to hold data controllers accountable. The corrective measures falling within the powers of the CNIL's restricted formation can be taken directly in all cases, whether or not the breach can still be brought into compliance. Recital 148 of the GDPR thus specifies that any breach of this Regulation may be subject to sanctions: In order to strengthen the application of the rules of this Regulation, sanctions including

administrative fines should be imposed for any breach of this Regulation, in addition to or instead of appropriate measures imposed by the supervisory authority under this Regulation. […]. However, due consideration should be given to the nature, gravity and duration of the breach, the intentional nature of the breach and the measures taken to mitigate the damage suffered, the degree of responsibility or any relevant breach previously committed, how the supervisory authority became aware of the breach […]. The criterion of the duration of the breach therefore applies both to a completed breach and to a persistent breach. preparatory work of the law of October 7, 2016, that the restricted formation of the CNIL may, without prior formal notice, sanction a data controller whose breaches of the obligations incumbent on him are not likely to be regularized, or that they are unlikely to be, or that it has already been remedied. (CE, n° 423559, April 17, 2019, Association for the development of hearths). Secondly, the company maintains that the absence of prescription rules for breaches in the Data Protection Act and the GDPR demonstrates that only breaches in progress on the day of the restricted training session can be sanctioned and that an interpretation otherwise would come up against the case law adopted by the European Court of Human Rights according to which the rules of limitation are a condition of a fair trial. The rapporteur recalls that the Commission received four complaints between 2018 and 2019, that checks were carried out by the CNIL delegation in May 2019 and February 2020 and that the rapporteur appointed in December 2019 for the purpose of examining these elements notified his report on February 28, 2020. The Restricted Committee therefore considers that the Commission has applied a reasonable time between the observations made by the delegation of control and the referral to the restricted committee. The restricted committee is responsible for this regard that it follows from the case law of the Court of Justice of the European Union that the obligation of the administration to act within a reasonable time, the observance of which is liable to be reviewed by the judge of the European Union , offers a sufficient level of protection in situations where no limitation period is set by law. (CJEU, n° T-342/14, Order of the General Court, CR v European Parliament and Council of the European Union, 12 December 2014). The Restricted Committee thus considers that the company is not justified in maintaining that it only has the power to pronounce the measures referred to in Article 20 III of the Data Protection Act in the presence of persistent and current breaches, and that the procedure followed before it violated the right to a fair trial.2. On the grievance alleging ignorance of the scope of referral to the restricted trainingThe company considers that the restricted training cannot rule on the alleged breach of the provisions of article L. 34-5 of the postal and electronic communications code (hereinafter the CPCE). Firstly, the company maintains that the control decision n° 2019-082C of the president of the CNIL, the acts of investigation or instruction

which followed, as well as the decision of the president of December 19, 2019 appointing of a rapporteur and referral to the Restricted Committee, do not refer to Article L. 34-5 of the CPCE. Consequently, the Restricted Committee could not rule on the alleged breach of the provisions of Article L. 34-5 of the CPCE without disregarding the scope of its referral. The company also maintains that the Restricted Committee cannot rely on the elements of the investigation to establish a breach of Article L. 34-5 of the CPCE without disregarding the principles of specialty of the investigation - requiring that the investigation be carried out within the limits of its scope defined by the decision which constitutes it the legal basis – and of fairness of the investigation – obliging the investigators to mention the object and the legal basis of the investigations. or instruction that result are carried out within this framework. Article 8 of the law sets out the missions of the CNIL and specifies in particular that it ensures that the processing of personal data is implemented in accordance with the provisions of this law and the other provisions relating to the protection of data. personal data provided for by laws and regulations, European Union law and France's international commitments. The rapporteur thus maintains that the modified law of 6 January 1978 refers to all the provisions relating to the protection of personal data provided for by the legislative and regulatory texts. The prospecting operations referred to in Article L. 34-5 of the CPCE concern the processing of personal data and this article gives the CNIL jurisdiction to ensure compliance when the data processed is of a personal nature. Paragraph 6 of Article L. 34-5 of the CPCE thus provides that: The National Commission for Computing and Liberties monitors, with regard to direct prospecting using the contact details of a subscriber or a person physical, in compliance with the provisions of this article by using the skills recognized by the law n ° 78-17 of January 6, 1978 mentioned above. The Restricted Committee considers that it is in this context that the CNIL delegation carried out three checks on the company and that the Restricted Committee was seized. The Restricted Committee also emphasizes that this interpretation was adopted by the Board which recognized the competence of the CNIL to ensure compliance with the provisions of article L. 34-5 of the CPCE (CE, n° 368624, March 11, 2015, TUTO4PC Company). Consequently, the restricted training was regularly seized and it is without disregarding the principles of specialty and loyalty that it bases itself on the elements of the controls to examine the acts committed by the company with regard to the provisions of article L 34-5 of the CPCE.Secondly, the company maintains that, if the restricted committee could be seized of alleged breaches of Article L. 34-5 of the CPCE, the CNIL investigators cannot carry out corrective measures. investigation to this effect, this prerogative being reserved, by virtue of paragraph 7 of article L. 34-5 of the CPCE, to agents of competition, consumption and the repression of fraud and to officials responsible for missions of economic protection of consumers.

