Deliberation SAN-2021-021 of December 28, 2021 National Commission for Computing and Liberties Nature of the deliberation: Sanction Legal status: In force Date of publication on Légifrance: Tuesday January 04, 2022 Deliberation of the restricted committee n°SAN-2021-021 of 28 December 2021 concerning FREE MOBILE The National Commission for Computing and Liberties, meeting in its restricted formation composed of Mr Alexandre LINDEN, President, Mr Philippe-Pierre CABOURDIN, Vice-President, Mrs Anne DEBET, Mrs Christine MAUGÜÉ, Mr Alain DRU and Mr. Bertrand du MARAIS, members; Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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 sector r electronic communications; Having regard to the postal and electronic communications code; Having regard to law no. 78-17 of 6 January 1978 relating to data processing, files and freedoms, in particular its articles 20 and following; Having regard to decree no. 2019 -536 of May 29, 2019 taken for the application of law no. 78-17 of January 6, 1978 relating to data processing, files and freedoms; Having regard to deliberation no. 2013-175 of July 4, 2013 adopting the internal regulations of the National Commission for Computing and Liberties; Having regard to decision no. 2019-188C of September 26, 2019 of the President of the National Commission for Computing and Liberties to instruct the Secretary General to proceed a mission to verify the processing implemented by these organizations or on behalf of the FREE and FREE MOBILE companies; Having regard to the decision of the President of the National Commission for Computing and Liberties appointing a rapporteur before the f Restricted information, dated December 17, 2020; Having regard to the report of Mr. François PELLEGRINI, commissioner rapporteur, notified to the company FREE MOBILE on August 2, 2021; Having regard to the written observations submitted by the company FREE MOBILE on September 13, 2021; Having regard to the response of the rapporteur to these observations notified on October 4, 2021 to the company; Having regard to the new written observations submitted by the company FREE MOBILE on October 22, 2021, as well as the oral observations made during the restricted training session; Having regard to the other documents of the file; Were present, during the session of the restricted committee of November 4, 2021:- Mr François PELLEGRINI, commissioner, heard in his report; As representatives of the company FREE MOBILE:- […];- […]; - […];- […];- […];- […];- […]. The company FREE MOBILE having the floor last; The Restricted Committee adopted the following decision: I. Facts and procedure1. FREE MOBILE (hereinafter "the company"), whose registered office is located at 16 rue de la ville l'Evêque in Paris (75008), is a subsidiary of the ILIAD group. The

company is a mobile phone operator that markets phones and / or mobile plans. Created in 2007, it has approximately 600 employees.2. For the year 2020, the company FREE MOBILE achieved a turnover of […] euros, for a net result of […] euros. As of December 21, 2020, the company had approximately […] subscribers to mobile offers, […].3. Between December 2018 and November 2019, the National Commission for Computing and Liberties (hereinafter "the CNIL" or "the Commission") received 19 complaints against the company FREE MOBILE. The complainants reported in particular on the difficulties encountered in exercising their rights of access or opposition to receiving commercial prospecting messages.4. For the purposes of investigating complaints, two on-site inspection operations at the premises of the FREE company and then of the FREE MOBILE company were carried out in application of decision no. 2019-188C of September 26, 2019 the CNIL. These missions were carried out on January 21 and 22, 2020 respectively. Pursuant to this same decision, a check on documents was also carried out at the companies FREE MOBILE and FREE on June 3, 2020.5. The purpose of these assignments was to verify compliance by FREE MOBILE 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 modified law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms (hereinafter "the modified law of January 6, 1978" or the "Data Protection Act").6. During the first two inspections, the CNIL delegation endeavored to verify the management, by the company FREE MOBILE, of the rights of individuals, and more particularly the way in which it had handled requests to exercise the rights of individuals. seized the Complaints Commission. These checks were also intended to verify the security measures put in place by the company to protect the personal data it processes. At the end of these checks, the reports n° 2019-188/1 and n° 2019-188/2 were notified to the company FREE MOBILE by letter dated January 23, 2020. The company transmitted to the services of the Commission, by emails of 3 and 10 February 2020, the additional documents requested at the end of these inspection missions.8. In view of the answers provided by the company, and with a view to clarifying certain findings previously made, a new documentary check was carried out by the CNIL on June 3, 2020, which resulted in the sending of a questionnaire to the company FREE MOBILE.9. The company sent to the Commission services, by email of June 29, 2020, the additional documents and information requested during this inspection.10. For the purpose of examining these elements, the President of the Commission, on December 17, 2020, appointed Mr François PELLEGRINI as rapporteur on the basis of Article 22 of the law of January 6, 1978 as amended and informed the company by letter dated December 23, 2020.11. At the end of his investigation, the rapporteur, on August 2, 2021, had FREE MOBILE notified of a report detailing the breaches of the

GDPR that he considered constituted in this case. The notification letter for the report informed 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, 2019.12. This report proposed that the restricted committee of the Commission issue an injunction to bring the processing into compliance with the provisions of Articles 15, 16, 21, 25 and 32 of the GDPR, accompanied by a penalty payment for each day of delay at the end of of a period of three months following the notification of the deliberation of the restricted formation, as well as an administrative fine. He also proposed that this decision be made public, but that it would no longer be possible to identify the company by name after the expiry of a period of two years from its publication.13. On September 13, 2021, the company filed its observations in response to the sanction report.14. On September 23, 2021, the rapporteur requested a deadline to respond to the observations made by the company FREE MOBILE. By letter dated September 24, 2021, the chairman of the Restricted Committee informed the rapporteur that he had an additional period of six days to produce his observations. In a letter dated the same day, the company was informed by the chairman of the Restricted Committee that it also had an additional period of six days to submit its observations.15. By letter dated October 4, 2021, the rapporteur's response to the company's observations was sent to him, accompanied by a notice to attend the restricted training session of November 4, 2021.16. On October 22, 2021, FREE MOBILE produced new observations in response to those of the rapporteur.17. The company and the rapporteur presented oral observations during the session of the restricted committee.II. Reasons for decisionA. On FREE MOBILE18's processing responsibility. Article 4, paragraph 7 of the GDPR provides that the controller is "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of treatment ".19. In his report, the rapporteur first emphasizes that the delegation was informed during the on-site inspection of January 21, 2020 that "the company FREE MOBILE is the mobile radio telecommunications operator of the ILIAD group and the company FREE is the operator ILIAD group's fixed telecommunications service" and that "each customer is attached to the FREE company and/or to the FREE MOBILE company" depending on the offer to which he has subscribed. The rapporteur then notes that each of the FREE MOBILE and FREE companies "has its own information system in which [its] customers are listed" and that the "prospect databases are also distributed by company", so that the companies can access their own databases. A common database is also used by each of the companies, on its own behalf, in order to carry out commercial prospecting. Finally, the rapporteur observes that the processing register transmitted to the CNIL delegation indicates that the company FREE MOBILE considers itself responsible in particular for processing relating to the management

