Deliberation SAN-2019-010 of November 21, 2019 National Commission for Computing and Liberties Nature of the deliberation: Sanction Legal status: In force Date of publication on Légifrance: Tuesday November 26, 2019 Deliberation of the restricted committee n°SAN-2019-010 of 21 November 2019 concerning company X The National Commission for Computing and Liberties, meeting in its restricted formation composed of Messrs Alexandre LINDEN, president, Philippe-Pierre CABOURDIN, vice-president, and Mesdames Anne DEBET, Sylvie LEMMET and Christine MAUGÜE , members; Having regard to Convention No. 108 of the Council of Europe of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data; Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 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 January 6, 1978 relating to data processing, fi files and freedoms as amended, 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. 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 referral PL18002670 received by the National Commission for Computing and Liberties on February 6, 2018 Having regard to decision no. 2018-060C of March 16, 2018 of the President of the National Commission for Computing and Liberties to instruct the Secretary General to carry out or to have carried out a mission to verify all the prospecting processing carried out implemented by or on behalf of company X; Having regard to the decision of the President of the National Commission for Computing and Freedoms appointing a rapporteur before the restricted committee, dated April 29, 2019; Having regard to the report rt of Mrs. Sophie LAMBREMON, commissioner rapporteur, notified to company X on June 11, 2019; Having regard to the written observations of Mr. […], lawyer for company X, received on July 10, 2019; Having regard to the response of the rapporteur to these observations notified on July 25, 2019 to the board of the company; Having regard to the new written observations of the board of company X received on July 31, 2019 as well as the oral observations made during the session of the restricted committee, on September 19, 2019; Having regard to the documents communicated by email on October 7, 2019, after the closing of the investigation; Having regard to the other documents in the file; Were present, during the restricted training session of September 19, 2019: - Mrs. Sophie LAMBREMON, commissioner, in her report; As representative of company X:- […], lawyer for the company;The counsel for company X having spoken last;The Restricted Committee adopted the following decision:I. Facts and procedure1. Company X (hereinafter "the company") is a simplified joint-stock company with a single shareholder, whose registered office is located […]. Its activity is the installation of

insulation equipment, heat pumps and openings.2. In 2017, the company achieved a turnover of 27,647,300 euros for a net profit of more than 500,000 euros. This turnover was EUR […] for a net result of approximately EUR […] for the year 2018. In March 2018, it employed approximately 75 employees.3. On February 6, 2018, Ms […] lodged a complaint with the National Commission for Computing and Liberties (hereinafter "the CNIL" or "the Commission") alleging telephone canvassing by the company X. The complainant also indicated that, despite opposition to canvassing expressed orally to the telephone operators and by letter addressed to the company's headquarters, the calls had not ceased several months after these steps.4. On March 20, 2018, in application of the President's decision no. the processing in connection with commercial prospecting implemented by or on behalf of the company in accordance with the provisions of the law of January 6, 1978 as amended and, more particularly, to investigate Mrs. […].5's complaint. On the occasion of this check, the delegation was informed that the company processed, within the framework of its activity, the data of customers and prospects obtained either directly from the persons concerned (taking initiative to contact the company or contacted in as part of telephone prospecting operations by service providers using their own directories) or collected from third parties as part of a sponsorship program.6. The delegation was informed that the company's telephone sales prospecting was carried out by several call centers acting as subcontractors and being located, for the most part, in North Africa. The company indicated to these subcontractors the department that it wished to see targeted, and the teleoperators of the call centers called the persons concerned in order to offer them the services of the company. If people declared themselves interested, they were either put directly in contact with an employee of company X, or called back later, so that the eligibility criteria for "energy saving certificates", a device better known as the term "one-euro insulation". People could also be contacted this way when they had been referred by customers of the company who had provided their contact details. The delegation was informed that the company had not put in place a centralized mechanism for taking into account the requests for opposition expressed by the people canvassed. She took copies of nineteen e-mails sent to the company by private individuals expressing their refusal to carry out future prospecting operations.7. The delegation was informed that customer data was processed in the "Progibos" customer management software, in which the teleoperators could record customer comments intended for the employees of company X. The delegation noted, among these comments, remarks relating to the state of health of the persons canvassed as well as abusive remarks against them.8. Having obtained copies of recordings of conversations between telephone operators and prospects, the delegation noted that, in a significant number of conversations, people were not informed of the recording of the call. When

people were notified of the registration, no other information relating to the protection of personal data was communicated.9. In addition, following the inspection, the Commission services asked the company to provide several documents necessary for the performance of their mission, in order to assess the company's liability. These included contracts with call centers. A period of eight days was granted to the company to communicate these documents. At the company's request, two time extensions were granted, until April 11 and then until April 20, 2018. The company sent certain documents on April 11, 17, 19 and 20, without all of the requested documents are not communicated, despite two reminders from the Commission services on 23 April and 4 June 2018, including one by registered letter with acknowledgment of receipt.10. In view of these facts, the chairperson notified the company of decision no. MED-2018-039 of September 27, 2018 giving it formal notice, within two months, to take the following measures: ensure the relevance and non-excessive nature of the data collected, in accordance with article 5-1-c) of the general data protection regulation n° 2016/679 of April 27, 2016, in particular

by:

~ deleting inappropriate and excessive comments with regard to the purpose of the processing;

~ taking the necessary measures to prevent excessive comments from being recorded in the PROGIBOS software, for example, by setting up an automatic detection system for inappropriate, irrelevant and excessive words with regard to the purpose of the processing, in order to exclude them from the comment areas and by raising awareness among staff of the need to record only adequate, relevant and non-excessive data; justify the reasons for which partial responses were sent to the email of April 23, 2018 and the letter of June 4, 2018 from the Commission and communicate to the latter:

~ the exhaustive list of call centers working on behalf of the company;

~ for each of the call centers, the fifty most recent recordings relating to prospecting telephone calls made on behalf of the company;

the one hundred most recent recordings available to the company relating to telephone conversations between prospects and employees of the society ; inform the persons from whom personal data is collected directly, under the conditions now provided for in Articles 12 and 13 of the General Data Protection Regulation No. 2016/679 of April 27, 2016, in particular by providing, at the time the personal data are collected, information relating to the identity of the controller, the purpose pursued by the processing, the rights of individuals and the transfer of data to a non-EU Member State European Union, and by providing, on the "www.[...].fr" site, information relating to the transfer of data to a non-Member State of the European Union as well as the retention periods of the categories of data processed or the criteria used to determine these durations; inform the persons from whom personal data is collected indirectly, under the conditions now provided for in Article 14 of the General Data Protection Regulation No. 2016/679 of April 27, 2016, in particular by providing godchildren, at the latest at the time of the first communication with them, information relating to the identity of the controller, the purpose pursued by the processing, the rights of individuals and the transfer of data to a non-Member State of the European Union, and by providing a comprehensive information notice on the "www.[...].fr" site; define and implement an effective opposition right procedure aimed at complying with the provisions of Article 21-2 of the General Data Protection Regulation No. 2016/679 of April 27, 2016 and in particular, granting the request made by Mrs […]; no longer transfer personal data to a State that does not ensure an adequate level of protection of privacy and fundamental rights and freedoms, unless one of the conditions provided for in Articles 46 to 49 of the Regulation is met general on data protection no. 2016/679 of 27 April 2016; justify to the CNIL that all of the aforementioned requests have been complied with, within the time limit.11. The formal notice was received by the company on October 2, 2018.12. On November 29, 2018, the President of the CNIL received a request to extend the deadline set by the formal notice. In this letter, a lawyer representing the company explained that she had been appointed as a data protection officer with the CNIL, without having been informed, and that the company had received this formal notice late. Consequently, the company's board requested that the two-month period initially granted be doubled, a request which was granted on December 13, 2018.13. On February 15, 2019, the company's board sent a letter to the president of the CNIL, informing her of the fact that, despite several reminders from her, he had been unable to obtain communication of the supporting documents requested from the society. He could not, therefore, prove that company X had been brought into compliance, but nevertheless provided some documents provided by the company.14. For the purpose of examining these elements, the President of the Commission

appointed Mrs. Sophie LAMBREMON as rapporteur, on April 29, 2019, on the basis of Article 47 of the law of January 6, 1978 amended in the version applicable to the day of designation.15. At the end of his investigation, the rapporteur had company X notified by hand, on June 11, 2019, of a report detailing the breaches of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 relating to the protection of data (hereinafter "the Regulation" or "the GDPR") which he considered constituted in this case.16. This report proposed that the restricted committee of the Commission issue an injunction to bring the processing into compliance with the provisions of Articles 5-1.-c), 12, 13, 14, 21 and 44 of the Regulations, accompanied by a penalty payment five hundred euros per day of delay at the end of a period of fifteen days following the notification of the deliberation of the restricted formation, as well as an administrative fine of an amount of five hundred thousand euros. He also proposed that this decision be made public but that it no longer allow the company to be identified by name after the expiry of a period of two years from its publication.17. Also attached to the report was a summons to the restricted committee meeting of September 19, 2019, indicating to the company that it had one month to submit its written observations.18. On July 10, 2019, through its new board, the company filed submissions. The rapporteur replied on 25 July.19. On 31 July, the company submitted new observations in response to those of the rapporteur.20. During the session of the restricted committee on September 19, 2019, the rapporteur maintained the proposals made in his sanction report with the exception of the injunction relating to the adequacy of the free comments, the company having brought itself into compliance on this point.II. Reasons for decision1. On the applicable law21. The Restricted Committee notes that the check carried out by the Commission services took place on 20 March 2018. This date predates the entry into application of the GDPR. For this reason, the formal notice of September 27, 2018, although notified after the entry into force of the text, falls within breaches of Law No. 78-17 of January 6, 1978 as amended, while enjoining compliance to the Regulations, now applicable.22. The Restricted Committee considers that the principle of non-retroactivity of the criminal sanction prohibits in principle the application of the Regulation to sanction instantaneous breaches occurring before its entry into force.23. It nevertheless notes that the shortcomings noted in the formal notice are continuous shortcomings, which are defined by an action (or an omission) extending over a certain period of time, within the meaning of the case law of the European Court of Human Rights. man (European Court of Human Rights, main ch., case Rohlena v. Czech Rep., application 59552/08, paragraph 28).24. The Restricted Committee considers that these breaches continued at least until the notification of the sanction report, i.e. after the entry into application of the GDPR, for lack of the company having demonstrated compliance.25. The Restricted Committee