However, the rapporteur recalls that the provisions of paragraph 6 of article L. 34-5 of the CPCE provide that the CNIL uses its powers to ensure compliance with the aforementioned article for this which concerns direct prospecting u using the contact details of a subscriber or a natural person. These powers are specified in the law of January 6, 1978 as amended and they include, under articles 19 and 20, powers of investigation and sanction. The restricted committee thus considers that CNIL agents are competent to carry out control missions under the provisions of Article L. 34-5 of the CPCE in order to ensure compliance with this article with regard specifically to direct marketing using the contact details of a subscriber or a natural person.3. On the vagueness of the grievances against the companyThe company points out that the grievances notified in the sanction report are not limited either materially or in time and do not meet the standard of proof required in criminal matters. Consequently, the company maintains that it is not in a position to effectively exercise its rights of defence. CNIL on May 3 and 14, 2019 and February 20, 2020. These breaches were materially and temporally characterized in the report notified to the company. The rapporteur thus considers that he has enabled the company to usefully exercise its rights of defence. 'thus the standard of proof required before the restricted panel must not meet the requirements of criminal matters but those set by the Data Protection Act and its implementing decree. In this respect, the rapporteur also recalls that each grievance is supported by elements from control operations in the context of which a report, including annexed documents, is drawn up. In view of all of these elements, the Restricted Committee considers that the delegation of control ensured a high standard of proof which makes it possible to guarantee their reliability, that the shortcomings have been materially and temporally characterized in the report notified to the company and that thus , the company cannot claim that the grievances against it are imprecise. electronic communications pursuant to Article L. 34-5 of the CPCE1. On the lack of consent of persons to receive commercial prospecting messagesArticle L. 34-5 of the CPCE provides: Direct prospecting by means of an automated electronic communications system within the meaning of 6° of Article L is prohibited 32, 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. For the application of this article, Consent means any manifestation of free, specific and informed will by which a person accepts that personal data concerning him be used for the purpose of direct marketing. […] . 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 competences which are recognized by the aforementioned law n° 78-17 of January 6, 1978. To this end, it may in particular receive, by any

means, complaints relating to breaches of the provisions of this article […]. The rapporteur maintains that the company does not obtain the consent of persons whose personal data is accessible on the Internet, prior to sending commercial prospecting messages. The rapporteur noted that, during the inspection of March 14, 2019, the company has indicated to the CNIL's delegation of control that it builds its prospect database from personal data accessible online on the company's professional social network website [...]. She specified working with two companies, A and B, for the creation of personal databases intended for commercial prospecting. First of all, company A establishes prospecting lists containing the surnames and first names of prospects, associated to the name of the company in which they work. This data is collected by the Sales Navigator service offered by the company [...], which lists all the people working in a company and a region. Subsequently, the NESTOR company transfers the file established by company A, to company B, which proceeds to enrich this file, in particular by adding the professional electronic address of the persons. The company indicated to the delegation of control of the CNIL that the files compiled with the help of these two companies allow it, subsequently, to solicit people likely to be interested in its services. To do this, it is finally up to another company, company C, to send these prospects information emails and promotional codes on behalf of the company NESTOR. The company informed the delegation that, 635,033 prospects have received, since 2017, such prospecting e-mails. The company maintains that the legal basis of the processing for the purpose of commercial prospecting of people, carried out on their professional e-mail address is the legitimate interest of the data controller. The company also specified that it had the ambition to become the benchmark for business lunch delivery services in the professional premises of its customers and that it was therefore vital for it to acquire a base of potential professional customers. noted that initially, the company had informed the delegation that it did not collect the consent of the people since this prospecting emailing - whose legal basis is the legitimate interest of NESTOR - intervenes strictly within the professional framework that constitute business lunches (professional e-mail address, delivery to professional premises, during the client's business hours, etc.). In its response to the sanction report, the company then argued that it secures individuals' consent to their personal data being used for targeted advertising purposes by choosing the company's services [...], whose confidentiality policy provides for the communication of the personal data of its members to advertisers: By choosing the services of the company [...], NESTOR has taken the necessary precautions to ensure the consent of prospects to that their data be used for advertising targeting purposes and that they be communicated to advertisers. In this case, NESTOR uses the services of the company [...] as one of its subcontractors. The company [...] therefore acts in the name and on behalf of