of contracts taken out with it by its subscribers and for processing related to prospecting operations. commercial that are carried out with its customers and prospects on its behalf.20. The Restricted Committee notes that these elements have not been contested by FREE MOBILE. It considers that it follows from the foregoing that the company FREE MOBILE must be regarded as responsible for the processing of the personal data of its customers, implemented within the framework of the execution of the mobile telephone subscription contracts, and the people it contacts for commercial prospecting purposes, insofar as it determines the purposes and means of this processing.B. On the grievances of the company in connection with the procedure21. The company considers that the rapporteur failed in his duty of care by sending him, more than eighteen months after the control operations and during the holidays in August, the report proposing to the restricted committee to withhold a sanction for against him. The company argues, on the basis of an average that it states that it established from the decisions of the restricted committee rendered between 2018 and 2021 following an on-site inspection, that the average time for transmission of the procedure to the restricted formation is approximately thirteen months and that, in this case, this period has been extended to eighteen months. The company also claims that it was not given the opportunity to take cognizance, before receipt of the report, of two complaints on which the rapporteur relied to hold against it a breach of its obligation to ensure the security of the processing. Finally, the company is surprised not to have been given formal notice beforehand to correct the shortcomings at the origin of the disputed facts, which would demonstrate the low seriousness of the shortcomings alleged by the rapporteur, in particular with regard to its procedures for security.22. Firstly, the Restricted Committee notes that the applicable texts do not provide for a limit on the period between the conduct of controls and the transmission of a report proposing a sanction. Moreover, the present proceedings took place during the health crisis, which led to an extension of the time limits.23. Secondly, with regard to the two referrals No. 19012802 and No. 19019490 for which the company claims that it was not given the opportunity to read them before receiving the report, the Restricted Committee recalls that the applicable texts do not impose a prior investigation of complaints before the transmission of a report proposing a sanction and do not prevent the rapporteur from bringing them to the attention of the data controller at the stage of his report, the complaints being at this stage occasion paid to the adversarial procedure. Finally, Article 50 of the CNIL's internal regulations only requires that the subject of the complaint be "communicated to the data controller in question […] so that the latter provides all the useful explanations", which was done in this case through the penalty report.24. Thirdly, with regard to the transmission of the report in August and the need for the company to respond to it during the summer holidays, the Restricted Committee observes that

the company benefited from a period of approximately six weeks to produce its first observations, to take account of this period, it being recalled that Article 40 of Decree No. 2019-536 of May 29, 2019 only imposes a minimum period of one month.25. Finally, with regard to the grievance relating to the absence of prior formal notice, the Restricted Committee notes first of all that it is apparent from the provisions of Article 20 of the law "Informatique et Libertés" amended by the law n° 2018-493 of June 20, 2018 that the supervisory authority has a set of corrective measures, adapted according to the specific characteristics of each case, which can be combined with each other and may or may not be preceded by a formal notice . Corrective measures can be taken directly in all cases.26. The Restricted Committee also notes that the Constitutional Council (Cons. const., June 12, 2018, No. 2018-765 DC) did not express a reservation regarding the possibility for the President of the CNIL to initiate proceedings sanction without prior notice. Finally, the Restricted Committee recalls that the Council of State has ruled (EC, October 9, 2020, SERGIC Company, No. 433311) that "it clearly follows [from the provisions of Article 20 of the law of January 6, 1978 as amended], that the pronouncement of a sanction by the restricted formation of the CNIL is not subject to the prior intervention of a formal notice to the controller or its subcontractor by the president of the CNIL […]".27. Consequently, the Restricted Committee considers that this procedure and the various actions carried out in this context have not infringed the company's rights of defense.C. On the qualification of the facts with regard to the GDPR1. On the breach of the obligation to respect the right of access of individuals to personal data concerning them28. Article 12, paragraph 3, of the GDPR provides that "The data controller shall provide the data subject with information on the measures taken following a request made pursuant to Articles 15 to 22, as soon as possible and in any event within one month of receipt of the request. If necessary, this period may be extended by two months, taking into account the complexity and the number of requests. The data controller shall inform the data subject of this extension and the reasons for the postponement within one month of receipt of the request". In addition, under the terms of paragraph 4 of this article "if the data controller does not respond to the request made by the data subject, it shall inform the latter without delay and at the latest within one month of receipt of the request of the reasons for its inaction and of the possibility of lodge a complaint with a supervisory authority and bring a judicial remedy". personal data concerning him are or are not processed and, when they are, access to personal data concerning him and in particular "when the personal data are not collected from the data subject, any e information available as to their source". According to paragraph 3 of the same article "the controller provides a copy of the personal data being processed".30. The rapporteur relies on three referrals received by the CNIL, from Messrs […] (complaint no. 19018344), […] (complaint no.

