Deliberation SAN-2020-014 of December 7, 2020 National Commission for Computing and Liberties Nature of the deliberation: Sanction Legal status: In force Date of publication on Légifrance: Thursday December 17, 2020 Deliberation of the restricted committee no SAN-2020-014 of December 7 2020 concerning Mr [...] By a decision of July 22, 2022, the Council of State reformed the deliberation of the restricted formation by reducing the amount of the sanction from 3,000 euros to 2,500 euros in consideration of the absence obligation to notify the CNIL of the data breach with regard to the information already available to the CNIL and which had enabled it to initiate a check. Consult decision no. 449694.The National Commission for Computing and Liberties, meeting in its restricted formation composed of Messrs Alexandre LINDEN, president, Philippe-Pierre CABOURDIN, vice-president, and Mesdames Dominique CASTERA, Anne DEBET and Christine MAUGÜE, members; Having regard to Convention No. 108 of the Council of Europe of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data; Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 relating to the protection of personal data and the free movement of such data; Having regard to law no. 78-17 of January 6, 1978 relating to data processing, files and freedoms, in particular its articles 20 and following; Having regard to decree no. 2019-536 of May 29, 2019 taken for the application of law no. 78-17 of January 6, 1978 relating to data processing, files and freedoms; Having regard to deliberation no. 2013-175 of 4 July 2013 adopting on the rules of procedure of the National Commission for Computing and Liberties; Having regard to decision no. to carry out a mission to verify the processing, in particular accessible from the IP address bearing the number [...]; Having regard to the decision of the President of the National Commission for Computing and Liberties appointing a rapporteur before the Restricted Committee, dated July 27, 2020; Having regard to the report of Mr. François PELLEGRINI, reporting commissioner, notified to Mr [...] on September 23, 2020; Having regard to the oral observations made during the meeting of the Restricted Committee; Having regard to the other documents in the file; Were present at the restricted committee meeting of December 3, 2020: Mr. François PELLEGRINI, commissioner, heard in his report; As the representative of e Mr [...]:[...];Counsel for Mr [...] having spoken last;The Restricted Committee adopted the following decision:I.Facts and procedureMr. [...] exercises a liberal activity [...] in Paris [...]. On […], the website […], reported free access to medical imaging computer servers located […] allowing consultation and downloading […] of medical images (MRIs, x-rays, scanners, etc…) followed in particular by the surname, first names, date of birth and date of consultation of the patients. Pursuant to decision no. -after the CNIL or the Commission), the CNIL services carried out an online check, on September 20 and 24, 2019, which confirmed the freely

accessible nature of this data, which can be used via simple software consultation of medical images. The control also made it possible to draw up a list of the IP addresses of these servers which are located in France. The purpose of this control was in particular to verify compliance, by the recipients of these IP addresses, with all the provisions of the regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (hereinafter the Regulation or the RGPD) and of the amended law no. 78-17 of January 6, 1978 relating to data processing, files and freedoms (hereinafter the Data Protection Act). After having asked the various Internet access providers to provide them with the identity and contact details of the data controllers using these French IP addresses, the CNIL services were informed that one of these addresses, bearing the number [...], was awarded Mr [...]. By e-mail dated October 8, 2019, the control delegation notified the online control to Mr. [...], after having informed him of the freely accessible nature of the medical images of his patients from the IP address from its server. By email of October 9, Mr. [...] replied that he had taken the necessary measures to put an end to the violation. On December 6, 2019, Mr. [...] was heard by the delegation of control in the premises of the CNIL. He indicated that in order to be able to remotely access the medical images hosted on the hard disk of the fixed computer at home, he opened the ports of the LiveBox used at his home by activating the latter's DMZ mode, in the purpose of making the VPN work. For the purpose of examining these elements, the President of the Commission appointed Mr François PELLEGRINI as rapporteur, on July 27, 2020, on the basis of Article 22 of the Data Protection Act. At the end of his investigation, the rapporteur had a report personally delivered to Mr [...], on September 23, 2020, detailing the breaches of the GDPR that he considered constituted in this case. On the same day, the CNIL services notified it of a summons to the restricted training session of December 3, 2020. This report proposed that the restricted training of the Commission impose an administrative fine on Mr. [. ..] for