NESTOR, which can therefore legitimately rely on the consent obtained by the company [...] on its behalf. The Restricted Committee notes that the professional social network [.. .] allows people to register in order to get in touch with professionals, as part of a job search, or to share information with their professional network and to extend this professional network. The Restricted Committee therefore considers that the prospecting messages sent by the company for the sale of meals in people's workplaces have little connection with the professional activity of the prospects. The Restricted Committee also considers that the prospects approached were not aware of the collection of their personal data by the company and that it carried out prospecting by email and SMS, without having previously obtained their consent. In addition, the Restricted Committee underlines that the prospecting commercial carried out by the company falls within the scope of paragraph 1 of article L. 34-5 of the CPCE which provides for a specific legal basis based on consent, thus ruling out the possibility of legitimate interest as a legal basis for these prospecting operations. In such circumstances, the Restricted Committee considers that the company is required to obtain the prior, free, specific and informed consent of persons to receive direct prospecting messages by e-mail, in accordance with Article L. 34-5 of the CPCE, which it does not do. The Restricted Committee considers that the deletion of personal data collected without the consent of persons is necessary insofar as these data are processed without a legal basis, the persons concerned having not given their consent. She notes that the company told her that it had destroyed its database containing the personal data of prospects, without however justifying it. It also considers that the deletion of the data of prospects who have now become customers of the company is not necessary. Under these conditions, the Restricted Committee considers that the company has disregarded the provisions of Article L. 34 -5 of the CPCE.2. On the lack of consent of persons creating an account on the company's website or application, upon receipt of commercial prospecting messages The rapporteur maintains that the company does not obtain the consent of persons creating an account on its website or its application for the processing of their personal data for the purposes of commercial prospecting by e-mail. The rapporteur noted that when an account was created by the CNIL delegation on the company's website, at On the occasion of the check carried out on 3 May 2019, no procedure aimed at obtaining consent to the collection and processing of data for the purposes of commercial prospecting by e-mail was put in place. The rapporteur also noted that the delegation from the CNIL, which had not placed any order or given such consent, received prospecting emails and text messages from the company. Such mailings continued until August 2019 and are recognized by the company. The restricted formation considers that the company is required to obtain the prior, free, specific and informed consent of the persons

creating an account on the website or on the application of the company, to receive direct prospecting messages by e-mail, in accordance with paragraph 1 of article L. 34-5 of the CPCE. obtaining consent from September 11, 2019 on the website and March 5, 2020 on the application, and its compliance with article L. 34-5 of the CPCE since as soon as a customer account is created on the website or on the NESTOR application, the user must fill in a registration form, one of the sections of which consists in informing, in particular, his choice to receive by email the menus of the day, the week, or the offers specials by ticking one of the corresponding boxes. ondantes.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 completely complied on the date of the closing of the investigation.C. On the breach relating to the obligation to inform persons pursuant to Articles 12 and 13 of the GDPR Under the terms of paragraph 1 of Article 12 of the GDPR: The controller takes 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, comprehensible and easily accessible manner, in terms clear and simple […] . 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. The rapporteur notes that, as evidenced by the findings made during the online check of February 20, 2020, the information made available to users of the site and the application was neither complete within the meaning of Article 13 of the Regulations nor easily accessible within the meaning of Article 12 of the Regulations. In defence, the company indicated that it had made corrections, within the framework of the procedure, in order to issue training in accordance with the requirements of the GDPR. 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. It notes, in this regard, that this provision must be interpreted in the light of recital 61 of the Regulation, according to which: information on the processing of personal data relating to the data subject should be provided to him at the time when these data are 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 11 April 2018 (hereinafter the guidelines on transparency), which recalls that the data subject shouldn't have to search for the information but should be able to access it right away. In