19008608) and […] (complaint no. 19016049), in the context of which the plaintiffs reported the difficulties encountered in the exercise of their rights, to propose to the Restricted Committee to consider that the company has breached its obligations resulting from Article 15 of the GDPR.31. In defence, the company argues that it cannot be accused of any breach under these three referrals. It indicates that these are isolated facts, on the basis of which the existence of a systemic problem cannot be inferred. It also points out the difference between the small number of complaints noted in the report concerning the exercise of rights (7) and the number of requests for the exercise of rights handled by the company per year (around 600). It thus considers that the alleged breaches are indicative of human error but in no way a "problem with the very operation of the procedure" of FREE MOBILE. Finally, the company indicates that the disputed referrals are contemporaneous with the date of entry into force of the GDPR and prior to the implementation of a new ticketing tool used by FREE MOBILE, since June 2019, which has made it possible to provide improvements to the procedure for processing requests to exercise FREE MOBILE's rights. It therefore considers that these specific shortcomings have now been resolved.32. Firstly, with regard to referral No. 19008608 of May 2019, Mr. […] referred the matter to the CNIL, explaining that he had asked FREE MOBILE, via the email address dedicated to "Informatique et Libertés" requests, to access to data concerning him which would be associated with his telephone number.33. The rapporteur observes that it emerges from the elements communicated by the company following the checks that, although the company clearly indicates that it has received the complainant's request, it has not, on the other hand, "found any trace of a response given to the complainant". The rapporteur therefore considers that the company failed in its obligation to deal with the complainant's request for access.34. In defence, the company first explains that it could not satisfy this request since it no longer had the requested data. It specifies in this sense that Mr […] having terminated his contract with the company FREE MOBILE four years before sending his request for access, he only had information relating to the existence of a contractual relationship. until March 4, 2015. Following the questioning of the rapporteur, who was surprised at the absence of personal data relating to the complainant which would be kept by the company as an intermediate archiving base under its legal or accounting obligations (billing data, management of any litigation, etc.), in its second statement of defence, the company indicates that it found thirteen invoices concerning the plaintiff following a search in its archiving database and sent, by email of 14 October 2021, an additional response to the complainant by providing him with these elements.35. The Restricted Committee first recalls that it follows from Article 12, paragraph 4, of the GDPR that when the data controller no longer holds data on the person who exercises his right of access (for example if the data has deleted), he

must nevertheless reply to the applicant within a maximum period of one month to inform him of this. Thus, the Restricted Committee considers that the company should at the very least have informed the complainant that, according to it, it no longer had any information concerning him, apart from that relating to the existence of a contractual relationship until March 4, 2015.36. The Restricted Committee then notes that the company had other data relating to the complainant, in this case the thirteen invoices kept by the company in its intermediate archiving database, which fall within the scope of the data to be communicated under the law of access. In this regard, the Restricted Committee recalls that data subjects must be able to be aware of the fact that data concerning them are stored and processed by the data controller, including several years after the termination of the contractual relationship, as is the case here. Indeed, it emphasizes that only the communication of this data allows the persons concerned to measure the nature and extent of the processing carried out by the company. In the present case, the Restricted Committee notes that it was only from the sending of the email of October 14, 2021 that the company provided an exhaustive response to the complainant's request for access, i.e. more than two years after Mr. […] had exercised his rights, following the initiation of the sanction procedure and receipt of the report in response to the company's observations dated October 4, 2021.37. Under these conditions, the Restricted Committee considers that by not responding to the request for access and by not responding to the applicant within the time limits provided, the company has failed to comply with its obligations arising from Articles 12 and 15 of the GDPR.38. It nevertheless notes that, in the context of the sanction procedure, the company justified having provided a response to the complainant and, therefore, having taken measures to comply with the obligations of the GDPR.39. Secondly, with regard to referral No. 19016049 of September 2019, Mr. […] seized the CNIL, explaining that he had asked the company FREE MOBILE to indicate to him whether it held personal data concerning him. If so, the complainant wanted to obtain a copy of his data and, more specifically, a copy of the recording of a call that would have been made by a person who usurped his identity as well as any document that would have been sent to this occasion.40. The rapporteur notes that it appears from the findings made during the inspection procedure that the company did not respond to the complainant, without being able to justify the reason. He also noted that this request was not qualified as a "Data Protection" request but as a "termination" request. The rapporteur therefore considers that the company has failed in its obligation to inform the complainant whether personal data concerning him figured in the processing it implements and, if necessary, in its obligation to send him a copy. .41. In defence, the company argues that this request was not addressed to the service dedicated to requests for the exercise of rights, so that a human error could have been made in its qualification as a

request for termination and not in as a right of access request. Next, the company explains that it could not provide a favorable response to the complainant insofar as his request for access related to the personal data of a third party. With regard to the other data held by the company, relating to the complainant, it indicates that it replied by email of August 26, 2021, attaching a copy of the personal data concerning him which is recorded in the database.42. On the first point relating to the address to which the complainant sent his request, the Restricted Committee considers that if it is not disputed that the complainant did not send his request to the e-mail or postal address which is identified by the company as being the dedicated channel for the transmission of requests to exercise rights, the fact remains that it belonged to the company, since this request has been received by the latter and that it was clear in its terms, to process it within the time limits provided for by the GDPR and to ensure that it is transmitted to the competent services. Indeed, if the implementation of organizational measures to facilitate the exercise of the rights of individuals complies with the requirements and the objective pursued by the GDPR, this cannot on the other hand exonerate the company from its obligation to respond to requests that are made to it when they are not sent to it through the channel which it will have dedicated for this purpose, a fortiori when, as is the case here, the content of the request is clear.43. On the second point in connection with the company's argument that the request for access concerned data from a third party, the Restricted Committee notes that the complainant's request is, primarily, a general request for the right to which aims, on a subsidiary basis, to communicate data relating to a telephone call. Therefore, if the Restricted Committee can hear the elements put forward by the company on the need to preserve the rights of third parties in connection with the part of the request relating to the telephone call, it considers, on the other hand, that the company would have in any case had to provide a response to the general request for the right of access made by the complainant, which was not the case before August 26, 2021, i.e. more than two years after his request and after the notification to the company on August 2, 2021 of the report proposing that the restricted committee impose a sanction.44. Under these conditions, the Restricted Committee considers that by not responding to the request for access and by not responding to the applicant within the time limits provided, the company has failed to comply with its obligations arising from Articles 12 and 15 of the GDPR.45. It nevertheless notes that, in the context of the sanction procedure, the company justified having provided a response to the complainant and therefore having taken measures to comply with the obligations of the GDPR.46. Thirdly, with regard to referral no. 19018344 dated October 2019, Mr. […] referred the matter to the CNIL, explaining that he had asked the company FREE MOBILE for access to the data concerning him.47. The rapporteur notes that the company did not respond to the complainant.48. In defence, the