breaches of Articles 32 and 33 of the Rules. On November 20, 2020, Mr. [...] requested, through his counsel, the postponement of the restricted committee meeting. This request was rejected on November 26, 2020 by the chairman of the Restricted Committee.Counsel for Mr [...] and the rapporteur presented oral observations during the Restricted Committee meeting.II.Reasons for the decisionA .On the breach of the obligation to ensure the security of the data processed14. Pursuant to Article 32(1) of the GDPR, the controller implements appropriate technical and organizational measures to ensure a level of security appropriate to the risk .15. Paragraphs a) and b) of this same paragraph 1 provide that, depending in particular on the scope, context and purposes of the processing as well as the risks for the persons concerned, the data controller implements the encryption of personal data. personnel and the means to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and

services .16. The rapporteur argues that the vulnerability of the medical imaging device at the origin of the data breach is attributable to Mr. […] who did not implement the appropriate technical measures to guarantee the security of the processing .17. Counsel for Mr. […] replies that his client had no intention of allowing free access to these medical images and that the violation is only the unfortunate consequence of the connection to his Internet box of the external hard drive plugged in on his home computer.18. The Restricted Committee notes that pursuant to Article 32 of the GDPR, it was the responsibility of Mr [...], as data controller, to ensure the security of the data he processed in the context of his professional activity.19. First of all, the Restricted Committee points out that it is not disputed that the data breach was caused by the opening of the network ports of the Internet box used at Mr. [...]'s home coupled with the configuration of the server function of the imaging software [...] .20. She notes that in her email of December 9, 2019, Mr [...] stated: it happens that this software [the imaging software [...]] includes a server function, that the mac is behind a LiveBox connected to the Internet and that (…) I think that the port of 11112 of the LiveBox is open to all winds. In addition, during his hearing on December 6, 2019, the latter specified that he had not used a service provider for the installation and configuration of the software [...] and that he himself had opened the ports of the LiveBox used at his home (…) for the purpose of running the .21 VPN. It therefore appears from these elements that Mr [...] had not taken care to limit the network functions to those which were strictly necessary for the operation of the processing.22. However, the Restricted Committee emphasizes that the protection of the internal computer network and the encryption of personal data are part of the basic requirements in terms of computer security, which are incumbent on any data controller.23. In this regard, in the guide The security of personal data , which offers useful information to data controllers as to the measures to be implemented in order to guarantee the security of their processing, the Commission recommends authorizing only the network functions necessary for the treatments implemented. Similarly, the Practical Guide for Physicians, published by the CNIL in consultation with the National Council of the Order of Physicians, invites physicians to limit as much as possible the connection of non-professional devices to the network within which patient data, as well as to use strong authentication means to access this network.24. Next, the Restricted Committee points out that it also emerges from the hearing of December 6, 2019 that Mr [...] had also not taken care to encrypt the data contained in his three laptops and in his desktop computer .25. However, in the absence of encryption, the medical data contained in the hard disk of these computers could be read in clear text by any person taking possession of these devices (for example, following their loss or theft) or by any person improperly intruding on the network to which these devices were connected.26. In this regard, in its guide The

security of personal data, the CNIL recommends providing means of encryption for mobile workstations and mobile storage media (laptop, USB keys, external hard drive, CD-R, DVD-RW, etc. .), for example via encryption of the entire hard disk when the operating system offers it, encryption file by file or the creation of containers (file likely to contain several files) encrypted. Similarly, the Practical Guide for Physicians invites physicians to encrypt their patients' data with suitable software.27. Finally, the Restricted Committee notes that the processing in question concerns medical data, which constitute special categories of personal data, within the meaning of Article 9 of the Regulation. The nature of this information therefore called for particular vigilance in order to avoid a data breach.28. The Restricted Committee thus recalls that among the data concerned by the violation, there were, in addition to the medical images, the surname, first names and date of birth of the patient, the date of the