this case, the Restricted Committee notes that the form for collecting personal data allowing registration on the company's website did not include all the information required by Article 13 of the GDPR or did not refer not to a dedicated page containing all the information provided for by the GDPR. Thus, the Restricted Committee notes that no information relating to the legal bases of the processing implemented, the recipients or the categories of recipients of the data, the retention period of the latter or the existence of the right to introduce a complaint to a supervisory authority was provided. In addition, the Restricted Committee considers that the privacy policy present on the home page of the website was incomplete with regard to information relating to data retention periods of a personal nature of prospects. The Restricted Committee also considers that the privacy policy does not allow people to know, for each processing operation, what legal basis it is based on, nor the legitimate interest pursued by the data controller when a processing of personal data is based on this legal basis. The Restricted Committee further considers that the privacy policy is i imprecise with regard to the information relating to the recipients of the personal data since it is indicated that the data may be transmitted to certain partners […]. The Restricted Committee considers that if the company is not required to provide the identity of all the recipients of the data, it must however, at least, inform the persons of the categories of recipients of the data. Finally, the Restricted Committee observes that no information relating to the protection of personal data was provided to persons creating an account on the mobile application. It nevertheless notes that, within the framework of the procedure, the company justified having taken in accordance with articles 12 and 13 of the GDPR. First of all, concerning the registration form on the website, the company justifies having inserted in the form, a link entitled Your personal data referring to the privacy policy. The company also justifies having brought its privacy policy into compliance, which now contains all the information required by Article 13 of the GDPR. Finally, the company indicates that it has redesigned its mobile application since March 5, 2020, and that the registration page and the application's home page have since offered a link to the privacy policy. confidentiality, which also contains all the information required by article 13 of the GDPR. on the closing date of the investigation. D. On the breach relating to the obligation to respect the right of access of individuals pursuant to Article 15 of the GDPR Article 15, paragraph 1, of the GDPR provides that the right for a person to obtain from the controller access to personal data concerning him and in particular when the personal data are not collected from the person concerned, any information available as to their source. It is also provided for in paragraph 3 of the same article that the controller provides a copy of the personal data undergoing processing. Finally, Article 12.4 of the GDPR provides that the controller provides 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 event. within one month of receipt of the request.During the investigation of two complaints received by the CNIL (referrals no. […] and […]), it appeared that the company failed to its obligation to provide complainants with a copy of the personal data concerning them that it held in its database, as well as information relating to the source of this data. With regard to the first complaint (No. […]), the company maintains that after the complainant, Mr. X, referred the matter to the CNIL, it sent him supporting documents specifying that the unsubscription from the lists had been unsuccessful due to the redirection of e-mails from a second address. email to the first .Concerning the second complaint (no. […]), the company maintains that, after the complainant, Mr. Y, referred the matter to the CNIL, it would have communicated to him the source of his personal data. The company adds that the request made by Mr. Y was a portability request under Article 20 of the GDPR and not a request relating to the right of access under Article 15 of the GDPR. company argued that it had not understood the scope of these two requests. Firstly, the Restricted Committee notes that it appears from the complaint lodged by Mr X that the latter asked the company, by email from the November 8, 2018, that a copy of all of his personal data be sent to him as well as information on the source of his data. The Restricted Committee notes that the company only indicated in return to Mr X that he had indeed been unsubscribed from its mailing lists. The Restricted Committee thus notes that it emerges from the answers provided by the company to the complainant that it did not communicated a copy of his personal data, nor their source, as requested. Secondly, the Restricted Committee notes that it appears from the complaint filed by Mr Y that the company responded to his request for access of December 14, 2018 more than five months later, i.e. May 14, 2019. The Restricted Committee considers that the company did not indicate the source of the data, but merely told Mr. Y that he had reconstructed his email address on the basis of another e-mail address without indicating to him that this other e-mail address had been obtained via the professional social network [...]