recalls that in the event of continuous breaches, account should be taken of the law applicable at the last state of the breach (CE 9/10, 5 Nov. 2014, Sté UBS France SA, no 371585, point 24) .26. Consequently, the Restricted Committee considers that the GDPR is applicable to the facts of the case and that the breaches will therefore have to be assessed in the light of this text.2. On the breach of the obligation to process data that are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed27. Article 5-1-c) of the GDPR provides that "personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed".28. The Restricted Committee observes that offensive terms relating to the state of health of people have been noted in the "Progibos" software used to manage the company's customers. It considers that, by their very nature, abusive comments are inadequate with regard to the purpose for which the data are processed and that nothing justifies, in this case, the presence of data relating to the health of individuals in the customer and prospect management. It notes in this regard that the excessive nature of this data is not called into question by the company.29. The Restricted Committee also notes that the company has not demonstrated that it had deleted the excessive or inadequate comments at the end of the period granted in the formal notice and that, consequently, the breach of the obligation not to deal that adequate, relevant and limited data to what is necessary in relation to the purposes for which they are processed was constituted on that date.30. The Restricted Committee therefore considers, in view of these elements, that a breach of Article 5-1-c) of the GDPR was established at the expiry of the time limit set by the formal notice.31. The Restricted Committee notes that the company has produced evidence justifying that it purged excessive comments during the sanction procedure.32. The Restricted Committee also takes note of the observations made by the rapporteur during the meeting of September 19, 2019. The rapporteur considers that the company has demonstrated its compliance and that, therefore, there is no longer any need to issue an injunction. on this point.33. The Restricted Committee nevertheless notes that, if information is actually delivered using a contextual banner to users of the "Progibos" software, it does not appear from the bailiff's report drawn up on July 30, 2019 that the company would have put in place a computerized mechanism preventing the recording in the software of offensive terms or terms relating to the state of health of individuals. This does not appear either from the documents provided by the company during the sanction procedure, or from the statements of its counsel during the meeting of September 19, 2019.34. However, given the findings made by the delegation of control on March 20, 2018 as to the nature of the comments entered by users of the "Progibos" software, the Restricted Committee considers that a simple information notice intended for users cannot sufficient, in this case, to ensure compliance

with the provisions of Article 5-1-c) of the GDPR. On the contrary, it considers that the data controller must put in place a binding system allowing him to ensure that the behavior observed is not repeated, either by automatically preventing the recording of certain terms as soon as they are entered, or by carrying out a review daily automated recorded comments.35. These elements are therefore not such as to call into question the characterization of the breach mentioned at the close of the investigation.3. On the breach of the obligation to inform people36. The first paragraph of Article 12 of the GDPR provides that "the controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 […] with regard to the processing to the data subject in a concise manner, transparent, comprehensible and easily accessible, in clear and simple terms, in particular for any information intended specifically for a child.Information is provided in writing or by other means including, where appropriate, by electronic means. When the data subject so requests, the information may be provided orally, provided that the identity of the data subject is demonstrated by other means".37. Regarding the information of persons whose personal data is collected directly from them by the company, Article 13 of the GDPR provides: "1. When personal data relating to a data subject is collected from this person, the controller shall provide it, at the time the data in question is obtained, with all of the following information: a) the identity and contact details of the controller and, where applicable, of the controller's representative; b) the where applicable, the contact details of the data protection officer; c) the purposes of the processing for which the personal data are intended as well as the legal basis of the processing; d) where the processing is based on Article 6, paragraph 1 , point f), the legitimate interests pursued by the controller or by a third party; e) the recipients or categories of recipients of the personal data, if s exist; andf) where applicable, the fact that the controller intends to transfer personal data to a third country or to an international organisation, and the existence or absence of a decision to adequacy rendered by the Commission or, in the case of transfers referred to in Article 46 or 47, or in the second subparagraph of Article 49(1), the reference to the appropriate or suitable guarantees and the means of obtaining one copy or the place where they were made available;2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject, at the time the personal data is obtained, with the following additional information which is necessary to ensure fair and transparent processing: a) the duration of retention of personal data or, where this is not possible, the criteria used to determine this duration; b) the existence of the right to request from the controller access to personal data, rectification or erasure thereof, or restriction of processing relating to the data subject, or the right to object to processing and the right to data portability; c) where the processing is based on Article 6, paragraph 1, point a), or on Article 9, paragraph 2, point a), the existence of the

