Deliberation SAN-2022-021 of November 24, 2022 National Commission for Computing and Liberties Nature of the deliberation: Sanction Legal status: In force Date of publication on Légifrance: Tuesday November 29, 2022 Deliberation of the restricted committee n°SAN-2022-021 of 24 November 2022 concerning the company ÉLECTRICITÉ DE FRANCE The National Commission for Computing and Liberties, meeting in its restricted formation composed of Mr Alexandre LINDEN, Chairman, Mr Philippe-Pierre CABOURDIN, Vice-Chairman, Mr Alain DRU and Mr Bertrand du MARAIS, members; Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data and the free movement of such data; Having regard to Directive 2002/58/EC of the European Parliament and of the Council of July 12, 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. information technology, files and freedoms; Having regard to deliberation no. 2013-175 of July 4, 2013 adopting the internal regulations of the National Commission for Information Technology and Freedoms; Having regard to decision no. 2021-020C of January 4, 2021 of the President of the National Commission for Computing and Liberties to instruct the Secretary General to carry out or have carried out a mission to verify the processing carried out by the company ÉLECTRICITÉ DE FRANCE or on its behalf; Having regard to the decision of the President of the National Commission for Computing and Liberties appointing a rapporteur to the restricted committee, dated May 19, 2022; Having regard to the report of Mrs Valérie PEUGEOT, rapporteur commissioner, notified to the company ÉLECTRICITÉ DE FRANCE on June 23 2022; Having regard to the written observations submitted by the board of ÉLECTRICITÉ DE FRANCE on July 25, 2022; Having regard to the response of the rapporteur to these observations notified on August 11, 2022 to the board of the company; Having regard to the written observations submitted by the board of the company ÉLECTRICITÉ DE FRANCE on September 9, 2022; Having regard to the other documents in the file; Were present, during the restricted committee session of October 13, 2022: - Mrs. Valérie PEUGEOT, auditor, heard in her report; in her capacity as representatives of the company ÉLECTRICITÉ DE FRANCE:- […];The company ÉLECTRICITÉ DE FRANCE having the floor last;The Restricted Committee adopted the following decision:I. Facts and procedure1. Founded in 1955, ÉLECTRICITÉ DE FRANCE (hereinafter "EDF" or "the company") is a public limited company with a board of directors whose registered office is located at 22 avenue de Wagram in Paris (75008).2 . The EDF group, which includes the parent company

EDF and its subsidiaries, is mainly active in France and abroad on the electricity markets and, in particular, in the production of electricity (nuclear, renewable and fossil). and wholesale, trading, transmission, distribution and supply of electricity. The EDF group is also present in the gas and energy services markets, as well as in the construction, operation and maintenance of power plants and electricity networks and provides waste recycling and energy services. The EDF group employs more than 131,000 people, including more than 63,000 for EDF.3. In 2020, the EDF group achieved a turnover of more than 69 billion euros for a net result of […] euros. In 2021, its turnover amounted to more than 84 billion euros for a net profit of […] euros.4. As part of the services provided by the company, personal data of its customers and prospects are processed. At the end of December 2020, the company had 25.7 million customers in its databases for the supply of electricity, gas and services and approximately […] prospects, in the private market.5. The National Commission for Computing and Liberties (hereinafter "the CNIL" or "the Commission") has received several complaints against EDF, relating to the exercise of rights between August 2019 and December 2020.6. An online check was carried out on the "www.edf.fr" website on February 15, 2021. Minutes no. 2021-020-1, drawn up by the delegation following the check, were notified to EDF on February 17, 2021.7. A control mission on documents was also carried out by sending a questionnaire to the company on March 25, 2021, to which the company replied on April 29, 2021.8. Two requests for additional information were sent to the company on July 13 and August 18, 2021. The company responded to them on July 30, August 31 and September 3, 2021.9. For the purposes of investigating this case, the President of the Commission appointed Mrs Valérie PEUGEOT as rapporteur, on May 19, 2022, on the basis of Article 39 of Decree No. 2019-536 of May 29, 2019 as amended. 10. On June 23, 2022, the rapporteur notified the company of a report detailing the breaches of the GDPR that she considered constituted in this case. This report proposed to the restricted formation of the Commission to impose an administrative fine with regard to the breaches constituted by Articles 7, paragraph 1, 12, 13, 14, 15, 21 and 32 of the GDPR and L. 34-5 of the Postal Code and electronic communications (hereinafter "the CPCE"). It also proposed that an injunction to bring the processing into compliance with the provisions of Articles 7, paragraph 1, 14 and 32 of the GDPR and L. 34-5 of the CPCE, accompanied by a penalty payment, be issued. Finally, he proposed that the sanction 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.11. On July 25, 2022, the company produced its observations in response to the sanction report.12. The rapporteur responded to the company's observations on August 11, 2022.13. On September 9, 2022, the company produced new observations in response to those of the rapporteur.14. By letter dated September 15, 2022, the