company explained that it never received the plaintiff's request and therefore could not respond to it.49. Insofar as it has not been established that the plaintiff regularly exercised his rights, the Restricted Committee considers that there is no reason to find any breach of the obligation to respect the right of access s with regard to this complaint.50. Finally, with regard firstly to the argument that the facts alleged against the company are isolated in nature and therefore do not constitute a breach of the applicable provisions, the Restricted Committee considers that, if the complaints received by the CNIL does not reveal the existence of a structural breach in terms of the right of access, the fact remains that the company has disregarded its obligations in the processing of requests from Messrs […] and […]], although these were clearly formulated. These facts constitute a breach of the obligations arising from Articles 12 and 15 of the GDPR.51. Next, with regard to the argument that the breaches of which the company is accused are contemporaneous with the date of entry into force of the GDPR, the Restricted Committee recalls that most of the obligations in question, relating to access rights, rectification of opposition and security, existed before the entry into application of the GDPR and that the law "Informatique et Libertés" already made it possible to sanction them. The Restricted Committee therefore considers that the company cannot usefully plead a change in the legal framework to justify the lack of compliance on the day of the inspections.52. Finally, with regard to the improvements made by the company to its rights management procedure, while emphasizing the appropriateness of their adoption to improve the processing of requests, the Restricted Committee recalls that they have no impact on the existence of the breach on the day of the checks, which lasted many months and which was only ended after the initiation of the sanction procedure.53. In view of the foregoing, the Restricted Committee considers that a breach of the obligations of Articles 12 and 15 of the GDPR is constituted for the complaints filed by Messrs. […] and […], regardless that he did not wear a structural character.54. It nevertheless notes that, in the context of the sanction procedure, the company justified having taken measures to comply with the obligations of the GDPR by providing a response to the complainants.2. On the breach relating to the right of rectification pursuant to Article 16 of the GDPR55. Article 16 of the GDPR provides the right for a person to obtain from the controller "the rectification of personal data concerning him which are inaccurate".56. The rapporteur relies on a referral received by the CNIL, from Mrs […] (complaint no. 19017852 made in October 2019) and in the context of which the complainant reported difficulties encountered in exercising her right of rectification , to propose to the Restricted Committee to consider that the company has disregarded its obligations resulting from Article 16 of the GDPR. She indicated that she had asked the company to correct her postal address appearing on the telephone bills, which had become necessary following a renumbering of the

road network by the town hall.57. The rapporteur observes that it appears from the findings made during the inspection of 22 January 2020 that the complainant's request, made in September 2019, was not taken into account since the postal address subject of the request for rectification that appears on the complainant's invoice dated October 14, 2019 is the same as that appearing on the invoice dated January 14, 2020. The rapporteur therefore considered that between October 14, 2019 and January 14, 2020, the complainant's request for rectification was not taken into account by FREE MOBILE, i.e. several weeks after sending her request.58. In defence, the company argues that faster processing of Mrs. […]'s request was impossible in view of the imperatives of combating fraud. It specifies that when a person is both a customer of the companies FREE (because it has a fixed line) and FREE MOBILE (because it has a mobile line), as is the case of the complainant, it The postal address relating to the fixed line must first be changed with FREE. It specifies that this modification can only take place once the physical installation address of the telephone line has been modified within a tool called "SETIAR", which is administered by the company ORANGE S.A. The company specifies that this tool "makes it possible to ensure perfect correspondence between a telephone number and the physical installation address of the telephone line, in order to avoid any error when carrying out an operation on this line". The company indicates that these various steps cannot be carried out in a short time and that it has acted diligently to process this request. The company considers in any event to have responded to Mrs. […]'s request by sending her a letter, on September 17, 2019, i.e. four days after receiving her request, indicating that she could change her address online, directly from its subscriber space.59. The Restricted Committee notes that the need for Ms […] to change her address herself in her subscriber area should have been better explained to her. During the meeting, however, the company clearly explained the need, in the context of the fight against fraud, to use the "SETIAR" tool.60. Under these conditions, the Restricted Committee takes note of the elements provided by the defending company and considers that, with regard to this complaint, the elements of the debate do not allow it to conclude that the company has committed a breach. 3. On the breach relating to the obligation to respect the request for opposition of the persons concerned61. Article 12, paragraph 3, of the GDPR provides that "The data controller shall provide the data subject with information on the measures taken following a request made pursuant to Articles 15 to 22, as soon as possible and in any event within one month of receipt of the request. If necessary, this period may be extended by two months, taking into account the complexity and the number of requests. The controller informs the person concerned of this extension and the reasons for the postponement within one month of receipt of the request. unless the data subject requests otherwise". Finally, under the terms of paragraph 4 of this

