Deliberation of the restricted committee no SAN-2020-015 of December 7, 2020 concerning Mr […]

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 27 April 2016 relating to the protection of personal data and the free movement of such data;

Considering the law n ° 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 July 4, 2013 adopting the internal regulations of the National Commission for Computing and Liberties;

Having regard to decision no . 2019-152C of September 20, 2019 of the President of the National Commission for Computing and Liberties to instruct the Secretary General to carry out or to have carried out a mission to verify the processing operations, 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 Freedoms appointing a rapporteur before the restricted formation, dated July 27, 2020;

Having regard to the report of Mr François PELLEGRINI, reporting commissioner, notified [...] on September 23, 2020;

Having regard to the written observations submitted by counsel for Mr [...] on October 22, 2020;

Having regard to the oral observations made during the session of the Restricted Committee;

Having regard to the other documents in the file;

Were present at the restricted training session of December 3, 2020:

Mr. François PELLEGRINI, commissioner, heard in his report;

As a representative of Mr [...]:

Master […] ;

Mr. […], data protection officer and computer specialist, was heard pursuant to Article 22, paragraph 1, of Law No. 78-17 of 6 January 1978 as amended relating to data processing, files and freedoms;

Mr. [...] having spoken last;

The Restricted Committee adopted the following decision:

I.Facts and procedure

Mr […] is a self-employed person in a firm […] in Paris […].

On […], an investigation by the computer security company […], relayed by the […] website, reported free access to medical imaging computer servers located […] allowing consultation and downloading […] of medical images (MRI, 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. 2019-152C of September 20, 2019 of the President of the National Commission for Computing and Liberties (hereinafter the CNIL or the Commission), the CNIL services carried out an inspection in line, on September 20 and 24, 2019, which confirmed the freely accessible nature of this data, which can be used via a simple medical image consultation software. The control also made it possible to establish the list of IP addresses of these servers which are located in France.

The purpose of these missions was in particular to verify compliance, by the recipients of these IP addresses, with all the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the Regulation or the RGPD) and the modified law n° 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 of October 2, 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 his server.

By e-mail of the same day, Mr [...] replied that he had taken the necessary measures to put an end to the violation.

On December 17, 2019, Mr. [...], assisted by his counsel, was interviewed by the supervisory delegation on the premises of the CNIL. He indicated that, in 2015, he configured his imaging software [...] to be able to automatically transfer images from his

X-ray equipment to the database of his imaging software hosted in his office and access remotely to pictures.

By letter dated January 7, 2020, Mr. [...] sent the delegation of control several documents requested in the context of his hearing, such as the volumetrics of the images contained in the database of the medical imaging software as well as the registers of the processing of personal data implemented in his office.

By letter dated January 20, 2020, Mr [...] sent the delegation of control documents reporting on the strengthening of the security measures taken to the medical imaging system of his office.

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 the latter of a summons to the restricted training session of December 3, 2020.

This report proposed that the restricted committee of the Commission impose an administrative fine on Mr. […] for breaches of Articles 32 and 33 of the Rules.

On October 22, 2020, through his counsel, Mr. […] submitted observations and made a request that the session before the Restricted Committee be held behind closed doors.

On October 29, 2020, the President of the Restricted Committee granted this request on the grounds that the personal data entered into the debate were protected by medical secrecy.

Mr [...] and the rapporteur presented oral observations during the restricted session.

II. Reasons for the decision

A. On the breach of the obligation to ensure the security of the data processed

17. 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 .

18. 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 the data . of a personal nature and the means to guarantee the constant confidentiality, integrity, availability and resilience of the processing systems and services .

19. 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 treatment.

20. Mr [...] responds in particular that he is not the cause of the data breach since the configuration of the Internet box, which serves as a router for his professional computer equipment, was, according to him, carried out by service providers outside the firm. However, he acknowledges that he is not in a position to prove the materiality of these interventions, as he has not kept any records.

21. The Restricted Committee notes that pursuant to Article 32 of the GDPR, it was Mr. […] who, as data controller, was responsible for ensuring the security of the data that he dealt, the determination of the author of the setting of the Internet box being inoperative in this case.

22. First of all, the Restricted Committee emphasizes that it is undisputed that the data breach was caused by the opening of the network ports of the Internet box used in Mr. [...]'s office coupled with the configuration of the server function (PACS) of the imaging software [...].

23. She notes that in her email of October 2, 2019, Mr [...] indicated: I do not use a PACS in the firm because we directly view the images taken on the secure Ethernet network. In addition, during his hearing on December 17, 2019, he specified that he had implemented remote access to images in 2015 and had not used a service provider for the installation and configuration of the software [...] . It therefore emerges 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.

24. 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. 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 methods to access this network.

25. Next, the Restricted Committee points out that it also emerges from the hearing of 17 December 2019 that Mr [...] had not

taken care to encrypt the data contained in his personal laptop either, considering that encryption slows down the execution of applications too much (medical records, image viewing tool) .

26. However, in the absence of encryption, the medical data contained in the hard disk of this computer could be read in plain text by anyone taking possession of this device (for example, following its loss or theft) or by anyone trespassing on the network to which this computer was connected.

27. In this regard, in its guide The security of personal data, the CNIL recommends providing means of encryption for mobile computers and mobile storage media (laptop, USB keys, external hard drive, CD-R, DVD-RW , etc.), for example via the 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 patient data with suitable software.