rapporteur informed the company's board that the investigation was closed, pursuant to Article 40, III, of amended decree no. 2019-536 of May 29, 2019.15. By letter of the same day, the company's board was informed that the file was on the agenda of the restricted meeting of October 13, 2022.16. The company and the rapporteur presented oral observations during the session of the restricted committee.II. Reasons for decisionA. On the breach of the obligation to obtain the consent of the persons concerned for the implementation of commercial prospecting by electronic means17. 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. […] ".18. 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 ".19. Under Article 7(1) of the GDPR, “In cases where processing is based on consent, the controller shall be able to demonstrate that the data subject has given consent to the processing of personal data. concerning her ".20. The rapporteur, to propose to the restricted committee to consider that the company has disregarded 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 EDF, which carries out commercial prospecting operations electronically, is not in a position to have and provide proof of a consent validly expressed by the prospects whose data comes from data brokers before being solicited. In addition, the rapporteur noted that, in the context of the investigation of three complaints, it appeared that the company had difficulties in obtaining from the data broker concerned evidence concerning the collection of consent: the data broker produced the standard form, and not the form completed individually by each prospect, thus not being able to provide individual proof of consent.21. In defence, the company argues that none of the three complaints referred to in the report concerns commercial prospecting operations by electronic means and therefore that Article L. 34-5 of the CPCE is inapplicable. The company adds that commercial prospecting operations by electronic means on the basis of data collected from data brokers are very specific and target an insignificant number of prospects ([…]%). In addition, the company indicates that it has always strictly framed its contractual relations with the data brokers it uses and that frequent exchanges took place, even if they were not necessarily

formalized in the form of audits. Finally, the company explains […] that the data already collected in the context of previous campaigns has been deleted. However, it adds that it has changed the contracts concluded with the data brokers and set up, from November 2021, formal audits.22. Firstly, the Restricted Committee recalls that, when the data of prospects has not been collected directly from them by the prospecting organization, consent may have been obtained at the time of the initial data collection by the primo - collecting, on behalf of the organization that will carry out subsequent prospecting operations. Failing this, it is up to the prospecting organization to obtain such consent before carrying out prospecting activities. With regard to the provisions of Article 7, paragraph 1, of the GDPR, the prospector must then be able to prove that he has this consent. In addition, for consent to be informed, individuals must in particular be clearly informed of the identity of the prospector on whose behalf the consent is collected and of the purposes for which the data will be used. To do this, an exhaustive and updated list must be made available to people at the time of obtaining their consent, for example directly on the collection medium or, if it is too long, via a hypertext link referring to said list and the privacy policies of service providers and suppliers.23. The Restricted Committee notes that the three complaints received by the CNIL and referred to by the rapporteur do not relate to electronic commercial prospecting operations. On the other hand, it notes that […] prospects were the subject of commercial prospecting by electronic means by the company EDF between 2020 and January 2021, for which EDF is not in a position to communicate documents demonstrating the obtaining of valid consent obtained from the persons.24. Moreover, while the company provided the delegation of control with two examples of the standard form for collecting data from prospects made available by the data broker […], the Restricted Committee notes that no list of partners - including EDF - which must be made available to prospects at the time of consent, has not been communicated in the context of the procedure, despite the rapporteur's requests to this effect.25. Secondly, the Restricted Committee notes that, in the context of the documentary check, the company indicated that the data brokers are in charge of collecting the consent of the persons concerned and that it asks them to undertake contractually