. Thus the company only listed the type of data it processed. The Restricted Committee also considers that it was clear that this was not a request for portability, in particular as Mr. Y precisely indicated in his email sent to the company on December 14, 2018 […] I would like to introduce a subject access request under the European Data Protection Regulation (GDPR/GDPR) to obtain a copy of any information you maintain about me, whether in computerized or manual form, in relation to my information […] . In any event, whether it is a request addressed to the company under Article 15 of the GDPR or on the basis of its Article 20, the Restricted Committee considers that the company has not granted it since no set of data concerning him has not been communicated to him in any format whatsoever. structural nature of the breach alleged against the company. The Restricted Committee also

considers that the company had still not complied on the closing date of the investigation.E. On the breach relating to the obligation to ensure the security of personal data in application of Article 32 of the GDPRArticle 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 likelihood and severity of which 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 others, as required: a) pseudonymization and encryption personal data; b) the means to guarantee the constant confidentiality, integrity, availability and resilience of the processing systems and services; c) the means to restore the availability of the personal data and the access to them in a timely manner in the event of a physical or technical incident; d) a procedure aimed at regularly testing, analyzing and evaluating the effectiveness of the measures s technical and organizational measures to ensure the security of the processing. […]. The rapporteur noted that during the online check of 3 May 2019, the delegation noted that a password consisting of a single character was accepted when creating an account by a person via the mobile application and that a six-character password was accepted when creating an account via the company's website. During the inspection of February 20, 2020, the rapporteur noted that if the company had taken measures to strengthen the composition of the password required for the creation of an account on the company's website, a password consisting of a single character was always accepted for the creation of an account on the mobile application. rapporteur therefore maintains that the password for connecting customers to their personal space, accessible from the mobile application, was still insufficiently robust to ensure the security of personal data, as it was made up of a single character. defence, the storytelling society ste the deliberate nature of the security defect for which it is accused and indicates that it modified the measures relating to the management of passwords for connecting to user accounts on its mobile application when it was updated, the March 5, 2020.The restricted formation considers that the length and complexity of a password remain basic criteria for assessing its strength. It notes in this respect that the need for a strong password is also underlined by the National Information Systems Security Agency, which indicates that a good password is above all a strong password, c is to say difficult to find even with the help of automated tools. The strength of a password depends on its length and the number of possibilities existing for each character composing it. Indeed, a password consisting of lowercase letters, uppercase letters, special characters and numbers is technically more difficult to discover than a password consisting only of lowercase letters. 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 (e.g. captcha) and/or blocking of the account after several authentication attempts or unsuccessful. In this case, the Restricted Committee considers, firstly, that with regard to the undemanding rules governing their composition, the robustness of the passwords accepted by the company was too weak, leading to a risk of compromise of the associated accounts and the data they contain. The Panel notes, however, that the company justifies having modified the measures relating to the management of login passwords to user accounts. Consequently, the Restricted Panel considers that the breach relating to the he obligation to ensure the security of personal data has been established, but in view of the elements provided by the company during the procedure, there is no need to issue an injunction.III. On corrective measures and their publicity Under the terms of III of article 20 of the law of January 6, 1978 as amended: When the data controller or its subcontractor does not comply with the obligations resulting from regulation (EU) 2016/679 of 27 April 2016 or of 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: […] 2° An injunction to bring the processing into conformity with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or from this law or to satisfy the requests presented by the person concerned in order to exercise their rights, which may be accompanied, except in cases where the processing is put in implementation by the State of a penalty payment, the amount of which may not exceed €100,000 per day of delay from the date set by the restricted committee; […] 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 turnover total worldwide annual business for the previous fiscal year, whichever is greater. 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 committee takes into

