Deliberation SAN-2022-022 of November 30, 2022 National Commission for Computing and Liberties Nature of the deliberation: Sanction Legal status: In force Date of publication on Légifrance: Thursday, December 08, 2022 Deliberation of the restricted committee no. SAN-2022-022 of 30 November 2022 concerning the company FREEThe National Commission for Computing and Liberties, meeting in its restricted formation composed of Mr. Alexandre LINDEN, President, Mrs. Christine MAUGÜÉ, Mr. Alain DRU and Mr. Bertrand du MARAIS, members; Having regard to the 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 (RGPD); Having regard to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector; Having regard to the postal and electronic communications code; Having regard to law no. 78-17 of January 6, 1978 relating to data processing , files and freedoms, in particular its articles 20 and following; Having regard to decree no. 2019-536 of May 29, 2019 taken for the application of law no. to freedoms; Having regard to deliberation no. 2013-175 of July 4, 2013 adopting the internal regulations of the National Commission for Computing and Freedoms; Having regard to decision no. 2019-188C of September 26, 2019 of the President of the National Commission IT and Liberties to instruct the Secretary General to carry out or have carried out a mission to verify the processing carried out by the FREE and FREE MOBILE companies or on their behalf; Having regard to the decision of the President of the National Commission of data processing and freedoms appointing a rapporteur before the restricted committee, dated December 17, 2020; Considering the report of Mr. François PELLEGRINI, reporting commissioner, notified to FREE on April 21, 2022; Having regard to the written observations paid by the company FREE on June 2, 2022; Having regard to the rapporteur's response to these observations notified to the company FREE on July 13, 2022; Having regard to the new written observations submitted by the company FREE on August 26, 2022, as well as the oral observations made during of the restricted committee meeting; Having regard to the other documents in the file; Were present at the restricted committee meeting of September 29, 2022:- Mr François PELLEGRINI, statutory auditor, heard in his report; As representatives of the company FREE:- […];- […];- […];- […];- […];- […];- […];- […]. As representatives of the company […], joined by videoconference:- […];- […]. The FREE company having had the floor last; The Restricted Committee adopted the following decision: I. Facts and procedure1. The company FREE (hereinafter "the company"), whose head office is located at 8 rue de la Ville-L'Evêque in Paris (75008), is a subsidiary of the ILIAD group which is a fixed telecommunications operator. Founded in 1999, the company has approximately 179 employees.2. For the year 2020, the company achieved a

turnover of approximately […] euros, for a net result of approximately […] euros. In 2021, the company had approximately […] subscribers, […].3. Between October 2018 and November 2019, the National Commission for Computing and Liberties (hereinafter "the CNIL" or "the Commission") received 41 complaints against the Company. Of these complaints, 10 were examined in the context of this sanction procedure. The complainants notably reported difficulties encountered in exercising their rights of access or erasure. Some of these referrals also related to the security of the personal data of the company's customers.4. On February 8, 2019, the company notified the CNIL of a personal data breach and then, on February 22, 2019, an additional notification. They indicated that approximately 4,100 Freeboxes had been put back into circulation without their reconditioning being effective, that is to say without the data of the previous subscriber being erased from the hard disk of the Freebox.5. Two on-site inspection missions, at the premises of the FREE company and then of the FREE MOBILE company, were carried out on January 21 and 22, 2020.6. Reports No. 2019-188/1 and No. 2019-188/2, drawn up by the delegation on the day of the inspections, were notified to the company on January 23, 2020. On this occasion, requests for additional additional information and documents have been sent to the company. The legal department of the ILIAD group responded by emails of February 3 and 10, 2020.7. A documentary check was also carried out at the companies FREE and FREE MOBILE on June 3, 2020. The legal department of the ILIAD group responded by email dated June 29, 2020.8. For the purposes 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.9. A request for additional information was finally sent to the company by letter dated March 16, 2022. The legal department of the ILIAD group responded by letter dated March 31, 2022.10. On April 21, 2022, the rapporteur notified the company of a report detailing the breaches of the GDPR that he considered constituted in this case.11. This report proposed to the Restricted Committee to issue an administrative fine and an injunction to bring the processing into compliance with the provisions of Article L.34-5 of the Post and Electronic Telecommunications Code (CPCE) and Articles 7-1 , 15, 17, 32 and 33 of the GDPR, accompanied by a penalty payment per day of delay at the end of a period of three months following the notification of the deliberation of the restricted formation. 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.12. On June 2, 2022, the company produced its observations in response to the sanction report.13. On July 13, 2022, the rapporteur sent his response to the company's observations.14. On August 26, 2022, the company produced new observations in response to those of the rapporteur.15. On September 5, 2022,