right to withdraw consent at any time, without prejudice to the lawfulness of the processing based on the consent and made before its withdrawal; d) the right to lodge a complaint with a supervisory authority; e) information on whether the requirement to provide personal data is of a regulatory nature or contractual or if it conditions the conclusion of a contract and if the person concerned is obliged to provide the personal data, as well as on the possible consequences of the non-provision of these data; f) the existence of a automated decision-making, including profiling, referred to in Article 22(1) and (4), and, at least in such cases, meaningful information about the underlying logic, as well as the significance and intended consequences of this processing for the data subject. "38. Regarding the information to be provided where the personal data has not been collected from the data subject, Article 14 provides: "1. Where the personal data has not been collected from the data subject, the controller shall provide the latter with all of the following information: a) the identity and contact details of the controller and, where applicable, of the controller's representative; b) where applicable, the contact details of the delegate to data protection;c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;d) the categories of personal data concerned;e) where applicable, the recipients or the categories of recipients of the personal data; f) where applicable, the fact that the controller intends to transfer the personal data to a recipient in s a third country or an international organisation, and the existence or absence of an adequacy decision issued by the Commission or, in the case of transfers referred to in Article 46 or 47, or Article 49 , paragraph 1, second subparagraph, the reference to the appropriate or suitable safeguards and the means of obtaining a copy thereof or the place where they have been made available;2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing vis-à-vis the data subject: a) the duration for which the personal data will be stored or, where this is not possible, the criteria used to determine this period; b) where the processing is based on Article 6(1)(f), the legitimate interests pursued by the controller or by a third party; c) the existence of the right to request from the controller access to personal data, rectification or erasure thereof, or restriction of processing relating to the data subject, as well as the right to object to processing and the right to data portability; d) where the processing is based on Article 6(1)(a) or Article 9(2)(a), exists ence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent given before its withdrawal; e) the right to lodge a complaint with a supervisory authority; ) the source from which the personal data originated and, where applicable, a statement indicating whether or not they originated from publicly available sources; g) the existence of automated decision-making, including a profiling, referred to in Article 22(1) and (4), and, at least

in such cases, meaningful information about the underlying logic, as well as the significance and the intended consequences of such processing for the data subject.3 . The controller shall provide the information referred to in paragraphs 1 and 2: a) within a reasonable period of time after obtaining the personal data, but not exceeding one month, having regard to the particular circumstances in which the personal data is processed b) if the personal data is to be used for the purpose of communication with the data subject, at the latest at the time of the first communication to said person; orc) if it is intended to communicate the information to another recipient, at the latest when the personal data is communicated for the first time. "39. Guidelines on transparency within the meaning of Regulation (EU) 2016/679 were adopted by the "Article 29" working party on 29 November 2017 (version revised and adopted on 11 April 2018, WP260 rev.01) They specify, page 22, that while information at several levels is possible for greater clarity, "the G29 recommends that the first level […] include details of the purpose of the processing, the identity of the controller and a description of the rights of data subjects", before recommending that "this information should be brought directly to the attention of the data subject at the time of collection of personal data".40 The Restricted Committee observes that it is clear from the telephone recordings communicated by the company that the persons who are the subject of telephone prospecting are either not recipients of any information relating to the recording of the call or are simply informed of the recording of the conversation without any other information being communicated to them as to the processing of their personal data, such as the purpose of the processing, the identity of the data controller or the rights available to them.41. The Restricted Committee notes that the company neither affirms nor demonstrates having set up, during the period granted by the formal notice, an information mechanism in accordance with the aforementioned provisions, no details appearing on this point in the summary response provided to the formal notice on February 15, 2019. The same applies to the information provided to sponsored persons whose personal data is indirectly collected.42. The Restricted Committee therefore considers, in the light of these elements, that a breach of Articles 12, 13 and 14 of the GDPR was established at the expiry of the time limit set by the formal notice.43. The Restricted Committee notes that the company indicates that it will henceforth communicate complete information in the form of an email to any person subject to telephone prospecting, as well as to persons whose data is not collected directly.44. The Restricted Committee nevertheless notes that, although the company claims to make complete information notices available to persons subject to telephone prospecting and those whose data is collected indirectly, it has not justified the information that it delivers, for example by producing a model of the email sent. In addition, with regard to people whose data is collected directly, the Restricted Committee notes that the company

indicates that it offers information in the form of an email sent after the telephone conversation. The Restricted Committee recalls that Article 13 of the GDPR requires information to be provided at the time of collection of personal data. Indeed, with regard to this text, it is necessary for the person to be able to read the information relating to the processing of their personal data at the time their data is collected, and not only subsequently. Thus, information, even summary, must be communicated to him via the voice service or the teleoperator, by offering him the possibility of obtaining communication of complete information either by activating a key on his keyboard telephone, or by sending an e-mail, for example.45. These elements are therefore not such as to call into question the characterization of the breach mentioned at the close of the investigation.4. On the breach of the obligation to respect the right of opposition46. Article 21 of the GDPR provides, in its second paragraph, that "when personal data are processed for marketing purposes, the data subject has the right to object at any time to the processing of personal data. regarding for such prospecting purposes, including profiling insofar as it relates to such prospecting".47. In addition, Article 12 of the aforementioned GDPR provides, in its second paragraph, that "the controller shall facilitate the exercise of the rights conferred on the data subject under Articles 15 to 22".48. The Restricted Committee therefore considers, under the terms of these two articles combined, that it was up to the company to put in place a mechanism allowing effective consideration of the right to object expressed by the persons subject to telephone prospecting. As such, it had to be able to ensure that the opposition expressed by the interested parties was respected and that the people who expressed their opposition no longer received prospecting calls from its subcontractors. .49. The Restricted Committee notes that it appears from the statements of the employees of the company, collected during the inspection carried out on March 20, 2018, that no procedure had been put in place allowing the opposition expressed to the company to be communicated to its subcontractors or that the opposition expressed directly to the teleoperators of the call centers is centralized at the level of the company's head office and passed on to the company and all of the subcontractors.50. Therefore, it appears that the opposition expressed by the people canvassed was futile: when it was expressed at the company's headquarters, the subcontractors were not informed and continued prospecting operations; when it was expressed directly to a subcontractor, neither the head office nor the thirty-five other call centers then working for the company were informed, and prospecting continued despite the refusal expressed by the people. It is apparent from the foregoing that, however the opposition was expressed, it remained ineffective.51. The Restricted Committee also considers that the failure to take into account the opposition expressed emerges from the complaint of Mrs. […] who reports a large number of calls