to comply with the GDPR and the rules applicable to commercial prospecting. The company admitted that it did not exercise any control over the collection forms used, nor carried out audits on its co-contractors, but affirmed that it conducted informal exchanges with them.26. The Restricted Committee therefore considers that the measures put in place by EDF to ensure with its partners that the consent has been validly given by the prospects before being canvassed were insufficient.27. Under these conditions, the Restricted Committee considers that the company has disregarded 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.28. It nevertheless notes that, in the context of this procedure, the company indicated that it had deleted the data already collected in the context of previous campaigns.B. On the breach of the obligation to inform persons29. Article 13, paragraph 1, of the GDPR lists the information that must be communicated by the data controller to the data subjects when their personal data is collected directly from them, including "the purposes of the processing for which they are intended the personal data as well as the legal basis for the processing ".30. Paragraph 2 of the same article provides that "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 guarantee fair and transparent processing: (a) the retention period of the personal data or, where this is not possible, the criteria used to determine this period […]".31. Article 14 of the GDPR lists the information that must be communicated by the data controller to the data subjects when their personal data has not been collected from them. Paragraph 2 of the same article provides that "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 with regard to the data subject: […]f) the source from which the personal data originated and, where appropriate, a statement indicating whether or not they originated from publicly available sources […]".32. The guidelines on transparency within the meaning of Regulation (EU) 2016/679, adopted by the "article 29" working group in their revised version on 11 April 2018, clarifying the provisions of article 13, specify that: " the retention period […] should be formulated in such a way that the data subject can assess, depending on the situation in which he finds himself, what the retention period will be in the case of specific data or in the event of specific purposes. controller cannot simply state in a general way that personal data will be kept for as long as the legitimate purpose of the processing requires. Where appropriate, different storage periods should be mentioned for the different categories of data to be stored. personal character and/or the different processing purposes, in particular periods for archival purposes. They also specify that "the waiver of the obligation to provide the data subject with information about the source of his or her personal data only applies when such provision is not possible due to the impossibility of attributing different elements of personal data relating to the same individual to a particular source.In contrast, the mere fact that a database comprising the personal data of several data subjects has been compiled by a data controller using more of a source is not sufficient to waive this obligation if it is possible (although time-consuming or cumbersome) to determine the source from which the personal data of the data subjects originate" (paragraph 60).34. The rapporteur notes, on the one hand, a breach of Article 13 of the GDPR insofar as, at the time of the

online check carried out on February 15, 2021, the legal basis was not mentioned and the data retention periods were not developed in a sufficiently precise manner in the “personal data protection charter” appearing on the “particulier.edf.fr” sub-domain; it also notes a breach of Article 14 of the GDPR, insofar as the persons contacted by post by the company were not informed of the precise source of their personal data, namely the identity of the company from which EDF obtained them.35. In defence, the company considers that the "personal data protection charter" which appeared on the "particulier.edf.fr" website during the online check of February 15, 2021 contained all the information required under the Article 13 of the GDPR and guaranteed a "fair and transparent processing" of the data concerned. With regard to retention periods, the company notes that certain retention periods were mentioned, although not exhaustive because the company was carrying out, on the date of the online check, a major overhaul of retention periods. It considers that it was therefore not possible to indicate all the retention periods, since these were being reviewed and modified. Regarding the legal bases, the company indicates that Article 13, paragraph 1, c) of the GDPR does not require the data controller to indicate to the data subjects each legal basis for each purpose pursued, but simply that it informs of the legal bases used. It specifies that it has nevertheless undertaken a profound modification of the aforementioned charter, the update of which was published in April 2021 on the "particulier.edf.fr" website.36. With regard to the breach of Article 14, the company indicates that the nature of the