article "if the data controller does not comply with the request made by the data subject, he shall inform the latter without delay and at the latest within a period of one month from the receipt of the request of the reasons for its inaction and the possibility of lodging a complaint with a supervisory authority and of lodging a judicial remedy".62. Article 21 of the GDPR provides that "when personal data is processed for marketing purposes, the data subject has the right to object at any time to the processing of personal data concerning him or her for such marketing purposes. canvassing, including profiling insofar as it is linked to such prospecting".63. The rapporteur relies on four referrals received by the CNIL, from Mrs. […] (complaint no. 19008223) as well as Mr. […] (complaint no. 19016318) and […] (complaints no. 17017795 and no. 19018125) and in the context of which the plaintiffs reported their difficulties in exercising their rights, to propose to the Restricted Committee to consider that the company has breached its obligations resulting from Article 21 of the GDPR.64. In defence, the company argues that it cannot be blamed for any breach of these four referrals, because it took the plaintiffs' requests into account in its databases. It then argues, in summary and as developed in point 31, that the alleged shortcomings, given the low number of complaints referred to in the report, are at best indicative of human errors and not of a problem with the functioning of the procedure for processing requests to exercise rights by the company, which would constitute a breach of the applicable provisions. It considers that the disputed referrals are contemporaneous with the date of entry into force of the GDPR and prior to the implementation of the new ticketing tool in June 2019 which has improved the processing of requests to exercise rights.65 . Firstly, with regard to referral No. 19008223 made in April 2019, Ms. […] seized the CNIL, explaining that during the years 2018 and 2019, she had been the subject of telephone canvassing by the company FREE MOBILE. During this period, the complainant expressed on two occasions, by letters dated September 27, 2018 and April 29, 2019, her opposition to the processing of her personal data for prospecting purposes.66. The rapporteur notes that it appears from the findings made by the supervisory delegation that the complainant was the subject of two prospecting campaigns on 28 August 2018 and 11 April 2019. The rapporteur therefore considers that the complainant was made him the recipient of commercial prospecting nearly eight months after he first expressed his opposition.67. In defence, the company admits that a "human error" was committed, so that the complainant was the subject of a prospecting campaign in April 2019 when she had previously exercised her right of opposition. However, the company considers that no breach can be held against it insofar as it "duly took into account" the complainant's opposition formulated by letter of April 29, 2019, i.e. before the on-site inspection operations which the CNIL carried out in January 2020.68. On this last point, the Restricted Committee considers that the existence of a breach cannot be limited to the

elements attesting to non-compliance on the day of the findings made within the framework of an inspection carried out pursuant to Article 19 of the "Informatique et Libertés" law, but may just as well be based on any element obtained by the CNIL services or the rapporteur, attesting to non-compliance for facts that gave rise to a complaint to the CNIL and to a referral to the restricted training, even if at the time of the control this non-compliance was put an end to. In the present case, the breach is based on evidence, and is therefore proven.69. Under these conditions, the Restricted Committee considers that by not taking into account the complainant's opposition to the processing of her personal data for prospecting purposes within the time limits provided for, the company has disregarded its obligations arising from Articles 12 and 21 of the GDPR.70. It nevertheless notes that, in the context of the sanction procedure, the company justified having taken into account the complainant's request for opposition and therefore having taken measures to comply with the obligations of the GDPR.71. Secondly, with regard to referral No. 19016318 made in September 2019, from Mr […], he explained that he had been the subject of commercial prospecting by SMS on offers marketed by the company FREE MOBILE until in July 2019, and provided screenshots of the corresponding text messages in its complaint. The complainant indicates that he has expressed his opposition to the processing of his personal data for commercial prospecting purposes on several occasions, in particular in June 2018 with the data protection officer (hereinafter "the DPO") of the ILIAD group. 72. The rapporteur observes that it appears from the additional information communicated by the company following the checks that the company had "on the day of this communication, not found any trace of a response to the complainant" without being able to justify the reason. He therefore considers that the company did not take into account the complainant's opposition to receiving commercial prospecting since the latter continued to receive solicitations until July 2019, i.e. almost a year after having expressed its opposition.73. In defence, the company indicates that it "promptly" took into account the complainant's request, as of July 25, 2018, after having received two emails from him on June 10 and July 8, 2018. The company attaches to this effect a screenshot of screen showing the date of the complainant's registration in an "anti-prospecting" database. With regard to the screenshots attached by the complainant, the company argues that they are "devoid of probative value since the recipient's number does not appear, so that it has not been established that the SMS captured by the plaintiff were actually received by him". On the other hand, it does not dispute the lack of response to the complainant's request for opposition. It indicates that the new ticketing tool put in place from June 2019 now makes it possible to ensure a systematic response to the persons concerned.74. The Restricted Committee considers that even if the company indicates that it took the complainant's request

into account "promptly", this does not mean that it provided him with an answer, since the latter did not receive any and did not therefore had no information as to whether his request had been taken into account, which is contrary to the provisions of Article 12 of the GDPR.75. Next, while it is true that the telephone number does not appear on the screenshots transmitted by the complainant, the Restricted Committee notes that it is frequent and understandable for people who file a complaint with the CNIL to transmit screenshots of messages received on their telephone, which logically does not allow the telephone number of the recipient of the message to appear. It also observes that the requests appearing on the screenshots communicated by the complainant do indeed refer to dates subsequent to the taking into account of the complainant's request for the right of opposition, confirmed by the DPO, since they mention offers valid between December 11, 2018 and July 11, 2019. Thus, the Restricted Committee notes that there is no reason to doubt the complainant's good faith. Finally, the Restricted Committee recalls that the right of opposition is attached to a person and not to a telephone number. The Restricted Committee therefore considers that these screenshots reveal that the complainant continued to receive solicitations almost a year after expressing his opposition to the DPO of the ILIAD group, in June 2018.76. Finally, the Restricted Committee recalls that the improvements made by the ticketing tool have no impact on the existence and materiality of the breach, both with regard to the provisions arising from Article 12 of the GDPR (lack of response from the company to the complainant) and its Article 21 (Mr. […] having continued to receive commercial prospecting almost a year after expressing his opposition to the use of his data for this purpose).77. Under these conditions, the Restricted Committee considers that by not taking into account the complainant's opposition to the processing of his personal data for prospecting purposes within the time limits provided, the company has disregarded its obligations arising from Articles 12 and 21 of GDPR.78. It nevertheless notes that, in the context of the sanction procedure, the company has justified having taken measures to comply with the obligations arising from Articles 12 and 21 of the GDPR.79. Finally, with regard to referrals No. 17017795, of September 2017 and No. 19018125, of October 2019, from Mr […], the latter explained that he was the subject of several canvassing by SMS and by mail from the company FREE MOBILE relating to the marketing of offers, in particular that relating to the "Free plan with unlimited calls […]". He indicates that he expressed by mail on several occasions, from March 2015, his opposition to the processing of his personal data for commercial prospecting purposes and that he nevertheless continued to receive commercial solicitations until October 2019.80. By email of 21 September 2018, the Commission services reminded the company of its obligations in terms of commercial prospecting and asked it to no longer process the complainant's data for this commercial purpose. By email of