received after expressing her opposition. This fact is also apparent from the emails received by the partnership from persons no longer wishing to be the target of telephone prospecting, the majority of these emails reporting several calls received despite the refusal expressed.52. The Restricted Committee notes that the company sent to the Commission services, after the inspection carried out on 20 March 2018, three call center certificates stating that they had received from the company a list of people no longer wishing to be canvassed.53. The Restricted Committee notes that only three certificates were provided, while the company indicated that it was working at the time with thirty-six call centers. It therefore considers, considering the company's obligation fulfilled vis-à-vis these three call centres, that no measure has been taken to ensure that the opposition is effectively respected by all of its subcontractors. -contractors.54. In addition, the Restricted Committee notes that the information appearing on the certificates and which the company claims to have communicated to the call centers does not allow sufficient identification of the persons who have expressed their refusal to be canvassed by telephone. On the one hand, the absence of any mention of the telephone number prevents the registration of the person on a list of opposition to telephone prospecting. On the other hand, the mere mention of the person's e-mail address and surname (a fortiori when the latter is particularly widespread) leads to a risk of confusion in the event of homonymy. Thus, the subcontractors were unable to ensure that the persons concerned would no longer be contacted by them.55. Finally, the Restricted Committee considers that the supporting documents produced by the company do not make it possible to demonstrate that, at the end of the time limit set in the formal notice, the company ensured that the opposition expressed by a person solicited from the teleoperator of a subcontractor call center was communicated for the purpose of being centralized and then retransmitted to all the subcontractors. The Restricted Committee considers that in the absence of such a mechanism, any opposition expressed during a telephone prospecting call will not lead to the cessation of any prospecting operation on behalf of the company, in particular by another call centre.56. The Restricted Committee therefore considers, in the light of these elements, that a breach of Article 21 of the GDPR was established at the expiry of the time limit set by the formal notice.57. The Restricted Committee takes note of the statements of the company, both during the written exchanges with the rapporteur and during the meeting of September 19, 2019, according to which it has set up, in the "Progibos" software, an opposition list regularly kept up to date.58. However, the Restricted Committee considers that this mechanism is insufficient to impose its respect by the call centers and, consequently, the effective taking into account of the opposition of the people. Indeed, the Restricted Committee observes that this exclusion list takes the form of a simple table, to which an information banner in the software refers, inviting

call center operators to consult the table. Nothing is in place to automate the process and ensure its reliability, for example by providing that each number called by a teleoperator is automatically and previously compared to this opposition list to prevent the call. With regard firstly to the economic interests that commercial prospecting represents, both for company X and for its subcontractors, secondly the volume of calls made on behalf of the company and thirdly the number of people concerned (more than 300 people had already expressed their opposition on the day of the meeting), the Restricted Committee considers that only an automated mechanism is sufficiently effective to guarantee that the opposition expressed by the persons concerned is respected.59. In addition, the Restricted Committee notes that this list contains data relating to the postal addresses of individuals. These data are personal data, and are not necessary for the specific purpose of this processing, which is to constitute a list of opposition to telephone prospecting. Indeed, the surnames, first names and telephone numbers are sufficient to ensure compliance with this obligation, except to demonstrate that the list also makes it possible to materialize the opposition to postal prospecting.60. Finally, the Restricted Committee observes that the company does not demonstrate that the data of the people who have expressed their opposition to the processing have actually been purged from the "Progibos" software, the bailiff's report made on July 30, 2019 being silent on this point. 61. This element is therefore not such as to call into question the characterization of the failure referred to at the close of the investigation.5. On the breach of the obligation to cooperate with the supervisory authority62. Article 31 of the GDPR provides that "the controller and the processor as well as, where applicable, their representatives cooperate with the supervisory authority, at the latter's request, in the performance of its tasks. ".63. The Restricted Committee notes the numerous requests from the Commission services after the inspection of March 20, 2018 to obtain the documents necessary for the exercise of their mission, as well as the very partial answers of company X which only communicated a very small proportion of the items requested. It also points out that the Commission systematically granted the company's requests for an extension of time limits without this enabling the disclosure of the documents requested.64. The Restricted Committee also notes that the company did not respond satisfactorily to the formal notice served on it since the response was not accompanied by the supporting documents requested in the context of this procedure and was not intended not all of the shortcomings identified. Here again, the Restricted Committee notes that the company requested and obtained a maximum extension of the period granted by the formal notice.65. The company states that it was badly advised, but the Restricted Committee notes, on the one hand, that in its capacity as data controller, it was up to the company alone to respond to the requests addressed to it and to report on compliance with the GDPR, it being up to it, if

