Deliberation SAN-2018-010 of September 6, 2018 National Commission for Computing and Liberties Nature of the deliberation: Sanction Legal status: In force Date of publication on Légifrance: Thursday, September 27, 2018 Deliberation of the restricted committee no. SAN-2018-010 of 6 September 2018 pronouncing a pecuniary penalty against the XDeliberation of the restricted committee no. SAN-2018-010 of September 6, 2018 pronouncing a pecuniary penalty against the association XLa National Commission for Computing and freedoms, meeting in its restricted formation composed of Mr. Jean-François CARREZ, President, Mr. Alexandre LINDEN, Vice-president, Mrs. Dominique CASTERA, Mrs. Marie-Hélène MITJAVILE and Mr. Maurice RONAI, members; Having regard to Convention No. 108 of Council of Europe of 28 January 1981 for the protection of individuals with regard to the automatic processing of personal data; Having regard to Directive 95/46/EC of the European Parliament and of the Council, of 24 October obre 1995, relating to the protection of individuals with regard to the processing of personal data and the free circulation of such data; Having regard to law n° 78-17 of 6 January 1978 relating to data processing, files and Freedoms, amended by Law No. 2011-334 of March 29, 2011, in particular Articles 45 and following; Having regard to Decree No. 2005-1309 of October 20, 2005 taken for the application of Law No. of January 6, 1978 relating to data processing, files and freedoms, amended by decree no. 2007-451 of March 25, 2007; Having regard to deliberation no. 2013-175 of July 4, 2013 adopting the internal regulations of the Commission National Commission for Computing and Liberties; Having regard to decision no. verification of all processing accessible from the domain […]: Given the decision of the President of the National Commission for Computing and Liberties appointing a rapporteur to the restricted committee, dated May 24, 2018; Having regard to the report of Mr. François PELLEGRINI, rapporteur commissioner, notified to association X on June 5, 2018; Having regard to the written observations of association X received on July 6, 2018, as well as the oral observations made during the session of the restricted committee; Having regard to the other documents in the file; Were present, during the session of the restricted training of July 12, 2018: Mr. François PELLEGRINI, Commissioner, in his report;As representatives of association X:[…];[…];As counsel for association X:[…];The representatives of association X having taken to speak last; Adopted the following decision: Facts and procedure The association X (hereinafter the association) is an association created under the law of July 1, 1901, recognized as being of public utility, whose objective is to contribute to the development of the French language by offering French courses. Its turnover for the year 2017 is 8,871,905 euros. 'a security defect on the sub-domain […] forming part of the website […] operated by the association for the purposes of its activity. It was reported that this security flaw made it possible to access documents containing personal data from URL

addresses of the type […], where X represents an integer. On December 4, 2017, in application of the decision n° 2017-265C of November 27, 2017 of the President of the Commission, a delegation of the CNIL carried out online observations on the field […]. During the check, the delegation noted that the entry of several URL addresses of the aforementioned type made it possible to download documents containing personal data such as invoices, certificates of registration for a course or summaries of the courses followed . The delegation was thus able, by simply incrementing the value of X , to download 15,611 documents which all contained at least a surname and a first name and which for some also contained a postal address and a nationality. On the same day, the delegation contacted the association by telephone and email to inform it of the existence of this data breach and invited it to take the necessary measures to remedy it. On December 6, 2017, the association informed the delegation by email that it would proceed as soon as possible with the implementation of a patch preventing this data leak. Report No. 2017-265/1 was notified to the association on December 14, 2017. On February 5, 2018, the CNIL delegation carried out an inspection mission at the association's premises. The delegation noted on this occasion that the documents it had downloaded during the online check of December 4, 2017 were still accessible from the same URL addresses and that 413,144 documents were accessible. The association explained that the sub -domain […] had been carried out by its subcontractor, that not being satisfied with the latest version delivered, it had decided to terminate the contracts made with it and that it had taken over the administration and maintenance of the site in October 2017. The association explained that due to the dispute between it and its subcontractor, it had had the existence of the data breach noted by a bailiff on December 20, 2017 and that 'on this occasion, a fix had been put in place. On the day of the on-site inspection, the association had