source was at least referred to in the information notices brought to the attention of the persons concerned, namely an "organization specializing in the enrichment of data ". It adds that the fact of limiting itself to fairly general information on the origin of the data made it possible to avoid confusion by letting the data subject understand that he was only registered in the database of the data broker, while it was likely to appear simultaneously in several databases held by different data brokers. Finally, the company argues that there was no harm caused to persons who could contact EDF to obtain more information.37. Firstly, the Restricted Committee notes that the "personal data protection charter" present on the subdomain "particulier.edf.fr" constituted the information issued by the company under Article 13 of the GDPR for d other types of processing than prospecting (for example creation of a customer account or subscription to an online contract). However, the charter did not specify the legal basis corresponding to each purpose listed, an element nevertheless required by Article 13 of the GDPR.38. In addition, while the Restricted Committee takes note of the explanations provided by the company with regard to the overhaul of retention periods in progress at the time of the online observations made by the delegation of control, the fact remains that, at the At the time of these observations, the said charter specified "We only keep your data for the time necessary for their processing

according to the purpose that has been set", with an example relating to the retention periods for customers equipped with a Linky meter. The Restricted Committee considers that the information on retention periods was vague and imprecise, so that it was not sufficient to guarantee "fair and transparent processing" of the personal data processed.39. Therefore, the Restricted Committee considers that the company has failed to comply with its obligations resulting from Article 13 of the GDPR. It nevertheless takes note of the fact that the company has remedied this breach, since the legal bases and retention periods are now detailed in the charter mentioned above.40. Secondly, with regard to the breach of Article 14 of the GDPR, the Restricted Committee notes that, on the first prospecting letter sent to the complainants (requests No. […], No. […] and No. […]), whose data was obtained indirectly, the following statement appears: "EDF, data controller, is processing personal data for prospecting purposes […]. Your data has been collected from an organization specialized in data enrichment ".41. The Restricted Committee considers that the mere mention that the data was collected from an "organization specializing in data enrichment", appearing in the first commercial prospecting letter sent by EDF, is not sufficiently precise as to the source from which the data originates. This information is thus not likely to "guarantee fair and transparent treatment" with regard to the prospect, in particular in the context of successive resale of data between multiple actors and in the event that the prospect wishes to exercise his rights with the data broker whose identity he does not know.42. The Restricted Committee considers that the absence of significant harm for the persons invoked by the company and the possibility of contacting EDF in order to obtain more information has no influence on the characterization of the failure to inform the persons, which is a separate obligation from the right to obtain any available information as to the source of the data pursuant to Article 15(1)(g) GDPR.43. Therefore, the Restricted Committee considers that the aforementioned facts constitute a breach of Article 14 of the GDPR.44. The Restricted Committee notes that during the procedure, the company modified the information notices appearing in the prospecting letters, in order to include the name of the data broker concerned.C. On shortcomings in connection with the exercise of the rights of persons45. Under Article 12 of the GDPR: "1. The controller shall take appropriate measures […] to carry out any communication under Articles 15 to 22 and Article 34 in relation to the processing at the data subject in a concise, transparent, comprehensible and easily accessible manner, in clear and simple terms […] Information shall be provided in writing or by other means including, where appropriate, electronically. Where requested by the data subject, the information may be provided orally, provided that the identity of the data subject is demonstrated by other means […] 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 of receipt of the request. deadline 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 receiving the request. […] 4. If the controller does not respond to 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 from the reasons for its inaction and the possibility of lodging a complaint with a supervisory authority and bringing a judicial remedy. […] ".46. Article 15(1) of the GDPR provides the right for a person to obtain confirmation from the controller whether personal data relating to him or her are being processed and, where they are, access to personal data concerning him, in particular "g) when the personal data are not collected from the data subject, any information available as to their source". It is also provided for in paragraph 3 of the same article that "the controller provides a copy of the personal data undergoing processing. […] ".47. Article 21, paragraph 2, of the GDPR provides that, "Where personal data is processed for marketing purposes, the data subject has the right to object at any time to the processing. personal data concerning him for such prospecting purposes, including profiling insofar as it is linked to such prospecting. […] "1. On the breach of the obligation of transparency48. 