necessary, to choose the competent professionals to whom it intended to entrust the defense of its interests. It was up to her to call on new interlocutors if she felt she was faced with the incompetence of the first persons seized.66. On the other hand, the Restricted Committee points out that the breach relating to the lack of cooperation with the Commission departments, which it considers characteristic in this case, cannot arise from a simple ignorance of the rules relating to the protection data that the company puts forward to explain the difficulty it had in responding to the CNIL's requests. It considers that the lack of response to the requests formulated by the CNIL departments and to the formal notice sent by the President of the Commission, as well as the failure to take these requests into account before the notification of a sanction report, are sufficient to demonstrate, if not a clearly expressed desire not to follow up on the CNIL's requests, at the very least a flagrant lack of interest in these subjects.67. The Restricted Committee notes that this failure ended with the notification of the sanction report, the only moment from which an exchange could be established with the company, through its counsel.68. Finally, the company is wrong to consider that the characterization of this breach is incompatible with the possibility offered to the company to comply by means of a formal notice and to issue observations during exchanges with the rapporteur in the context of the sanction procedure. The principle of cooperation laid down by Article 31 of the GDPR pre-exists the procedure initiated: its non-compliance is established as such and is not linked to the subsequent compliance of the company or to the adversarial principle which governs the penalty procedure.69. The Restricted Committee therefore considers, in the light of these elements, that a breach of Article 31 of the GDPR was established at the expiry of the period set by the formal notice.70. The Restricted Committee takes note of the reality of the cooperation between the company and the rapporteur. It takes into account the compliance efforts of the controller when they are demonstrated, but the decision it issues is also intended to sanction past behavior.71. This element is therefore not such as to call into question the characterization of the breach referred to at the expiry of the time limit set by the formal notice.6. On the breach of the obligation to regulate the transfer of personal data outside the European Union72. Article 44 of the GDPR provides: "a transfer, to a third country or to an international organization, of personal data which are or are intended to be the subject of processing after this transfer can only take place if , subject to the other provisions of this Regulation, the conditions set out in this chapter are complied with by the controller and the processor, including for onward transfers of personal data from the third country or international organization to another third country or to another international organization. All the provisions of this Chapter shall be applied in such a way that the level of protection of natural persons guaranteed by this Regulation is not compromised".73. The Restricted Committee notes

that the company carried out, on the day of the inspection, a transfer of data to States considered as not ensuring an adequate level of protection with regard to Article 45 of the GDPR (Côte d'Ivoire, Morocco, Tunisia ) through its "Progibos" software.74. Given the lack of adequacy, the Restricted Committee finds that it was up to company X to provide appropriate safeguards, in accordance with the provisions of Article 46 of the GDPR.75. Concerning the situation on the day of the check carried out and subsequently emerging from the elements communicated by the company's counsel in response to the formal notice, the data controller has chosen to regulate the transfer of personal data to its subcontractors located outside the territory of the European Union by contractual clauses. The Restricted Committee nevertheless notes that these clauses do not meet the requirements of Articles 44 et seq. of the GDPR since they have not been adopted either by the European Commission or by a supervisory authority, contrary to what is required by the article 46 of the GDPR.76. The Restricted Committee takes note of the new clauses relating to the protection of personal data that the company's counsel communicated to the rapporteur in the context of the sanction procedure and notes that these clauses include the standard contractual clauses of the European Commission. 77. Nevertheless, the Restricted Committee notes on the one hand that, on the day of the closing of the investigation, the contracts which were communicated to it are not definitive documents, since certain clauses are not entirely drafted, and in particular the clauses relating to the provider's remuneration.78. On the other hand, and despite the rapporteur's requests relating precisely to this point during the procedure, the Restricted Committee observes that, on the day of the closing of the investigation, the company did not communicate a version of these contracts signed by both parties. The Restricted Committee finds that a brief examination of the contract binding company X to its subcontractor […] reveals that the company's stamp and the signature of its representative do not appear on the contract itself. but only on the printing of the photograph of the contract, the said stamp "protruding" from the photograph and therefore not being able to appear on the original document. Consequently, this document does not enable the Restricted Committee to find the company's compliance on this point.79. In addition, the Restricted Committee notes that the contract and the appendix linking company X and its subcontractor […] is not signed by the two parties.80. Finally, the standard contractual clauses of the European Commission provide that these clauses are subject to the law of the Member State where the exporter of personal data is established, in this case France. However, the Restricted Committee notes that, in the contracts provided by the company, the clauses are systematically subject to the law of the State where the subcontractor is established.81. The Restricted Committee therefore considers, in view of these elements, that a breach of Article 44 of the GDPR was established at the expiry of the time limit set