October 3, 2018, the DPO of the ILIAD group replied that it had taken the request into account and "deleted the contact details of Mr […]".81. The rapporteur observes that it emerges from the elements noted during the inspection that, despite the requests made by the complainant since 2015 and the assertion of the DPO of the ILIAD group in 2018 by which he confirms "having deleted the contact details of Mr […]" , his opposition to the processing of his data for prospecting purposes was not taken into account until December 17, 2019, i.e. more than four years after the company was the recipient of his first request.82. In defence, the company indicates that it has never received a request for opposition from the plaintiff, unlike the company FREE. It considers that a request for opposition filed with the company FREE is not opposable to the company FREE MOBILE. However, it indicates that it took into account the complainant's wishes when he "activated the anti-soliciting option on his subscriber area". It specifies that this opposition has been effective since December 17, 2019. The company then specifies that the email produced by the rapporteur, indicating that the DPO of the ILIAD group confirms "having deleted the contact details of Mr […]", is a reconstruction of an e-mail and not the original, which does not constitute admissible proof, and it also notes that the e-mail was not sent to the right people and that it was not up to FREE MOBILE to take into account the complainant's request for opposition.83. Firstly, with regard to the company's failure to receive the complainant's opposition request, the Restricted Committee notes that the DPO of the ILIAD group - who, by email of October 3, 2018, indicated to the CNIL " having deleted the contact details of Mr […]" - is the DPO in charge of requests relating to FREE subscribers and FREE MOBILE subscribers. The Restricted Committee considers that it was therefore incumbent on it to deal with this request as a whole or to pass it on, where appropriate, to the competent services so that it is taken into account.84. Consequently, the company's argument that it was up to FREE alone to take the complainant's request into account cannot be accepted. Indeed, the complainant's request was a request for general opposition to receiving commercial prospecting by post and electronically (SMS and email) which concerned both FREE and FREE MOBILE. In his letter of March 5, 2015 addressed to FREE's "Informatique et Libertés" department, the complainant had taken care to specify his Free Mobile and Free box identifiers and to formulate his request as follows: "In accordance with the provisions of Article 38 paragraph 2 of the amended law of January 6, 1978, I ask you to delete my details from your advertising contact files, whether by post, telephone or computer. ".85. Finally, with regard to the inadmissibility of the email of October 3, 2018 confirming the receipt and consideration of the complainant's request by the DPO of the ILIAD group, the Restricted Committee observes that the latter does not appear in its original form in the CNIL's business tool (business tool in which the elements related to the processing of a complaint are

recorded). This email was recorded in the form of a "communication", which is a tab in the business tool allowing the agent in charge of the complaint not to record the email as such as an attachment to the file but to manually indicate that he has received an email from the company, by entering the date of receipt, selecting the sender of the message from a list of pre-defined choices and copying the content of the original message. The Restricted Committee therefore considers that the way in which this email was reproduced corresponds to a procedure provided for in the CNIL's business tool and that it can take it into account insofar as all the relevant elements appear there, that is to say the date, the content of the text and the identity of its author, and that they manifestly present a direct link with the subject of the complaint. Finally, the Restricted Committee notes that, although the company disputes the admissibility of this email, it does not state that it never sent this message.86. Therefore, the Restricted Committee considers that the company's arguments are not such as to call into question the fact that the complainant's opposition was only taken into account from December 17, 2019, which corresponds according to the company to the date on which the complainant activated "the anti-solicitation option on his subscriber space", which occurred more than a year after the indication by the DPO of the ILIAD group, on October 3, 2018, the effective consideration of this request, initially made on March 5, 2015.87. Under these conditions, the Restricted Committee considers that by not taking into account the complainant's opposition to the processing of his personal data for prospecting purposes within the time limits provided, the company has disregarded its obligations arising from Articles 12 and 21 of GDPR.88. It nevertheless notes that the company has justified having taken measures to comply with the obligations arising from Articles 12 and 21 of the GDPR.89. In view of the foregoing, the Restricted Committee considers that a breach of the obligations of Articles 12 and 21 of the GDPR is constituted for the complaints filed by Mrs. […], Messrs. […] and […].4. On the breach of the obligation to protect personal data by design90. According to Article 25 of the GDPR "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, including the degree of probability and seriousness varies, that the processing presents for the rights and freedoms of natural persons, the controller implements, both at the time of the determination of the means of the processing and at the time of the processing itself, appropriate technical and organizational measures, such as pseudonymisation, which are intended to implement the principles relating to data protection, for example data minimization, in an effective manner and to provide the processing with the necessary safeguards in order to meet the requirements of this Regulation and to protect the rights of the data subject […] ".91. The rapporteur relies on two referrals to the CNIL in November 2019, from Messrs […] (complaint no.