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 12 of the GDPR, relies on two referrals to the CNIL, from Mr. […] (request No. […]) and Mr. […] (request No. […]) With regard to the first referral, the rapporteur noted that the company EDF had contacted the complainant by telephone to provide him with an answer, without writing to him, in violation of Article 12, paragraph 1, of the GDPR. was erroneous. Finally, the company answered his questions, again by telephone, more than nine months later. With regard to the second referral, the rapporteur noted that the company had closed the complainant's request instead of the send to the service in charge of requests for the exercise of rights and had not replied to Mr. […] It was only six months after his initial request – within the framework of the control procedure – that a response was received. brought to the complainant.49. In defence, the company indicates that EDF's policy has always been to respond in writing to all requests for the exercise of rights from its prospects and customers. It specifies that, for any written complaint, the adviser tries to contact the prospect or the client by telephone, before sending him a documented response in written form. The company adds that the absence of a written response to Mr […] is a simple human error committed by the adviser, who did not follow the internal procedures. The company adds that the processing of complainants' requests to exercise their rights took place in the particularly difficult context of both the health crisis, which led to an increase in the number of requests to exercise their rights,

and postponement of the end of the winter break to September 1, 2020, which may explain why their mail could not be properly processed within the usual deadlines.50. The Restricted Committee notes that the company recognizes an error in the orientation of the complainants' requests which resulted in "either a lack of response within the time limit, or a poor quality of response". A breach of the obligations of Article 12 of the GDPR is constituted when the company has not provided a written response and has given the complainant erroneous information regarding the referral of Mr […]. Furthermore, the company did not deal with these requests to exercise rights within the time limit set for the two referrals.51. Consequently, the Restricted Committee considers that the breach of Article 12 of the GDPR has been established.2. On the breach of the obligation to respect the right of access52. The rapporteur, to propose to the Restricted Committee to consider that the company has disregarded its obligations resulting from Article 15 of the GDPR in terms of right of access, relies on two referrals to the CNIL, from Mr. (referral no. […]) and Mrs (referral No. […]). Regarding the referral to Mr […], the first answer given by telephone to the complainant on the source of the data collected was incorrect. As for the referral of Mrs. […], the company specifies that a response was sent to her on July 17, 2020, indicating to her that she had no other data concerning her than her first and last name in its databases. . The rapporteur considered that such an assertion was inaccurate and that the company had at least her address – or former address – to make the connection with the complainant's first and last name since the company EDF sent her a letter to the home of her parents.53. In defence, with regard to the referral relating to Mr […], the company acknowledges that the adviser's response to the complainant was "partly inaccurate" due to an error in the source of the data. As for the referral relating to Mrs […], the company considers that the response given to it by the adviser was correct since the only data relating to the complainant were her surname and first name.54. In view of the information provided by the company, the rapporteur proposes to the Restricted Committee not to uphold the breach of Article 15 of the GDPR with regard to the referral relating to Ms […].55. The Restricted Committee notes that the facts noted by the rapporteur are not disputed by the company with regard to the referral of Mr […] and that it has been proven that an inaccurate answer was given to him in the context of his request right of access. She considers that a breach of the obligations of Article 15 is constituted with regard to this complaint, since the company provided her with erroneous information on the source of the data collected as part of her request for right of access. . On the other hand, with regard to Mrs. […]'s complaint, the Restricted Committee takes note of the elements provided by the company and considers that the breach invoked is not characterized.3. On the breach of the obligation to respect the right of opposition56. The rapporteur, to propose to the Restricted Committee to consider that the