by the formal notice.82. The Restricted Committee takes note of the communication to the rapporteur of contracts entered into between the company and its subcontractors. It nevertheless notes that the company has not provided evidence of the establishment, in its relations with its subcontractors, of a legal framework in accordance with the provisions of Articles 44 to 50 of the Rules, and in particular of the fact that it has co-signed with them amendments to the contracts corresponding to the standard contractual clauses for the protection of personal data adopted by the European Commission. Indeed, the Restricted Committee finds that the contracts communicated on July 31, 2019 are incomplete, and that the photographed documents are not signed by the two contracting parties, only the photograph being stamped and signed by company X. Moreover, a contract remains not signed by all of the contracting parties.83. This element is therefore not such as to call into question the characterization of the breach mentioned at the close of the investigation.III. On corrective measures and their publicity84. 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. "85. Article 83 of the GDPR provides:" 1. Each supervisory authority ensures 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.2. Depending on the specific characteristics of each case, administrative fines are imposed in addition to or instead of the measures referred to in points (a) to (h) and (j) of Article 58(2). In deciding whether to

impose an administrative fine and in deciding the amount of the administrative fine, due account shall be taken in each individual case of the following elements: (a) the nature, gravity and the duration of the breach, taking into account the nature, scope or purpose of the processing concerned, as well as the number of data subjects affected and the level of damage they have suffered; b) the fact that the breach has was committed willfully or negligently; c) any action taken by the controller or processor to mitigate the harm suffered by data subjects; d) the degree of liability of the controller or processor, taking into account the technical and organizational measures they have implemented pursuant to Articles 25 and 32; e) any relevant breach previously committed by the controller or processor; f) the degree of cooperation established with the control in with a view to remedying the breach and mitigating its possible negative effects; g) the categories of personal data concerned by the breach; h) the manner in which the supervisory authority became aware of the breach, in particular if, and to what extent the controller or processor notified the breach; (i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned processor for the same purpose, compliance with these measures; j) the application of codes of conduct approved pursuant to Article 40 or certification mechanisms approved pursuant to Article 42; andk) any other aggravating or mitigating circumstances applicable to the circumstances of the case, such as financial benefits obtained or losses avoided, directly or indirectly, as a result of the breach. "86. Firstly, concerning the fine proposed by the rapporteur, the Restricted Committee considers that, in the present case, the aforementioned breaches justify the imposition of an administrative fine on the company for the following reasons 87. The Restricted Committee finds that the breaches of Articles 5-1-c), 12, 13, 14, 21 and 44 of the Rules persisted beyond the time limit set by the formal notice from the President of the Commission and that it was not until the notification of the sanction report that the company took measures to bring itself into compliance, more than eight months after the notification of the formal notice. The company therefore did not fully cooperate with services of the Commission until the initiation of the sanction procedure and has not demonstrated its compliance by the expiry of the time limit.88 It also notes that most of the breaches relate to obligations that the law no. 78-17 of January 6, 1978 as amended imposed it already to data controllers and which are not born of the GDPR. Consequently, it considers ineffective the argument that the company derives from the difficulty it had in applying a new legal framework in a short time.89. It also notes that some of these shortcomings relate to the rights of individuals (right to information and right to object), which were not respected by the company. On the day of the closing of the investigation, there was no evidence of compliance by the company and its subcontractors in this area. However, the Restricted Committee considers that the

non-respect of their rights affects the persons concerned, and particularly with regard to the right of opposition, which is demonstrated by the tone of the emails sent by prospects to the company. Consequently, in view of the consequences for individuals, these breaches should be severely punished.90. The Restricted Committee also recalls that the obligation to regulate the transfer of personal data outside the territory of the European Union is the consequence of the non-existence, on the territory of many states, of protective regulations relating to personal data. Failure to comply with this obligation by the data controller runs the risk of seeing this data processed outside any protective legal framework, to the detriment of the rights of the persons concerned. The Restricted Committee therefore considers that it must be particularly attentive to compliance with this obligation by data controllers.91. All of these reasons justify the imposition of an administrative fine.92. Secondly, regarding the amount of this fine, the company argues that it is disproportionate to the goodwill of the company, which had no intention of violating the GDPR and was only misinformed.93. On this point, the Restricted Committee notes, on the contrary, a perfectly characterized lack of cooperation in this case. The Restricted Committee considers that, far from constituting an element that should lead it to reduce the amount of the fine imposed, the behavior of the company up to the notification of the sanction report must, on the contrary, be taken into account to come increase the penalty imposed, as prompted by point b) of the second paragraph of article 83 of the GDPR.94. The company then considers that the amount of the fine is disproportionate in view of the company's turnover, the rapporteur also not having usefully taken into account the decrease in turnover that occurred in 2018 and announced for the year 2019.95. On this subject, the Restricted Committee considers that the amount of the fine proposed by the rapporteur is measured in the light of the accounting information provided by the company, which shows a turnover of approximately twenty-seven million euros in 2017 and 20 million euros in 2018. It notes that, in view of the breaches in question, Article 83-5-b) of the GDPR sets the amount of the fine incurred at twenty million euros, and that the amount of the proposed fine corresponds to 2.5% of the company's annual turnover, which is not excessive in view of the company's behavior, in particular before the notification of the sanction report, and with regard to the seriousness of the breaches, in particular the violation of the rights of individuals. Finally, if the company demonstrates that its turnover decreased during the year 2018, this result remains of the same order of magnitude as the result for the year 2017 despite a reduction in the net result, and does not justify a reduction in the amount of the fine imposed, which, moreover, is not directly correlated to the company's financial results even though the latter are taken into account in its calculation.96. The Restricted Committee emphasizes the plurality of breaches in question as well as their persistence and seriousness. It takes particular