the rapporteur informed the company and the chairman of the restricted committee of the closure of the investigation. On the same day, the chairman of the restricted committee sent a notice to attend the restricted committee meeting of September 29, 2022.16. On September 14, 2022, the company produced a certificate from its service provider, the company […], relating to the supply of telephone numbers and e-mail addresses intended for a commercial prospecting campaign over the period from December 2 to 6, 2019.17 . On September 21, 2022, the chairman of the Restricted Committee notified the company of the postponement of the closing of the investigation to Monday September 26, 2022 and asked it to notify the company […] so that one of its representatives could attend at the restricted training session.18. The company FREE and the rapporteur presented oral observations during the session of the Restricted Committee.19. Mr […] and Mr […], whose hearing was deemed useful, were heard pursuant to Article 42 of Decree No. 2019-536 of May 29, 2019. II. Reasons for decisionA. On the breach of the obligation to obtain the consent of the person concerned by a direct marketing operation by means of e-mail and SMS20. Under the terms of article L.34-5 of the CPCE: “Direct prospecting by means of an automated electronic communications system […], a fax machine or e-mails using the contact details of a natural person […] is prohibited.] who has not previously expressed their consent to receive direct marketing by this means. For the purposes of this article, consent means any expression of free, specific and informed will by which a person accepts that personal data personal data relating to it are used for the purpose of direct prospecting. […] ".21. Pursuant to Article 4(11) of the GDPR: "For the purposes of this Regulation, […] 'consent' of the data subject means any free, specific, informed and unambiguous expression of will by which the data subject accepts, by a declaration or by a clear affirmative act, that personal data relating to him or her may be processed ".22. Under Article 7(1) of the GDPR: "In cases where processing is based on consent, the controller is able to demonstrate that the data subject has given consent to the processing of personal data. concerning her ".23. The rapporteur to propose to the restricted committee to consider that the company has failed to comply with its obligations resulting from articles L. 34-5 of the CPCE and 7, paragraph 1, of the GDPR, as clarified by the provisions of article 4, paragraph 11, of the GDPR, is based on the fact that the company FREE, which carries out commercial prospecting operations electronically via a personal database collected by its service provider, the company […], is not able to provide proof of unambiguous, specific, free and informed consent of prospects before they were canvassed during a commercial prospecting campaign by electronic means (email and SMS) in December 2019. To consider the breach as constituted, the rapporteur relied on the elements collected during the on-site inspection operations (reports n° 2019-188/1 and n° 2019-188/2) as well as on additional documents transmitted at the end of

these verifications, in particular a document indicating that the company "obtained in December 2019 from this partner files of prospects to carry out a commercial prospecting campaign by SMS and by email" and that "this unique campaign […] was only made in December 2019 and not continued in 2020”.24. In defence, the company maintains that it "actually considered carrying out a prospecting campaign by SMS and e-mail with non-subscribers and signed an estimate with its partner […] [the company […]] for this purpose ". However, she indicates that she expressed herself poorly in the document produced in evidence and that she cannot be blamed for any breach because this campaign "was canceled before it was even launched". She adds that one of the reasons why this campaign was not carried out is "that it was originally intended to promote Free's fiber optic services. Due to a shortage, between October 2019 and January 2020, user equipment necessary for the installation of optical fiber […], Free ultimately did not wish to promote services whose delivery it could not have ensured". During the restricted training session, the company reiterated these elements.25. The Restricted Committee notes that the document on which the rapporteur relies contains erroneous elements and that the company has provided convincing explanations of the circumstances in which the error occurred.26. Under these conditions, the Restricted Committee considers that it has not been established that the electronic commercial prospecting campaign referred to was carried out and that the elements of the debate do not make it possible to conclude that there was a breach. to the obligations resulting from article L. 34-5 of the CPCE and article 7-1 of the GDPR.B. On breaches in connection with the exercise of rights27. Under Article 12 of the GDPR: "1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 as well as to carry out any communication under Articles 15 to 22 and Article 34 with regard to processing to the data subject in a concise, transparent, comprehensible and easily accessible manner, in clear and simple terms, in particular for any information intended specifically for a child. […].2. [… 3. The controller shall provide the data subject with information on the measures taken following a request made pursuant to Articles 15 to 22, as soon as possible and in any event within one month from 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 data subject of this extension and the reasons for the postponement. within one month of receipt of the request. Where the data subject submits the request in electronic form, the information shall be provided electronically where possible, unless the data subject requests otherwise.4. If the controller does not comply with the request made by the data subject, he shall inform the latter without delay and at the latest within one month of receipt of the request of the reasons for his inaction and the possibility of lodging a complaint with a supervisory authority and of lodging a