company has failed to comply with its obligations resulting from Article 21 of the GDPR, relies on the referral from Mr. […] (no. […]). The rapporteur indicates that the company did not take into account the complainant's opposition to the processing of the personal data of his minor son for the purposes of commercial prospecting. In fact, the minor son of Mr […] received a second commercial prospecting letter, despite the latter's request for the deletion of personal data relating to his son.57. In defense, the company explains that, in the "Complaint" guide of May 2020 intended for all advisers, the latter were instructed, for any request to erase a prospect's data, to "systematically collect the 'prospect opposition'. Concerning the referral of Mr. […], the adviser proceeded to erase the data as he had indicated to the complainant by telephone but did not completely follow the internal procedure by not proceeding with the opposition before erase data. The company adds that it has simplified this deletion procedure. Thus, since July 2021, when the adviser processes a deletion request, an opposition is automatically implemented.58. The Restricted Committee notes that the facts noted by the rapporteur with regard to the complainant's situation are not disputed by the company and constitute a breach of the obligations arising from Article 21 of the GDPR. It notes that during the sanction procedure, the company improved its procedure for managing requests for erasure.D. On the breach of the obligation to ensure data security59. 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 the password hash function of the "prime energy" portal 60. Given the company's initial statements during the inspection procedure, the rapporteur noted that the passwords to the customer area of the "prime energy" portal were stored using the MD5 hash function. The rapporteur then noted the company's new claims and the fact that since January 2018 the SHA-256 hash function has been used. However, she noted that, until July 2022, the passwords of more than 25,800 accounts were stored insecurely, with the MD5.61 hash function. In defence, the company explains that, since January 2018, all registrations or changes to a user password are recorded in the directory associated with the "prime energy" portal in SHA-256 with an associated random mechanism (salting). The MD5 hash only corresponds to the hash level historically implemented by the company […] , an

EDF subcontractor, and for which only a few thousand accounts were still concerned in April 2021. The company adds that these passwords were still stored with the robustness of the additional randomization (salting) mechanism, preventing attacks by precomputed tables. She concludes that the passwords were secure. In addition, the company indicates that, since the beginning of 2022, a final purge of passwords that were still stored by means of the MD5 hash function (approximately 3.2% of the total number of "prime energy" customers ") was realized. It thus specifies that all the passwords of users of the "prime energy" site are now stored with salt and a strong algorithm.62. The Restricted Committee recalls that 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. Thus, it is necessary to ensure that a password allowing authentication on a system cannot be disclosed. Storing passwords in a secure manner is an elementary precaution in the protection of personal data. As early as 2013, the National Information Systems Security Agency (ANSSI) alerted and recalled good practices regarding the storage of passwords, indicating that they must "be stored in a form transformed by a function one-way cryptographic (hash function) and slow to calculate such as PBKDF2" and that "the transformation of passwords must involve a random salt to prevent an attack by precomputed tables". Indeed, non-robust hash functions have known vulnerabilities that do not guarantee the integrity and confidentiality of passwords in the event of a brute force attack after the servers that host them have been compromised. Insofar as a large number of Internet users use the same password to authenticate themselves to their various online accounts, attackers could exploit the compromised data to multiply the intrusions on their other accounts to commit, for example, theft or scams.63. Similarly, the Commission also specifies in its deliberation no. 2017-012 of January 19, 2017, with regard to storage methods, that "the password must never be stored in clear text. It recommends that it be transformed into means of a non-reversible and secure cryptographic function (i.e. using a public algorithm known to be strong whose software implementation is free of known vulnerabilities), incorporating the use of a salt or a key The Commission further considers that the salt or key must be generated by means of a cryptographically secure pseudo-random number generator (i.e. based on a public algorithm known to be strong whose software implementation is free of known vulnerabilities), and not be stored in the same storage space as the ".64 password