not yet received the official report drawn up by the bailiff. In addition, the association told the delegation that an email informing it of the existence of a vulnerability on the subdomain had been sent to her on July 20, 2017 but that she had not succeeded in contacting her sender. On February 23, 2018, a second online check carried out by the delegation of the CNIL has shown that the documents can still be downloaded. The association was informed the same day by e-mail. The report n°2017-265/3 was notified to the association on February 28, 2018. On March 2, 2018, the association indicated that corrective measures ending the data breach had been put in place For the purposes of examining these elements, the President of the Commission appointed Mr. François PELLEGRINI as rapporteur, on May 24, 2018, on the basis of Article 46 of Law No. 78-17 of January 6 1978 amended relating to data processing, files and freedoms (hereinafter the Data Protection Act or the amended law of January 6, 1978). At the end of his investigation, the rapporteur notified association X on June 5, 2018 of a report detailing the

breaches of the law that he considered constituted in this case and proposed to the restricted committee to pronounce a pecuniary penalty of forty thousand (40,000) euros which would be made public. This report was accompanied by a notice of meeting for the restricted training session of July 12, 2018 and invited the association to produce observations in response within one month. July 6, 2018, the association produced written observations in response to the report, reiterated orally during the restricted training session of the following July 12. Reasons for the decision On the breach of the obligation to ensure security and confidentiality data. Article 34 of the amended law of 6 January 1978 provides that the controller is required to take all useful precautions, with regard to the nature of the data and the risks presented by the processing. ment, to preserve the security of the data and, in particular, to prevent them from being deformed, damaged, or that unauthorized third parties have access to them. It is up to the Restricted Committee to decide whether association X has failed in its obligation to implement means to ensure the security of the personal data contained in its information system and in particular those of the users of the sub-domain […] so that this data is not accessible to unauthorized third parties. In defence, the association recalls that it was its subcontractor who, between September 2012 and October 2017 was in charge of the design of the subdomain at the origin of the incident and that it only began to use this tool in October 2017, the date on which it terminated the contract with its subcontractor. She also claims that no user has exploited the vulnerability contained in the URLs in question and that in any case, her website is of no interest to an attacker. She also states that she did not receive the first trial -verbal only on December 14, 2017 and having corrected the vulnerability as of December 20, 2017 when the bailiff's report was drawn up. On this point, it recalls that because of the dispute between it and its subcontractor, it was essential for it, before any corrective action on its part, to have the existence of the data breach noted by a bailiff of justice. It adds that it was only informed of the persistence of the violation during the on-site inspection of February 5, 2018, then when it received the report of the online inspection of the following February 23. Firstly, the Restricted Committee notes that the association does not dispute the existence of a security incident on the sub-domain […] which made accessible 413,144 documents containing the personal data of people taking the courses of French that she dispenses. The Restricted Committee notes that the exploitation of this vulnerability did not require any particular skill insofar as access to the documents was possible thanks to the simple modification of the value of X in the URL address […]. This very frequent vulnerability could have been avoided if, for example, the association had implemented a means of authentication making it possible to ensure that the people accessing the documents were indeed those whose personal data were contained in the said documents and possibly accompanied a device

to avoid the predictability of URLs. The Restricted Committee recalls that the exposure of personal data without prior access control is identified as being among the most widespread security breaches and for which special monitoring is required. Secondly, the Restricted Committee recalls that the the fact that a data breach may have originated from an error committed by a subcontractor has no influence on the obligation on the data controller to ensure rigorous monitoring of the actions carried out by the latter. Indeed, paragraph 3 of article 35 of the modified law of January 6, 1978, in the version applicable at the time of the facts, provides that the subcontractor must present sufficient guarantees to ensure the implementation of the measures of security and confidentiality mentioned in Article 34. This requirement does not relieve the controller of his