19019626) and […] (complaint no. 19020342) and in the context of which the complainants reported the fact that they failed to stop the sending, by FREE MOBILE, of invoices on which the mention of a terminated mobile line appeared, in order to propose to the Restricted Committee to consider that the company had disregarded its obligations resulting from Article 25 of GDPR.92. In defence, the company explains first of all that it sends zero euro invoices to customers after the termination of their subscription because the latter benefit from a so-called "multiline" subscription. The company specifies that this service allows a subscriber to attach to a main mobile line, one or more secondary lines, which has the effect of grouping the invoices of the different lines on the main account associated with the main line, and to carry out a single direct debit corresponding to the sum of the associated packages. The company thus argues that "the processing of the telephone number corresponding to the terminated main [mobile] line is necessary, since it pursues purposes aimed at enabling FREE MOBILE to continue the proper performance of their contract by identifying the debtor of the multiple lines taken out by its subscribers and to improve for subscribers the legibility of the invoicing of their subscriptions and the debits made on their account". Next, the company nevertheless specifies that it has initiated an overhaul of its invoicing procedure so that the invoices for multi-line accounts associated with a terminated main mobile line now include the mention of an identifier enabling the subscriber and the FREE MOBILE company to know, for billing purposes, who is the sole debtor of the lines, without continuing to mention the terminated main line on the bill.93. The Restricted Committee notes that it follows from Article 25 of the aforementioned GDPR that data controllers must implement appropriate technical and organizational measures in order to effectively comply with the principles relating to data protection.94. The Restricted Committee considers that if the information that a person has been the holder of a terminated mobile line can actually be kept for the purposes of performance of the contract and for accounting purposes, or even for the management of litigation, it does not On the other hand, it is not necessary to continue to process this information within the framework of the issuance of invoicing in progress, and to make it appear on the latter, while the use of an identifier allowing the identification of the debtor of the various mobile lines (main and secondary) can be used instead. The company should have provided, from the design stage, organizational and technical measures to no longer process this data in this context following a request for termination of a main line by the data subject.95. Under these conditions, the Restricted Committee considers that the aforementioned facts constitute a breach of Article 25 of the GDPR since the company has not implemented the organizational and technical measures allowing the erasure of personal data. personnel who were no longer needed for billing purposes.96. It nevertheless notes that, within the framework of the sanction procedure,

the company justified having carried out an overhaul of its invoicing procedure, so that the invoices now include only the mention of the active lines, without mentioning the terminated lines. The Restricted Committee therefore considers that the company has complied with the obligations arising from Article 25 of the GDPR.5. On the breach of the obligation to ensure the security of personal data97. Article 32 of the GDPR provides that: "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, including the degree of likelihood 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 (…)" and, in particular , "means to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services" and a "procedure to test, analyze and regularly assess the effectiveness of technical measures and organizational to ensure the security of the processing ".98. Firstly, the rapporteur relies on two referrals from Ms […] (complaint no. 19012802 of July 2019) and […] (complaint no. 19019490 of October 2019) and in the context of which the complainants reported the absence of systematic authentication of the user to access a FREE MOBILE user account (for the user having a telephone equipped with a FREE MOBILE SIM card or for a person benefiting from the connection sharing of a user equipped with a telephone equipped with a FREE MOBILE SIM card), to propose to the restricted committee to consider that the company has disregarded its obligations resulting from article 32 of the GDPR.99. In defence, the company argues that the CNIL checks did not cover these complaints and that access to a subscriber's mobile space from another device via connection sharing is not possible. 100. In view of the elements provided by the company, the Restricted Committee considers that there is no reason to find a breach of Article 32 of the GDPR in respect of these facts.101. Secondly, the rapporteur observes that it emerges from the observations made within the framework of the control procedure that the company sends by e-mail, in clear text, the passwords of users when they subscribe to an offer with the company FREE MOBILE.102. In defence, the company first argues that as data controller, it is free to choose the security measures to be put in place and that the guides and recommendations issued by the CNIL or the National Agency for information systems security (ANSSI) are not mandatory and do not have the force of law. Therefore, the company considers that no breach can be accepted in the absence of a "characterised breach of the security obligation, materialized by the occurrence of a breach of personal data", which does not is not the case here according to it.103. The company then argues that at the time of the control operations, subscribers were encouraged to change their password on their subscriber area and made aware of the importance of keeping these passwords

confidential. It also indicates that the initial password assigned by the company FREE MOBILE has a high level of robustness. Finally, it specifies that the subscriber area only allows access to "basic" information and not to sensitive information.104. First of all, the Restricted Committee recalls that, pursuant to Article 32 of the GDPR, to ensure the protection of personal data, it is the responsibility of the data controller to take "appropriate technical and organizational measures in order to guarantee a level of security appropriate to the risk". The Restricted Committee considers that in this case, the methods of transmission of passwords implemented by the company are not appropriate with regard to the risk that the capture of their identifier and their password would pose to the person concerned. goes through a third party. Indeed, the transmission, in plain text, of a password which is neither temporary nor for single use and whose renewal is not imposed, makes it easily and immediately usable by a third party who would have improper access. to the message that contains it. This third party could thus access all the personal data present in the FREE MOBILE user account of the person concerned (in particular the surname, first name, mobile line number, postal address, e-mail address, bank account statement, line number mobile). He could also access his voicemail, download his bills and the statement of his consumption, modify the password, the e-mail address or the options of the account. The fact that the password itself is strong and that people are encouraged to change their password is not enough to compensate for these risks, which can lead to identity theft and phishing attempts, among other things. Therefore, taking into account these risks for the protection of personal data and the privacy of individuals leads the Restricted Committee to consider that the measures deployed to guarantee data security in this case are insufficient.105. Next, the Restricted Committee specifies that if deliberation no. 2017-012 of January 19, 2017, the purpose of which is to provide recommendations relating to passwords, the CNIL guide relating to the security of personal data and the note ANSSI's technique relating to the passwords cited in the rapporteur's writings are certainly not mandatory, they do however set out the basic security precautions corresponding to the state of the art. Therefore, the Restricted Committee recalls that it retains a breach of the obligations arising from Article 32 of the GDPR and not the non-compliance with the recommendations, which moreover constitute relevant insight for assessing the risks and the state of the art in personal data security.106. In addition to these recommendations, the Restricted Committee points out that it has, on several occasions, adopted pecuniary sanctions where the characterization of a breach of Article 32 of the GDPR is the result of insufficient measures to guarantee the security of the data processed, and not just the result of the existence of a personal data breach. Deliberations No. SAN-2019-006 of June 13, 2019 and No. SAN-2019-007 of July 18, 2019 relate in particular to the insufficient robustness of passwords as well