verification item. In addition to these recommendations, the Restricted Committee stresses that it has, on several occasions, adopted financial penalties where the characterization of a breach of Article 32 of the GDPR is the result of insufficient measures to guarantee the security of the data processed. She thus had the opportunity to recall that "the use of the MD5 hash function by the company is no longer considered since 2004 as state-of-the-art and its use in cryptography or security is prohibited. Thus , the use of this algorithm would allow a person having knowledge of the hashed password to decipher it without difficulty in a very short time (for example, by means of freely accessible Internet sites which make it possible to find the value corresponding to the hash password)" (deliberation SAN-2021-008 of June 14, 2021).65. However, the Restricted Committee notes that, until July 2022, the passwords of more than 25,800 accounts were stored insecurely, with the MD5 hash function. Under these conditions, given the risks incurred by individuals, the Restricted Committee considers that the company has failed to fulfill its obligations under Article 32 of the GDPR.66. It nevertheless 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. On the password hash function in the EDF67 customer area. Given the company's initial statements during the inspection procedure, the rapporteur noted that the passwords to the EDF customer space, accessible at the URL "www.particuliers.edf.fr", were stored in the form chopped and salted using the SHA-1 function, which is deemed obsolete. It therefore considered that the methods of storing passwords did not make it possible to guarantee the security and confidentiality of customers' personal data.68. In defence, the company indicates that the hashing algorithm used to store passwords in the directory […], which manages the authentication of customer spaces, is in fact SHA-512 supplemented by a mechanism for adding of hazard (salting) since May 17, 2017, and not SHA-1, contrary to what it had been able to indicate to the control delegation. The company adds that the renewal of passwords and the purging of old passwords were carried out gradually.69. In the latest form of her pleadings, the rapporteur notes that, while 11,241,166 account passwords are indeed hashed and salted, 2,414,254 account passwords are hashed only, without having been salted.70. In defense, the company recalls that it deploys significant resources, both human and material, in terms of cybersecurity. It adds that, since its last observations, the company has implemented the mechanism of adding randomness (salting) to the fraction of passwords in the directory […] which did not have it, but which were however already hashed with SHA-512. Thus, to date, there is no longer any hashed password in SHA-512 without a mechanism for adding randomness (salting).71. Restricted formation refers to the developments above regarding the need to involve a random salt for the transformation of passwords (§§ 62 and 63). It also notes that, in its guide

"Recommendations relating to multi-factor authentication and passwords" of October 8, 2021, the ANSSI writes: "It is recommended to use a salt chosen randomly for each account and to a length of at least 128 ".72 bits. The Restricted Committee notes that, here again, the company does not contest the breach in itself but asks not to be penalized insofar as it has now remedied the breach. The Restricted Committee considers that the company has breached its obligations under Article 32 of the GDPR, since it has not taken the necessary measures to ensure the security of all the data it processes. and which are accessible from user accounts at the URL "www.particuliers.edf.fr", without systematically using a salt in the transformation of passwords.73. It nevertheless 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.III. On corrective measures and their publicity74. Under the terms of article 20, III, of the amended 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 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. assumptions 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 ".75. Article 83 of the GDPR provides that "each supervisory authority ensures that the fines administrative measures 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 elements to be taken into account to decide whether there instead of imposing an administrative fine and to decide on the amount of this fine.76 Firstly, on the principle of imposing a sanction, the company indicates that, in addition to the fact that it contests the breaches of which the rapporteur or justifies them, it has already taken all measures to remedy all of the alleged facts and ensure its compliance with the applicable legislation. It emphasizes the goodwill and efforts it has demonstrated throughout along the procedure. The company considers that the mitigating factors posed by Article 83, paragraph 2, of the GDPR should lead the restricted committee not to impose a financial penalty or at the very least to very significantly reduce the amount of the