judicial appeal. […] “.28. Pursuant to Article 15 of the GDPR: “1. The data subject has the right to obtain confirmation from the controller as to whether or not personal data relating to him or her are being processed and , where available, access to such personal data and the following information:[…]g) where the personal data is not collected from the data subject, any available information as to its source. […] 3. The controller shall provide a copy of the personal data being processed. […].4. The right to obtain a copy referred to in paragraph 3 does not affect the rights and freedoms of others. "29. Pursuant to Article 17 of the GDPR:" 1. The data subject has the right to obtain from the controller the erasure, as soon as possible, of personal data concerning him and the controller has the obligation to erase this personal data as soon as possible, when one of the following reasons applies: a) the personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed; […]. “1. On the breach of the obligation to respect the right of access30. access, is based on five referrals to the CNIL, from Messrs. […] (complaint no. 19009149), […] (complaint no. 19005208), […] (complaint no. 19014037), […] (complaint no. ° 19015831) and […] (complaint no. 19016618). In the context of these complaints, people reported difficulties encountered in exercising this right, even though their requests had indeed been received.31. The rapporteur indicates that these five referrals relate in particular to access to personal data and, of these five referrals, four relate more specifically to obtaining information on the source from which their data originates.32. The rapporteur observes that it emerges from the observations made during the inspection procedure or from the elements communicated subsequently that the company did not respond within the prescribed time limits to the aforementioned requests to exercise the complainants' rights of access or that it gave them an incomplete answer as to the source of their data.33. In defence, the company argues, with regard to the lack of response provided within the deadlines, that the procedures implemented were not followed due to isolated human errors. It also argues that the small number of complaints noted in the report (2) should be compared to the number of requests it deals with per year (around 600). Finally, the company indicates that these referrals predate the implementation of a new ticketing tool that it has been using since June 2019, which has made it possible to make improvements to the procedure for processing requests to exercise rights . It therefore considers that these specific shortcomings have now been resolved.34. With regard to requests for information on the source of the data, the company considers that, in accordance with the provisions of recital 63 of the GDPR and Article 15-4 of the GDPR, it is not required to respond thereto. that it would be led to reveal information subject to business secrecy (the identity of the data broker who provided it with the data). It argues that in reality, the information that is sought by the applicants is the identity of the primary

source which is at the origin of the collection of the applicant's data. It indicates that it has changed its procedures during the sanction procedure since it now asks its data brokers to send it the identity of the primary source at the origin of this collection, information that the company transmits to his turn to the plaintiffs.35. The Restricted Committee notes, with regard to the lack of response provided within the deadlines, that it follows from Article 12 of the GDPR that when a request to exercise rights is addressed to it, the data controller must provide to the person concerned information on the measures taken to respond to his request as soon as possible and in any case within one month. The Restricted Committee also recalls that when the data controller no longer holds all or part of the data on the person exercising his right of access (for example, the data has been deleted or the organization has no data on the person), he must nevertheless respond to the applicant within a maximum period of one month.36. With regard to the information to be provided on the source of the data under Article 15 of the GDPR, the Restricted Committee notes first of all that it emerges from the aforementioned articles that the limitation of the right of access by "the rights and freedoms others" which include trade secrets, applies only to Article 15-4 of the GDPR, relating to persons requesting a copy of their data, and not to Article 15-1 of the GDPR, relating to persons requesting information from a data controller who is processing their data. In this case, the Restricted Committee notes that the plaintiffs are not asking the company to obtain a copy of their data or access to this data, but only information as to the source from which their data come . The Restricted Committee therefore considers that Article 15-4 of the GDPR is inapplicable. In any event, it considers that Article 15-1 of the GDPR could only be limited under the conditions provided for by Article 23 of the GDPR, which is not the case here.37. Next, the Restricted Committee notes that any processing of personal data must comply with the principles set out in Article 5, paragraph 1, a), of the GDPR which provides that personal data must be processed in a transparent manner with regard to of the person concerned. She points out that it emerges from the guidelines on transparency of the "Article 29" working group, which has become the European Data Protection Board, that "the source from which the personal data originates" is understood as " the specific source of the data or, failing that, the nature of the sources (i.e. public and private sources) and the types of organisations, companies and sectors". The Restricted Committee considers that the data subject's right of access constitutes a fundamental guarantee of the transparency of the methods of data processing. It deduces from this that the data controller must in principle communicate "the specific source" relating to the data and that the limitation of the right of access to indications of the "nature of the sources, types of organisations, companies and sectors "can only intervene when he does not hold this information, the identification of the specific source of the data subject's personal data being