examination, the name of the referring practitioner and the practitioner having carried out the examination and the name of the establishment in which it took place.29. It points out that it appears from Mr [...]'s own statements in the context of his hearing of 6 December 2019 that more than five thousand three hundred sets of medical images are concerned.30. Lastly, it notes that the file shows that those data were exposed for approximately four months.31. In view of all of these elements, the Restricted Committee considers that a breach of Article 32 of the GDPR has been constituted. B. On the breach of the obligation to notify the data breach to the CNIL32. Pursuant to Article 33(1) of the GDPR, in the event of a personal data breach, the controller shall notify the breach in question to the competent supervisory authority in accordance with Article 55, within as soon as possible and, if possible, 72 hours at the latest after becoming aware of it .33. The rapporteur argues that Mr [...] did not report the data breach to the relevant Commission services.34. Mr [...] replies that the need to notify the data breach to the Commission was never indicated to him. He also invokes the artificial nature of such an obligation when he became aware of the free access to his medical imaging server by the CNIL's delegation of control.35. The Restricted Committee considers that the data controller must comply with the notification requirement provided for in Article 33 of the Regulation unless the violation in question is not likely to create a risk for the rights and freedoms of natural persons. The fact that the data breach had been brought to the attention of Mr [...] by the CNIL's control department did not relieve him of this obligation.36. Indeed, following the control, the data controller may become aware of additional elements relating to the data breach which deserve to be communicated to the competent services of the CNIL, which are responsible in particular for centralizing the various data breaches and to ensure follow-up in order to prevent the compromise of personal data. A teleservice is available on the CNIL website to make these notifications.37. In the present case, the Restricted Committee

recalls that the existence and nature of the notification obligation appeared in the email of October 8, 2019 which informed Mr [...] of the said data breach.38. The Restricted Committee therefore considers that a breach of Article 33 of the Rules has been established.III.On corrective measures and publicity39. Under the terms of III of article 20 of the Data Protection Act: 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 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, the restricted formation of the commission with a view to pronouncing, after contradictory procedure, one or more of the following measures: […] 7° With the exception of cases where the processing is implemented by the State, a 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. In the cases mentioned in 5 and 6 of Article 83 of Regulation (EU) 2016/679 of April 27, 2016, these ceilings are increased, respectively, to 20 million euros and 4% of said turnover. The Restricted Committee takes into account, in determining the amount of the fine, the criteria specified in the same Article 83. 40. Article 83 of the GDPR provides:1. Each supervisory authority shall ensure that administrative fines imposed under this Article for breaches of this Regulation referred to in paragraphs 4, 5 and 6 are, in each case, effective, proportionate and dissuasive.2. Depending on the specific characteristics of each case, administrative fines are imposed in addition to or instead of the measures referred to in points (a) to (h) and (j) of Article 58(2). In deciding whether to impose an administrative fine and in deciding the amount of the administrative fine, due account shall be taken in each individual case of the following elements: (a) the nature, gravity and the duration of the breach, taking into account the nature, scope or purpose of the processing concerned, as well as the number of data subjects affected and the level of damage they have suffered; b) the fact that the breach has was committed willfully or negligently; c) any action taken by the controller or processor to mitigate the harm suffered by data subjects; d) the degree of liability of the controller or processor, taking into account the technical and organizational measures they have implemented pursuant to Articles 25 and 32; e) any relevant breach previously committed by the controller or processor; f) the degree of cooperation established with the control in with a view to remedying the breach and mitigating its possible negative effects; g) the categories of personal data concerned by the breach; h) the manner in which the supervisory authority became aware of the breach, in particular if, and to what extent the controller or processor notified the breach; (i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned processor for the same purpose,