28. 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.

29. It thus recalls that among the data concerned by the breach included, in addition to the medical image, the surname, first names and date of birth of the patient, the date on which the examination was carried out, the name of the referring practitioner and the practitioner having performed the examination and the name of the institution where the examination took place.

30. It points out that it appears from Mr [...]'s own statements in the context of his hearing of 17 December 2019 that more than one thousand two hundred sets of medical images are concerned.

31. Lastly, it notes that it is apparent from the file that these data were exposed for approximately five years.

32. 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 CNIL

33. 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, as soon as possible and, if possible, 72 hours at the latest after becoming aware of it.

34. The rapporteur argues that Mr […] did not report the data breach to the relevant Commission services.

35. 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 since he was aware of the free access to the database of his medical imaging software by the CNIL's delegation of control.

36. The Restricted Committee considers that the data controller must, in all circumstances, 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 Mr. [...]'s attention by the CNIL's control department did not relieve him of this obligation.

37. 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. data and to monitor it in order to prevent the compromise of personal data. A teleservice is available on the CNIL website to make these notifications.

38. In the present case, the Restricted Committee recalls that the existence and nature of the notification obligation appeared in the email of October 2, 2019 which informed Mr. [...] of the said data breach.

39. The Restricted Committee notes that on 24 September 2020, the day of the notification of the sanction report, Mr [...] had still not notified the data breach to the Commission, although he was aware of it since October 2, 2019.

40. The Restricted Committee therefore considers that a violation of Article 33 of the Rules has been constituted.

III. On corrective measures and publicity

41. Under 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 27 April 2016 or from this law, the President of the National Commission for Computing and Liberties may also, if necessary, after having sent it 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 exceeding 10 million euros or, in the case of a company, 2% of the annual worldwide turnover total for the previous 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.

42. 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 shall be 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:

a) the nature, gravity 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 the level of damage they have suffered;

b) whether the breach was committed willfully or negligently;

c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

d) the degree of responsibility 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 supervisory authority with a view to remedying the breach and mitigating its possible negative effects;

g) the categories of personal data affected by the breach;

h) how the supervisory authority became aware of the breach, including whether 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 for the same purpose, compliance with those 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 circumstances applicable to the circumstances of the case, such as the financial advantages obtained or the losses avoided, directly or indirectly, as a result of the violation.

43. Concerning the imposition of an administrative fine , Mr [...] considers in particular that the corrective measure proposed by the rapporteur is disproportionate in view of his responsibility for the data breach.

44. 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 stresses that he surrounded himself with competent specialists for this purpose.

45. He also claims to have implemented numerous security measures before the hearing and emphasizes his full cooperation with the Commission services.

46. The Restricted Committee recalls that in order to assess the advisability of imposing an administrative fine, reference should be made to the relevant criteria specified in Article 83(2) of the GDPR.

47. In the present case, it considers that it is appropriate to first apply the criterion provided for in subparagraph (f) of Article 83, paragraph 2, of the Rules relating to the degree of cooperation established with the authority of control with a view to remedying the breach and mitigating any adverse effects.

48. The Restricted Committee notes that as soon as he became aware of the violation, Mr [...] took the necessary measures to put an end to it immediately.

49. It thus recalls that in his e-mail of October 2, 2019 in response to the delegation of control, Mr [...] indicated that he had this PACS software purely and simply deleted upon receipt of your call and that he wrote a internal procedure to prevent a service provider from opening a port or a PACS on the server in the future and making it possible to connect to it as you seem to have been able to do .

50. It also points out that he subsequently surrounded himself with service providers, including the company […], in order to strengthen the security measures taken for the practice's medical imaging system, in particular through the encryption of the bootable hard drive and installation of an SSL certificate for the software's web server [...].

51. However, the Restricted Committee stresses that the criteria provided for in subparagraphs a) and g) of Article 83, paragraph 2, of the Rules should also be applied, relating firstly to the nature, seriousness 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 on the other hand, the categories of personal data concerned by the breach.

52. It thus notes that Mr [...] failed in two basic 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. .

53. 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 recital 75 of the GDPR.

54. It repeats that failure to comply with these elementary practices had the direct consequence of making more than one thousand two hundred sets of health data accessible, including, for each of these sets, in addition to the medical image, 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 the examination took place.

55. It recalls that the personal data hosted on the database of the image software […] remained accessible without any authentication for a period of just under five years, thus prolonging the risk that unauthorized third parties access the data and may possibly compromise it.

56. 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, including whether and to what extent the controller notified the breach.

57. It 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 the delegation of control has drawn his attention to this point.

58. In the light of these elements, the Restricted Committee therefore considers it necessary to impose an administrative fine on Mr [...].

59. 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.

60. It notes that according to his statements during the meeting of December 3, 2020, Mr [...] indicates that he earns approximately €8,000 per month 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.

61. Therefore, in the light of Mr [...]'s financial capacities and the relevant criteria of Article 83, paragraph 2, of the Rules, the Restricted Committee considers that the imposition of a fine of €6,000 appears effective, proportionate and dissuasive, in accordance with the requirements of Article 83(1) of these Rules.

FOR THESE REASONS

The CNIL Restricted Committee, after having deliberated, decides to:

impose an administrative fine on Mr. [...] in the amount of €6,000 (six 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 data controller.

President

Alexander LINDEN