impossible.38. The Restricted Committee also notes that the right of access – Article 15 of the GDPR being clarified by recital 63 – aims to enable the data subject to become aware of the processing of his data and to verify its lawfulness. The exercise of this right therefore presupposes that the information provided is as precise as possible.39. The Restricted Committee considers that the refusal to communicate the identity of the data broker from which the data of the person concerned was obtained, when the company has this information, and to limit the right of access to the "source primary" of the collection (i.e. the first actor in the chain to have collected the personal data of the person concerned), which was moreover not provided in this case at the time of the control , amounts to preventing the data subject from being able to verify the lawfulness of the processing carried out by the data controller and, in particular, the lawfulness of the data transmissions already carried out. The Restricted Committee therefore considers that the right to have access to the identity of the source of the data is necessary to allow the person concerned to give their consent and to exercise the rights conferred on them by the GDPR, in particular the right of opposition, depending on the type of commercial prospecting implemented by the controller having obtained the data from brokers.40. The Restricted Committee considers that a breach of the obligations of Articles 12 and 15 of the GDPR is constituted for all the above-mentioned complaints since the company has not processed the access requests sent to it within the time limit was assigned to it, thus leaving people in the dark about the data processed by the company concerning them or that it gave them an incomplete answer regarding the source of their data. In addition, the Restricted Committee considers that the company did not provide, on the date of the closing of the investigation, elements allowing to certify compliance with regard specifically to the point relating to the source data.2. On the breach of the obligation to respect the right to erasure41. The rapporteur, to propose to the Restricted Committee to consider that the company has failed to comply with its obligations resulting from Article 17 of the GDPR, relies on two referrals to the CNIL, from Messrs. […] (complaint no. 19009870) and […] (complaint no. 19012463), in which the complainants reported their difficulties in exercising their right to erasure.42. The rapporteur indicates that the interested parties requested the deletion of their "Free.fr" email account, by sending, respectively on February 10 and 3, 2019, a form dedicated to the "deletion of a main Free access account free" on which it is specified that "the effective deletion of accounts requires a period of 48 hours after receipt of the mail".43. The rapporteur observes that it emerges from the findings made during the review procedure and from the information communicated subsequently that the complainants did not obtain a response to their requests for deletion made by registered letter and that the measures to satisfy their requests erasure were not implemented, since the "SIEBEL" customer

database contained various personal data specific to the complainants, such as their connection identifier, surname, first name and postal address. In addition, the status of the latter's "free.fr" e-mail account was indicated as being "active".44. In defence, the company argues that requests for "deletion of a free access free account" are not requests for erasure within the meaning of the GDPR and are not subject to any legal deadline [...]" but are assimilated "to a request for termination of contract". The company concludes that it "would be totally disproportionate to consider that [these requests fall under] Article 17 of the GDPR and the deadlines set out in Article 12.3 of the GDPR". The company specifies that it is only required to "respect the principle of limiting the retention of the data concerned, without this imposing the immediate deletion of all the data concerned". It indicates in this sense that it has a "legal obligation to keep the data associated with electronic messaging accounts for a period of 1 year", in accordance with Article L. 34-1 of the CPCE.45. On this point, the Restricted Committee considers first of all that the plaintiffs' requests are clear, in that each involved a request for the general deletion of an e-mail account, addressed to the company by the dedicated form implemented by it. This request necessarily implied the request for the erasure of personal data related to the use of the account. The company cannot therefore rely on the fact that this request for deletion would not have been clear and treated as a request for deletion within the meaning of the GDPR.46. Next, the Restricted Committee considers that it follows from Article 12.3 of the GDPR that the controller must provide applicants with information on the measures taken following a request made pursuant to Article 17 of the GDPR in a maximum period of one month, which may be extended for a reasonable period in certain cases. However, it notes that it was only on May 23, 2022 that the company provided a response to the complainants, i.e. approximately three years after Messrs. […] and […] exercised their rights. This response time violates article 12.3 of the GDPR.47. Finally, the Restricted Committee considers that if the request to delete an e-mail account does not necessarily imply the deletion of all the data relating to this account (some data may be kept with an intermediate archive status), a breach of Article 17, paragraph 1, a) of the GDPR is in any case characterized in this case when the status of the account was active and the e-mail was still accessible to the persons concerned several years after making their requests.48. The Restricted Committee considers that a breach of the obligations arising from Articles 12 and 17 of the GDPR is constituted when it was the company's responsibility to process the request for erasure of the complainants' personal data within the time limits set.49 . It notes that, in the context of this procedure, the company has justified having taken measures to comply with the obligations arising from Article 17 of the GDPR.C. On the breach of the obligation to ensure the security of personal data50. According to Article 32(1) of the GDPR: "Taking into account