compliance with these measures; j) the application of codes of conduct approved pursuant to Article 40 or certification mechanisms approved pursuant to Article 42; and (k) any other aggravating or mitigating circumstance applicable to the circumstances of the case, such as financial benefits obtained or losses avoided, directly or indirectly, as a result of the breach.41. Concerning the imposition of an administrative fine, counsel for Mr [...] considers in particular that the corrective measure proposed by the rapporteur is disproportionate in view of his responsibility for the data breach and that the imposition of a reminder to the order would be more justified.42. He also claims to have reacted very quickly to put an end to the violation, as soon as he learned of it from the delegation, and asserts his full cooperation with the Commission services.43. The Restricted Committee recalls that in order to assess the appropriateness of imposing an administrative fine, reference should be made to the relevant criteria specified in Article 83, paragraph 2, of the GDPR.44. In the present case, it considers that it is appropriate first to apply the criterion provided for in subparagraph f) of Article 83, paragraph 2, of the Regulation relating to the degree of cooperation established with the supervisory authority in with a view to remedying the violation and mitigating its possible negative effects.45. The Restricted Committee notes that as soon as he became aware of the violation, Mr [...] immediately took the necessary measures to put an end to it immediately.46. It thus recalls that in its email of October 9, 2019 in response to the delegation of control, Mr. [...] indicated that it had deactivated the server function of the software and blocked the non-useful ports on the Livebox .47. However, the Restricted Committee stresses that the criteria provided for in subparagraphs a) and g) of Article 83(2) of the Rules should also be applied, relating, on the one hand, to the nature, seriousness and duration of the breach, taking into account the nature, scope or purpose of the processing concerned, as well as the number of data subjects affected and, on the other hand, the categories of personal data concerned by the breach.48. It thus notes that Mr […] failed in two elementary principles in terms of computer security, namely the protection of the internal computer network by limiting network flows to what is strictly necessary and the encryption of personal data.49 . The Restricted Committee emphasizes once again that the seriousness of the breach of Article 32 of the GDPR is all the more pronounced in that health data is concerned and that this particular category of personal data must benefit from reinforced security measures, in accordance with in recital 75 of the GDPR.50. It repeats that failure to comply with these elementary practices had the direct consequence of making more than five thousand three hundred series of health images accessible, including, for each of these series, in addition to the medical image, the surnames, first names and date of birth of each patient, the date of the examination, the name of the referring practitioner and of the practitioner who carried out the

examination and the name of the establishment in which it took place.51. It points out that the personal data stored on the hard disk of the fixed computer at Mr. [...]'s home remained accessible without any authentication for a period of approximately four months.52. Finally, the Restricted Committee emphasizes that the criterion provided for in subparagraph h) of Article 83, paragraph 2 of the Regulation relating to the manner in which the supervisory authority became aware of the breach should also be applied, in particular whether, and to what extent, the controller notified the breach.53. She recalls in this case that the Commission became aware of the data breach through a press article and that Mr [...] never notified it to the competent services of the Commission, even after that the delegation of control drew its attention to this point.54. In view of these elements, the Restricted Committee considers it necessary to impose an administrative fine on Mr [...].55. Regarding the determination of the amount of this fine, the Restricted Committee considers that the breach of Article 32 of the GDPR is of certain seriousness, that on the other hand the breach of Article 33 in this case is of a formal nature.56. It notes that according to the statements of its counsel during the meeting of December 3, 2020, Mr [...] received €97,000 in income in 2018 and that, pursuant to the provisions of Article 83, paragraph 4, of the GDPR, he incurs a financial penalty of a maximum amount of 10 million euros.57. Therefore, with regard to the financial capacity of Mr [...] and the relevant criteria of Article 83, paragraph 2, of the Rules, the Restricted Committee considers that the imposition of a fine of €3,000 appears times effective, proportionate and dissuasive, in accordance with the requirements of Article 83, paragraph 1, of this Regulation. ..] an administrative fine in the amount of €3,000 (three thousand euros) for breaches of Articles 32 and 33 of the GDPR; make this decision public on the CNIL website and on the Légifrance website without identifying the person responsible of treatment.The presidentAlexandre LINDENThis decision may be subject to appeal before the Council of State within two months of its notification.