account, in determining the amount of the fine, the criteria specified in the same article 83. Article 83 of the GDPR provides that each supervisory authority shall ensure that the 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. power to impose a fine for a breach of article L. 34-5 of the CPCE. In addition, the company notes that articles 20 of the law of January 6, 1978 and 83 of the GDPR do not indicate any applicable fine ceiling for a breach of article L. 34-5 of the CPCE and do not specify the criteria to be taken into account in determining the amount of the fine. As the restricted committee has previously demonstrated, paragraph 6 of article L. 34-5 of the CPCE gives full competence to the CNIL to ensure compliance for the matter which concerns it by using the skills which are recognized by the Data Protection Act. Article 20, paragraph III, point 7) of the amended law of January 6, 1978 specifies that the CNIL has the power to pronounce administrative fines, sets the ceilings and makes a reference to article 83 of the GDPR to know the criteria to be taken into account in determining the amount of these fines. Thus, contrary to what the company seems to maintain, it is not article 83 of the GDPR which is applied in this case to allow the restricted formation to impose a fine, but article 20 of the law of January 6, 1978, the application of which is expressly provided for by paragraph 6 of article L. 34-5 of the CPCE and which, for its part, makes a reference to the criteria of article 83 of the GDPR for the determination of the amount of the fine. With regard to the aforementioned provisions, the Restricted Committee therefore considers that it has the power to impose a fine for a breach of Article L. 34-5 of the CPCE. Secondly, the company maintains that the sanction report does not contain any reasoning with regard to the legal criteria justifying the pronouncement of a fine and its amount. The company adds that the proposed fine is disproportionate to the economic context caused by the Covid-19 health crisis. It points out that its financial situation has already been severely impacted by this crisis, so that imposing a fine on it would seriously compromise the sustainability of its activities. In this respect, the company produces an accounting certificate certifying that the estimated available cash for the month of December 2020 would amount to […] euros. The Restricted Committee considers, on the contrary, that the imposition of an administrative fine is justified with regard to the criteria posed by Article 83 paragraph 2 of the GDPR. With regard to the breach of Article L. 34-5 of the GDPR, the Restricted Committee considers that the company has shown gross negligence in considering that it could, to constitute its base of prospects, to abstain from obtaining the consent of the people. The seriousness of this violation is proven due in particular to the particularly large number of people affected by the breach and the fact that the CNIL has received several complaints, which are at the origin of the CNIL's control procedure. of the breach of

the obligation to inform individuals, the Restricted Committee recalls that information and transparency relating to the processing of personal data are essential obligations incumbent on data controllers so that individuals are fully aware of the the use that will be made of their personal data, once they have been collected. Therefore, the Restricted Committee considers that an administrative fine should be imposed with regard to the breaches of Articles L. 34-5 of the CPCE and 12 and 13 of the GDPR. With regard to the breach of the obligation to respect the right of access of individuals, pursuant to Article 15 of the GDPR, the restricted training notes that, in the context of the procedure, the company argued that it had not understood the scope of the requests and that the two complaints received do not demonstrate a structural nature of the breach alleged against the company. With regard to the breach of the obligation to ensure data security, pursuant to Article 32 of the GDPR, the Restricted Committee considers that, in view of the measures taken by the company, it has demonstrated good faith in the framework of the procedure. Consequently, the Restricted Committee considers, in view of the circumstances of the case, that there is no reason to base its fine on the basis of these two breaches, although they are characterized. amount of the administrative fine, the Restricted Committee recalls that paragraph 3 of Article 83 of the Rules provides that in the event of multiple violations, as is the case here, the total amount of the fine does not may exceed the amount set for the most serious breach. Insofar as the company is accused of breaching Articles L. 34-5 of the CPCE and 12 and 13 of the Regulations, the maximum amount of the fine that can be withheld is 20 million euros or 4% annual worldwide turnover, whichever is higher. However, the Restricted Committee also takes into account, in