the state of knowledge, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risks , the degree of probability and severity of which varies, for the rights and freedoms of natural persons, the controller and the processor implement the appropriate technical and organizational measures to guarantee a level of security appropriate to the risk, including including among others, as required: a) […]; b) means to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; c) […]; d) a procedure for regularly testing, analyzing and evaluating the effectiveness of the technical and organizational measures to ensure the security of the processing. On passwords for accessing customer accounts51. The rapporteur, to propose to the Restricted Committee to consider that the company has failed to comply with its obligations resulting from Article 32 of the GDPR, is based first of all on the fact that the password randomly generated by the company when creating he user account on the company's website, during a recovery procedure or during a password renewal, is eight characters long and can only contain the same type of characters. Next, the rapporteur notes that all the passwords generated when creating a user account on the company's website were stored in clear text in the company's subscriber database until January 23, 2020 Finally, the rapporteur notes that the delegation was informed that the password which is generated when creating a user account on the company's website is transmitted by e-mail or post to the user and indicated in clearly in the body of the message. Similarly, the rapporteur notes that three referrals from Messrs […] (complaint no. 19018181), […] (complaint no. 18023964) and […] (complaint no. 19013170) show that the password which is associated with the "free.fr" e-mail account is transmitted by e-mail or post to the user and indicated in clear text in the body of the message.52. In defence, the company argues that as data controller, it is free to choose the security measures to put in place. It maintains in this sense that the recommendations of the CNIL or the National Agency for the Security of Information Systems (ANSSI) cited in the report are not imperative. Therefore, the company considers that no breach can be found in the absence of a "data breach that affected access to the subscriber area".53. The company then argues in particular that at the time of the control operations, subscribers were encouraged to change their password on their subscriber area. She also indicates that the initial password she assigned has a high level of robustness and that the subscriber area only allows access to "basic" information and not to sensitive information. Finally, the company announced that it had taken several measures to comply with the obligations arising from article 32 of the GDPR with regard to security relating to passwords by strengthening the robustness of the passwords generated or created. by the company and the mandatory renewal of passwords during a recovery procedure or upon first connection. The company also indicates that it has stopped

storing passwords in the clear in the database and that it has stopped communicating passwords in the clear (in particular, by stopping the transmission of passwords to new subscribers in plain text by e-mail, the creation, by new subscribers, of their password, which must comply with the recommendations of the CNIL in this area and the elimination of paper forms that must be completed and then sent by post to obtain the deletion of a "Free free access" account in which the communication of the password in plain text was previously required).54. The Restricted Committee considers that in this case, the authentication procedure as well as the methods for storing and transmitting passwords implemented by the company are not appropriate with regard to the risk that the person concerned would the capture of their username and password by a third party.55. It follows from the provisions of Article 32 of the GDPR that the data controller is required to ensure that the automated data processing that he implements is sufficiently secure. The sufficiency of the security measures is assessed, on the one hand, with regard to the characteristics of the processing and the risks it induces, and on the other hand, by taking into account the state of knowledge and the cost of the measures. The implementation of a robust authentication policy is an elementary security measure that generally contributes to compliance with the obligations of Article 32 of the GDPR. Despite the non-mandatory nature of 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 technical note of the ANSSI relating to the passwords cited in the report, the latter set out basic security precautions corresponding to the state of the art and thus constitute relevant insight for assessing the sufficiency of the measures put in place by a person in charge of treatment.56. In this case, with regard to the authentication procedure, the Restricted Committee considers that the use of a short or simple password without imposing specific categories of characters and without additional security measures, can lead to attacks by unauthorized third parties such as "brute force" or "dictionary" attacks, which consist of successively and systematically testing numerous passwords and thus leading to a compromise of the associated accounts and data to be personal character they contain. The purpose of blocking measures is to limit these types of attacks.57. The Restricted Committee notes that the Commission recommends in its deliberation no. that, in order to meet the strength requirements for passwords and ensure a sufficient level of security, when authentication is based, as in this case, on a username and a password, without the implementation of a additional security, the password must have at least twelve characters and contain at least one uppercase letter, one lowercase letter, one number and one special character. When the password has eight characters, containing three of the four categories of characters (uppercase letters, lowercase letters, numbers and special characters), it must be