account of the consequences for the persons concerned and notes that this case originated in a complaint lodged by an individual with the Commission. It also notes the company's reluctance to take into account the applicable legislation on the protection of personal data and its lack of diligence in remedying the shortcomings noted, despite numerous reminders from the Commission's services.97. However, the restricted formation also takes into account the measures that the company has taken during the sanction procedure to bring itself into partial compliance, the fact that it is an SME and the evolution of its financial situation. , in order to determine the amount of a fair and proportionate administrative fine, pointing out that the latter must nevertheless be dissuasive.98. Thirdly, regarding the need to issue an injunction, the company considers that it has brought its practices into compliance with the requirements of the GDPR. It considers that these advances are demonstrated by the responses it provided to the penalty report and then to the observations of the rapporteur and that, therefore, an injunction is not necessary, compliance having already been achieved.99. As explained above, the Restricted Committee considers that the company has not demonstrated, on the day of the closing of the investigation, the compliance of the processing it implements with Articles 5-1-c), 12 , 13, 14, 21 and 44 of the GDPR.100. As the company has failed to comply with these breaches, the proposed injunction should be issued.101. Fourthly, concerning the publicity of its decision, the company indicates that this publicity would have dramatic consequences for the privacy of the people whose personal data is processed by the company, since it would make them a target of computer attacks. .102. On this point, the Restricted Committee notes that the advertisement has no impact on the security of personal data since its decision does not reveal any vulnerability which could be exploited by malicious persons.103. In view of the company's statements regarding its positioning in its field of intervention, which claims to be a major player in its sector, the Restricted Committee considers that the publication of the sanction is justified in view of the importance of the problem of commercial prospecting, both in terms of its scope and its practical consequences for the people canvassed. It also responds to a legitimate expectation of persons who have been or may in the future be the subject of commercial telephone prospecting by the company or other players and will alert them to their rights.104. It follows from all of the above and from consideration of the criteria set out in Article 83 of the GDPR that an administrative fine of 500,000 euros, an injunction accompanied by a penalty payment and an additional sanction of publication for a period of two years are justified and proportionate.FOR THESE REASONSThe Restricted Committee of the CNIL, after having deliberated, decides to: order company X to bring the processing into compliance with the obligations resulting from Articles 5 paragraph 1 point c), 12, 13, 14, 21 and 44 of Regulation No 2016/679 of 27 April 2016

relating to to data protection, and in particular: - to take measures to effectively prevent excessive comments from being recorded in the PROGIBOS software, for example by setting up an automatic detection system for inappropriate words, not relevant and excessive with regard to the purpose of the processing, in order to exclude them from the comment areas or to prevent them from being entered; - to inform the persons from whom personal data is collected directly and indirectly, in the conditions provided for in Articles 12, 13 and 14 of the General Data Protection Regulation No 2016/679 of 27 April 2016, for example by directly informing the data subject, by intermediary of the voice service or the teleoperator, of the existence and the purpose of the device as well as his right of opposition, and by offering him the possibility of obtaining communication of complete information either thanks to the activation of a key on his telephone keypad, or by sending an email; - to implement a procedure to ensure the effectiveness of the rights of opposition expressed by the prospected persons, this procedure having to ensure that the opposition expressed to the subcontractors carrying out the prospecting campaigns is transmitted to the company and passed on to the other subcontractors, that the opposition expressed to the company is transmitted to the subcontractors carrying out the prospecting campaigns, and to ensure that the calls made by the subcontracted teleoperators do not target people who have already expressed their opposition to the processing of their personal data for prospecting purposes; frame the relations between the company and its subcontractors carrying out telephone prospecting campaigns by legal acts meeting the criteria set out in articles 44 to 49 of the Regulations and to ensure, if the company chooses the standard protection clauses data adopted by the European Commission, that the clauses are signed by the parties and governed by the law of the Member State in which the data exporter is established, in this case France; attach to the injunction a penalty payment of 500 (five hundred) euros per day of delay at the end of a period of 1 (one) month following the notification of this deliberation, the supporting documents of compliance before be sent to the restricted training within this period; for breaches of articles 5-1-c), 12, 13, 14, 21, 31 and 44, impose an administrative fine on company X in the amount of 500,000 (five hundred thousand) euros; make public, on the CNIL website and on the Légifrance website, its deliberation, which will no longer identify the company by name at the end of a period of two years from its publication. Chairman Alexandre LINDEN This decision is subject to appeal before the Council of State within two months of its notification.