as their transmission to the company's customers by email, in clear (readable in the body of the message), after the creation of the account.107. Under these conditions, in view of the risks incurred by the persons mentioned above, the Restricted Committee considers that the aforementioned facts constitute a breach of Article 32 of the GDPR since the company sends by e-mail, in clear text, the words of password of users when they subscribe to an offer with the company FREE MOBILE.108. It nevertheless notes that, as part of the sanction procedure, the company certifies the mandatory implementation of the renewal of users' passwords when they first connect. The password requested by the company complies with the recommendations of the CNIL contained in its 2017 recommendation relating to passwords. In addition, the Restricted Committee notes that the company undertakes to no longer transmit the passwords of new subscribers in plain text by email but, from the end of March 2022, that the latter create their own password. pass, which must comply with the recommendations of the CNIL in this area.III. On corrective measures and their publicity109. 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: […] 2° An injunction to bring the processing into conformity with the obligations resulting from the regulation (EU) 2016/679 of April 27, 2016 or of this law or to satisfy the requests presented by the data subject with a view to exercising their rights, which may be accompanied, except in cases in which the treatment is implemented by the State, of a penalty whose m the amount cannot 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. "110. 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.111 Firstly, on the principle of imposing a fine, the company maintains that such a measure is not justified. shortcomings relating to the exercise of the rights of access and opposition, the company considers that the complaints underlying these shortcomings are of an isolated nature and that, in any event, it has responded to requests for access and taken into account the requests plaintiffs' objections. Regarding the breach of the obligation to protect data by design, the company considers that the processing of the telephone number corresponding to the main mobile line terminated is necessary for the purposes of the proper performance of the mobile telephone service. With respect to the breach relating to data security, the company considers that in the absence of a personal data breach, the transmission in clear text of user passwords is not a "characteristic breach of the security obligation ".112. The Restricted Committee recalls that it must take into account, for the pronouncement of an administrative fine, the criteria specified in Article 83 of the GDPR, such as the nature, gravity and duration of the violation, the measures taken by the controller to mitigate the damage suffered by data subjects, the degree of cooperation with the supervisory authority and the categories of personal data affected by the breach.113. The Restricted Committee firstly considers that the company has shown certain negligence with regard to the fundamental principles of the GDPR since four breaches have been established, relating in particular to the rights of persons and to basic measures related to the security of personal data. The Restricted Committee adds that several shortcomings have given rise to complaints. It also underlines, with regard to the breach relating to data security, that the transmission by e-mail, in plain text, of the passwords of users when they subscribe to an offer with the company FREE MOBILE, can present a risk for the privacy of data subjects.114. The Restricted Committee then notes that the company FREE MOBILE is a particularly important player in the telecommunications sector since it counted, in December 2020, approximately […] subscribers to mobile telephony offers, […]. The Restricted Committee also observes that the company, in its capacity as a mobile telephone operator, is at the heart of the routing of the daily flows of personal data of many people and must therefore show particular rigor in the management of the security of the personal data concerned.115. Finally, the Restricted Committee notes that the compliance measures put in place following the notification of the sanction report do not exonerate the company from its liability for the breaches noted.116. Consequently, the Restricted Committee considers that an administrative fine should be imposed with regard to the breaches constituted in Articles 12, 15, 21, 25 and 32 of the GDPR.117. Secondly, with regard to the amount of the fine, the Restricted Committee recalls that administrative fines must be both dissuasive and proportionate. In the present case, the Restricted Committee finds that the complaints giving rise to breaches appear to be extremely isolated

and few in number - their number, of seven, must be related to the number of subscribers, […] -, so that these breaches can in no way be regarded as having a systemic character. The restricted formation also takes into account the activity of the company and its financial situation.118. Therefore, in the light of these elements, the Restricted Committee considers that the imposition of a fine of 300,000 euros appears justified.119. Thirdly, an injunction to bring the processing into compliance with the provisions of Articles 12, 15, 21, 25 and 32 of the GDPR was proposed by the rapporteur when notifying the report.120. The company maintains that the actions it has taken with regard to all of the breaches noted should lead to the non-compliance with the rapporteur's proposal for an injunction.121. As indicated above, the Restricted Committee notes that the company has taken measures to bring its processing into compliance with the provisions of Articles 12, 15, 21, 25 and 32 of the GDPR. It therefore considers that there is no longer any need to issue an injunction.122. Finally, with regard to the publicity of the sanction, the company maintains that such a measure would be disproportionate in view of the shortcomings identified and the low number of complaints concerned. She also considers that this additional publicity penalty would cause irreversible damage to her reputation.123. The Restricted Committee considers that the publicity of the sanction is justified in view of the plurality of breaches noted, their persistence, and the number of people concerned. FOR THESE REASONS The Restricted Committee of the CNIL, after deliberation, decides to: pronounce against FREE MOBILE an administrative fine in the amount of 300,000 (three hundred thousand) euros for breaches of Articles 12, 15, 21, 25 and 32 of the GDPR; make public, on the website of the CNIL 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. The chairman Alexandre LINDEN This decision is likely to be the subject of a appeal to the Council of State within two months of its notification.