accompanied by an additional security measure in order to ensure a level of security and sufficient confidentiality.58. The Restricted Committee notes that the need for a strong password is also underlined by the ANSSI, which specifies that "a good password is above all a strong password, i.e. difficult to find even using automated tools. The strength of a password depends on its length and the number of possibilities existing for each character composing it. Indeed, a password made up of lowercase letters, uppercase letters, special characters and digits is technically more difficult to discover than a password consisting of only lowercase ".59. Consequently, in this case, the Restricted Committee considers that, given the volume and nature of the personal data that may be contained in the millions of subscriber accounts (in particular surname, first name, landline number, mobile phone number, e-mail address and invoices), the imposition by the latter of connection passwords to customer accounts, consisting only of eight characters, which can be of a single category of characters, without additional security measures, as well as the acceptance of their renewal according to these same methods, does not make it possible to ensure the security of the personal data processed by the company or to prevent unauthorized third parties from having access to the personal data of customers.60 . With regard to the procedure for storing passwords in plain text, the Restricted Committee observes that anyone with access to FREE's customer database - whether information system administrators at the within the company or of an attacker in the event of its compromise – could directly collect the identifiers and passwords in plain text of each of the subscribers and thus access the information contained in their accounts, then possibly modify them, attempt to access other service accounts using these identifiers (the same identifiers and passwords are often used on several services) or, again, resell these to other attackers.61. With regard to the transmission of the password in clear, the fact that these elements are transmitted in clear via a simple electronic or postal mail, makes them easily and immediately usable by a third party who would intercept them or have undue access to the messaging electronic mail of the user, since these passwords do not have a limited duration or their modification is not required during the first use. This third party could then not only access all the personal data present in the FREE user account of the person concerned (surname, first name, Freebox telephone number, postal address and e-mail address) but also download their invoices and the statement of its consumption, modify the password, the e-mail address or even the options of the account. Given these potential consequences for the protection of personal data and the privacy of individuals, the Restricted Committee considers that the measures deployed to guarantee data security in this case are insufficient.62. The Restricted Committee holds that breaches of the obligations arising from Article 32 of the GDPR are thus constituted due to the insufficient robustness of the passwords as well as their storage

and transmission in clear text to the company's subscribers.63. It notes that, in the context of this procedure, the company has justified having taken measures to comply with the obligations arising from Article 32 of the GDPR.2. On the reconditioning of "Freebox" boxes 64. The rapporteur, in order to propose to the Restricted Committee to consider that the company has failed to comply with its obligations resulting from Article 32 of the GDPR, relies on the fact that 4,137 boxes "were put back into circulation without their reconditioning being perfect", due in particular to an error having led to the deletion of a procedure (also called "test sequence") intended to erase the data stored on the hard disks of these "Freebox" boxes.65. In defence, the company argues that the security obligation provided for in Article 32 of the GDPR is an obligation of means, which only requires it to implement security measures adapted to the risks of the processing it carries out. It considers that in this case, the measures implemented were sufficient, given that this incident resulted from two successive human errors, that there is an "anecdotal risk that the Freeboxes will be misused to store sensitive data "and that the circumstance that a single subscriber reported these facts led to only one "effective access to the privacy of a former subscriber having occurred", which "reflects the limited likelihood of this risk materializing in practice ". The company also considers that the "seriousness of this incident must be qualified given the nature of the data usually stored on the Freeboxes" - which is mainly limited to the recording of TV programs and marginally to the storage of personal photos or videos. Finally, the company recalls that at the end of the campaign aimed at recalling the boxes concerned, it sent a replacement Freebox to the 322 subscribers who had not returned their Freebox and that in any event, these were deactivated in July 2022.66. The Restricted Committee considers first of all that the technical and organizational measures implemented were not sufficient with regard to the risk of data breach in this case since no process for raising the alert was implemented. to check the effective execution of the test sequences including the deletion of data. This failure made it possible for unauthorized third parties, in this case the new owners of the 4,137 badly reconfigured "Freebox" boxes, to gain access to the data of former subscribers which would have been stored on the hard drives of these boxes. This data could be photos, personal videos or the recording of television programs by the user. The Restricted Committee also recalls that it is not the data breach which is in question, but the insufficiency of security measures which made possible the occurrence of such a breach.67. Next, on the limited probability of the risk materializing due to the receipt of a single report by the company, the Restricted Committee notes that this report is indicative of the inadequacy of the technical and organizational measures implemented, the latter having led discovering the incident.68. Furthermore, on the nature of the data stored in the Freebox boxes, the Restricted Committee notes that the current and main use of the