fine proposed by the reporter. It considers that the alleged breaches are not substantial in the present case, since they represented a limited or even non-existent impact on the rights and freedoms of the persons concerned, given their small number and their non-structural nature.77. The Restricted Committee recalls that it must take into account, for the pronouncement of an administrative fine, the criteria specified in Article 83 of the GDPR, such as the nature, gravity and duration of the violation, the measures taken by the controller to mitigate the damage suffered by data subjects, the degree of cooperation with the supervisory authority and the categories of personal data affected by the breach.78. The Restricted Committee emphasizes that the breaches committed by the company relate to obligations relating to the fundamental principles of the protection of personal data and that numerous breaches have been established.79. The Restricted Committee then notes that the company is the leading player in electricity in France, since it counted, at the end of December 2020, 25.7 million customers for the supply of electricity, gas and services and approximately […] prospects, with regard to the individual market. It therefore has significant resources enabling it to deal with questions of protection of personal data.80. Consequently, the Restricted Committee considers that an administrative fine should be imposed with regard to the breaches of Article L. 34-5 of the CPCE and Articles 7, paragraph 1, 12, 13, 14, 15, 21 and 32 of the GDPR.81. The Restricted Committee nevertheless underlines the efforts that EDF has made in the context of the procedure, since it has brought itself into compliance with regard to all the breaches noted by the rapporteur. It also considers that the breach of the obligation to obtain the consent of the persons concerned for the implementation of commercial prospecting by electronic means, although being a structural breach, is in this case of limited seriousness in the given that the number of prospects whose data has been collected from data brokers and who have received commercial prospecting by electronic means represents only […]% over the period 2020-2022 of all the people targeted by actions commercial prospecting carried out by EDF with prospects whose data was obtained via data brokers. With regard to the breach of the obligation to inform, the Restricted Committee takes note of the company's declarations, according to which it was carrying out a major overhaul of the retention periods, thus preventing it from indicating them all since they were in course of review and modification. It also notes, with regard to the referrals made to the proceedings, that the breaches of the rights of individuals are not structural and are the result of human error.82. The Restricted Committee recalls that the breaches of the GDPR identified in this case are breaches of principles liable to be subject, under Article 83 of the GDPR, to an administrative fine of up to 20 000,000 euros or up to 4% of the worldwide annual turnover of the preceding financial year, whichever is higher.83. The Restricted Committee also recalls that administrative fines

must be both dissuasive and proportionate. It considers in particular that the activity of the company and its financial situation must in particular be taken into account for the determination of the amount of the administrative fine. It notes in this respect that the EDF group achieved a turnover of more than 69 billion euros for a net result of […] euros in 2020 and of more than 84 billion euros for a net result of […] euros in 2021.84. Therefore, in the light of these elements, the Restricted Committee considers that the imposition of an administrative fine in the amount of 600,000 euros appears justified.85. Secondly, an injunction to bring the processing into compliance with the provisions of Articles 7, paragraph 1, 14 and 32 of the GDPR and L. 34-5 of the CPCE was initially proposed by the rapporteur.86. The company maintains that the actions it has taken with regard to all of the breaches identified should lead to no injunction being issued under penalty.87. As indicated above, the Restricted Committee notes that the company has taken compliance measures with regard to all the breaches noted by the rapporteur. It therefore considers that there is no need to issue an injunction.88. Thirdly, with regard to the publication of the sanction decision, the company asks the restricted committee not to publish it or, in the alternative, to anonymize it immediately or at the latest within eight days. 89. The Restricted Committee considers that the publication of the sanction is justified in view of the nature and number of breaches committed, as well as the number of persons concerned by the said breaches, in particular more than 2,400,000 customers with regard to the breach of data security.FOR THESE REASONSThe Restricted Committee of the CNIL, after having deliberated, decides to: pronounce against the company ÉLECTRICITÉ DE FRANCE an administrative fine in the amount of 600,000 (six hundred thousand) euros for the breaches of Article L. 34-5 of the CPCE and Articles 7, paragraph 1, 12, 13, 14, 15, 21 and 32 of the GDPR; 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 may be subject to appeal before the Council of State in a period of two months from its notification.