determining the amount of the fine imposed, the financial situation of the company. The company reported its estimated turnover for the year 2020, for the period from January 1 to July 31, at […] euros, a sharp drop compared to 2019 when its turnover had reached […] euros at 31 December. The company also reports an estimate for the period from January 1 to July 31, 2020, of its earnings before interest, taxes and depreciation, negative […] euros. Therefore, in view of the economic context caused by the health crisis of Covid-19, its consequences on the financial situation of the company and the relevant criteria of Article 83, paragraph 2, of the Regulations mentioned above, the Restricted Committee considers that the imposition of a fine of 20,000 euros appears to be both effective, proportionate and dissuasive, in accordance with the requirements of Article 83, paragraph 1, of this Regulation.Thirdly, an injunction to bring the processing into compliance with the provisions of Articles L. 34-5 of the CPCE, 12, 13, 15 and 32 of the GDPR was proposed by the rapporteur when notifying the report. With regard to the breach relating to the obligation to obtain the consent of the person concerned by a direct prospecting operation by means of of one automated electronic communications system

pursuant to Article L. 34-5 of the CPCE, the Restricted Committee considers that the company having taken satisfactory measures to obtain the consent of persons when creating an account on the application and on the website, and having undertaken, within the framework of the procedure, to no longer send direct prospecting messages by e-mail to prospects without their prior consent, the injunction proposed in report no. is no longer necessary. However, the Restricted Committee considers that the company has not demonstrated that it has deleted the database of prospects whose prior, free, specific and informed consent to receive direct prospecting messages by e-mail has not been collected by the company. Consequently, the Restricted Committee considers that an injunction should be issued on this point. With regard to the breach of the obligation to respect the right of access of individuals, pursuant to Article 15 of the GDPR, the company maintains that it has put in place an internal procedure to grant requests made under Article 15 of the GDPR and that it has amended it in order to respond to requests for the right of access in a satisfactory manner. It communicated its internal procedure to the Restricted Committee, in accordance with the latter's invitation, on November 6, 2020. The Restricted Committee considers, however, that the company did not fully respond to the requests for the right of access presented by Mr. X and Mr. Y. Thus, without ignoring the company's steps to comply with the GDPR and the implementation and amendment of its internal procedure, the Restricted Committee considers that the company has still not demonstrated, its compliance with Article 15 of the Rules, failing to satisfy the requests of Mr. X and Mr. Y. The Restricted Committee therefore considers that an injunction should be issued. Fourthly, the Restricted Committee considers that the publicity of the penalty is justified in view of the plurality of breaches noted, their persistence and their seriousness. Indeed, the Restricted Committee considers that, while the company has taken measures within the framework of the sanction procedure allowing the processing of personal data that it carries out to be brought into conformity, it has not however taken into account all the requirements set by article L. 34-5 of the CPCE in terms of obtaining consent, nor those resulting from the Data Protection Act. In addition, the Restricted Committee considers that the practices of the company, which carried out prospecting operations by e-mail in the absence of people's satisfaction, justify the publication of its decision. Finally, the Restricted Committee considers that publication would allow to reinforce the dissuasive nature of the main penalty. thousand) euros for breaches of Articles L. 34-5 of the Postal and Electronic Communications Code (hereinafter the CPCE) and 12 and 13 of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (hereinafter the GDPR),;- issue an injunction against the company NESTOR SAS to bring the processing operations into compliance with the obligations resulting from Articles L. 34-5 of the CPCE and 15 of the GDPR, and in particular r: with regard

to the breach of the obligation to obtain the consent of the person concerned by a direct marketing operation by means of an automated electronic communications system: * Justify the deletion of all personal data previously collected without the consent of prospects; with regard to the breach of the obligation to respect the right of access: *Completely satisfy requests for access rights by communicating a copy of all of their personal data held to the applicants, as well as, where applicable, information relating to the source from which their data come; - to attach the injunction to a penalty payment of 500 (five hundred) euros per day of delay at the end of a period of 3 (three) months following the notification of this deliberation, the proof of compliance must be sent to the restricted body within this period; - make public, on the CNIL site and on the Légifrance site, its deliberation, which will no longer identify the company at the end of a period of two years from its publication. from its notification.