Freeboxes is the recording by the user of television programs, but considers that this current use does not cannot rule out the possibility that some of the badly refurbished Freebox boxes contain personal photos or videos, which are highly personal.69. Finally, the Restricted Committee considers that the fact that a replacement Freebox was sent to the 322 subscribers who did not return their old boxes does not rule out the risk that the latter had access to the data of former subscribers . Indeed, on March 31, 2022 – more than three years after the incident was reported – the company indicated that this risk had still not been ruled out since “322 [boxes] are still used by subscribers without we [the company] know if the data recorded is that of the previous subscriber or the subscriber who uses it”. In addition, only the deactivation of the 322 Freeboxes not returned made it possible to eliminate this risk; however, this deactivation took place in July 2022, more than three years after the incident was reported.70. The Restricted Committee considers that a breach of the obligations arising from Article 32 of the GDPR is constituted due to the insufficiency of the technical and organizational measures of the process of reconditioning the "Freebox" boxes to ensure the security of personal data. subscribers of the company.71. It notes that, in the context of this procedure, the company has justified having taken measures to comply with the obligations arising from Article 32 of the GDPR.D. On the failure to document any personal data breach72. Under Article 33(5) of the GDPR: "The controller shall document any personal data breach, stating the facts about the personal data breach, its effects and the measures taken to remedy it. The documentation thus compiled enables the supervisory authority to verify compliance with this article.”73. The rapporteur, to propose to the Restricted Committee to consider that the company has failed to comply with its obligations resulting from Article 33 of the GDPR, argues that the data breach was not documented in accordance with the provisions of the aforementioned article.74 . In defence, the company argues that Article 33 of the GDPR does not impose formalism and that the documentation of a security incident does not have to be included in a data breach register. It considers that the documentation provided following the inspection complies with the conditions of the aforementioned article and that it is not required to specify "the result of the measures taken", namely, as requested by the rapporteur, " the number of Freeboxes recovered by Free after the incident and the date of their recovery ".75. The Restricted Committee notes that at the end of the two days of on-site inspection, the company had not documented the data breach constituted by the recirculation of 4,137 badly reconditioned boxes in a data breach register data. The documentation subsequently communicated in response to requests from the delegation of control did not make it possible to know whether all the "Freebox" boxes whose reconditioning had not been effective had been repatriated and, if so, on what date. However, the Restricted Committee notes that it follows

from the principle of responsibility laid down by the GDPR that the data controller must sufficiently document his practices to be able to demonstrate his compliance. In this case, the Restricted Committee considers that the aforementioned elements - namely whether all the "Freebox" boxes whose reconditioning had not been effective had been repatriated and, if so, on what date - are part of the information to be communicated in order to ascertain the factual elements making it possible to assess the effectiveness of the measure taken in dealing with the violation.76. The Restricted Committee considers that a breach of the obligations arising from Article 33 of the GDPR is constituted when the documentation established at the end of the two days of on-site inspection and subsequently in response to requests from the CNIL delegation , did not make it possible to find out about all the measures taken to remedy the breach of personal data and its effects.77. It notes that, in the context of this procedure, the company has justified having taken measures to comply with the obligations arising from Article 33 of the GDPR.III. On corrective measures and their publicity78. Under the terms of III of article 20 of the modified law of January 6, 1978: "When the data controller or its subcontractor does not comply with the obligations resulting from regulation (EU) 2016/679 of April 27, 2016 or from the this law, the president of the National Commission for Computing and Liberties may also, if necessary after having sent him the warning provided for in I of this article or, if necessary in addition to a formal notice provided for in II, seize the restricted formation of the commission with a view to the pronouncement, after adversarial procedure, of one or more of the following measures: (…) 7° With the exception of cases where the processing is implemented by the State, an administrative fine not to exceed 10 million euros or, in the case of a company, 2% of the total worldwide annual turnover of the previous financial year, whichever is higher. mentioned in 5 and 6 of article 83 of regulation (EU) 2016/679 of April 27, 2016, these ceilings are increased, respectively, to 20 million euros and 4% of said turnover. The Restricted Committee takes into account, in determining the amount of the fine, the criteria specified in the same Article 83. "79. Under the terms of Article 83 of the GDPR:" 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. ", before specifying the factors to be taken into account in deciding whether to impose an administrative fine and in deciding the amount of this fine.80. Firstly, on the principle of imposing a fine , the company maintains that such a measure is not necessary and would not be proportionate in view of the facts with which it is charged.81 The Restricted Committee recalls that it must take into account, when imposing an administrative fine, the criteria specified in Article 83 of the GDPR, such as the nature, gravity and duration of the breach, the measures taken by the controller to mitigate the damage

suffered by the data subjects, the degree of cooperation with the supervisory authority and the categories of personal data affected by the breach.82 The Restricted Committee considers first of all that the company has demonstrated certain negligence with regard to fundamental principles of the GDPR since several breaches are constituted, relating in particular to human rights and security. The Restricted Committee adds that three breaches gave rise to complaints.83. The Restricted Committee then notes that the company is a particularly important player in the Internet access provider sector since it had approximately 6.9 million subscribers in 2021, which ranked it among the main access providers to the Internet in France. It therefore has significant resources enabling it to deal with questions of protection of personal data.84. Consequently, the Restricted Committee considers that an administrative fine should be imposed with regard to the breaches set out in Articles 12, 15, 17, 32 and 33 of the GDPR.85. Secondly, with regard to the amount of the fine, the Restricted Committee recalls that administrative fines must be both dissuasive and proportionate. In this case, the Restricted Committee considers that the company has failed to comply with its obligations resulting from Articles 12, 15, 17, 32 and 33 of the GDPR, relating in particular to the rights of individuals and to basic measures related to data security. of a personal nature. The Restricted Committee adds that several shortcomings have given rise to complaints, even if it observes that the complaints revealing the existence of shortcomings appear to be few in number – indeed, their number, of ten, must be related to the number of subscribers. amounting to approximately 6.9 million – so that these failings cannot be regarded as having a systemic character.86. The Restricted Committee also recalls that the activity of the company and its financial situation must be taken into account for the determination of the sanction and in particular, in the event of an administrative fine, of its amount. It notes in this respect that the company reports a turnover of […] euros in 2020 for a net profit of approximately […] euros.87. Therefore, in view of these elements, the Restricted Committee considers that the imposition of an administrative fine of 300,000 (three hundred thousand) euros appears justified.88. Thirdly, an injunction to bring processing into compliance with the provisions of Article L. 34-5 of the CPCE and Articles 7-1, 15, 17, 32 and 33 of the GDPR was proposed by the rapporteur during notification of the report.89. 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.90. As indicated above, the Restricted Committee notes that the company has taken measures to bring its processing into compliance with the provisions of Articles 17, 32 and 33 of the GDPR. The Restricted Committee considers, however, that the company did not provide, on the date of the closing of the investigation, elements enabling it to certify that its processing was in compliance with the provisions of

Article 15 of the GDPR, insofar as it intends to provide only information relating to the identity of the "primary source" of the collection of the data subject's data (i.e. the first actor in the chain to have collected personal data of the data subject). Consequently, the Restricted Committee considers that an injunction should be issued on this point.91. Finally, with regard to the publication of the sanction decision, the company maintains that such a measure would be neither necessary nor proportionate in view of the alleged breaches which it refutes and its compliance.92. The Restricted Committee considers that the publicity of the sanction is justified in view of the plurality of breaches committed and the need to inform the persons, and in particular the customers concerned, of the failures related to the processing of personal data put in place. work by the company. It also considers that this measure will make it possible to inform the persons concerned of the past existence of the breaches sanctioned, insofar as these facts have been the subject of several complaints.FOR THESE REASONSThe restricted formation of the CNIL, after having deliberated, decides to: pronounce against FREE an administrative fine in the amount of 300,000 (three hundred thousand) euros for breaches of Articles 12, 15, 17, 32 and 33 of the GDPR; issue an injunction against the company FREE to provide an exhaustive response to the requests of Messrs. […] (complaint no. 19014037), […] (complaint no. 19015831), […] (complaint no. 19016618) and […] (complaint no. 19005208) which specifies the identity of the data broker from which it obtained data subjects' data; accompany the injunction with a penalty payment of 500 (five hundred) euros per day of delay at the end of a period of one month following the notification of this deliberation, the supporting documents of compliance must be sent to the restricted training within this period; make public, on the CNIL site and on the Légifrance site, its deliberation, which will no longer identify the company by name at the end of a period of two years from its publication .President Alexandre LINDENThis decision may be appealed to the Council of State within two months of its notification.