obligation to ensure compliance with these measures. . The Restricted Committee then points out that the association explained during the control procedure that it was aware that the software delivered by its subcontractor had malfunctions. Therefore, it should have been more vigilant, especially when it was alerted in July 2017 by an outside person of the existence of a vulnerability on its subdomain. Furthermore, the association's assertion that no one consulted the documents from the URLs in question is not based on any evidence and in any event is incorrect since a person was able to access the data in question in July 2017. Finally, the Restricted Committee recalls that the implementation of security measures is an obligation incumbent on the data controller which does not depend on the potential attractiveness of the data processed or their value on the market. Only the means implemented to meet this obligation may vary according to a multitude of criteria such as the number of data processed, their nature and the categories of persons concerned. With regard to these elements, the Restricted Committee considers that the The association has not taken all the necessary precautions to prevent unauthorized third parties from having access to the data processed and considers that the breach of article 34 of the law of January 6, 1978 as amended is constituted. On the sanction and advertisingUnder the terms of I of article 45 of the amended law of January 6, 1978, in the version applicable on the day of the findings: When the data controller does not comply with the obligations arising from this law, the president of the Commission Nationale de l'Informatique et des Libertés may give him formal notice to put an end to the observed breach within a time limit that he sets. In the event of extreme urgency, this period may be reduced to twenty-four hours. If the data controller complies with the formal notice addressed to him, the chairman of the commission declares the procedure closed. Otherwise, the restricted committee may pronounce, after a contradictory procedure, the following sanctions: 1° A warning; 2° A pecuniary sanction, under the conditions provided for in Article 47, with the exception of where the processing is carried out by the State; 3° An injunction to cease the processing, when this falls under Article 22, or a

withdrawal of the authorization granted pursuant to Article 25. When the breach found cannot be brought into compliance within the framework of a formal notice, the restricted committee may pronounce, without prior formal notice, and after an adversarial procedure, the sanctions provided for in this I. paragraphs 1 and 2 of article 47 of the aforementioned law, in the version applicable on the day of the findings, specify that: The amount of the financial penalty provided for in I of article 45 is proportionate to the seriousness of the breach committed and to the benefits derived from this lack t. The restricted formation of the Commission Nationale de l'Informatique et des Libertés takes into account in particular the intentional or negligent nature of the breach, the measures taken by the data controller to mitigate the damage suffered by the persons concerned, the degree of cooperation with the commission in order to remedy the breach and mitigate its possible negative effects, the categories of personal data concerned and the manner in which the breach was brought to the attention of the commission. The amount of the penalty may not exceed 3 million euros. The association considers that with regard to the circumstances in which the data breach occurred, neither a financial penalty of 40,000 euros, nor the publicity of this penalty are justified. It considers that the seriousness of the breach is not established in the extent that no person affected by the data breach has lodged a complaint with them, that the data made accessible was not sensitive and that the number of users of the website is not a relevant element for assess the seriousness of the breach. First, the Restricted Committee recalls that the absence of complaints from users and the fact that the data accessible does not contain any data that could be qualified as sensitive, within the meaning of Article 8 of the Data Protection Act, have no influence on the characterization of the breach of the obligation incumbent on a data controller to ensure the security of the data he processes. It also points out that the data breach concerned a large number of documents all containing identifying data such as surname, first name and postal address. Secondly, with regard to the association's responsiveness to put end to the data breach, the Restricted Committee notes that as of December 4, 2017, the CNIL's supervisory delegation sent the association an email stating the existence of the data breach and which contained the type of URL address causing this violation. It was therefore, from this date, in a position to begin investigations on its sub-domain. The Restricted Committee points out that contrary to what the association maintains, the data breach was not put an end to on December 20, 2017 since the CNIL delegation noted its persistence for the first time during the on-site inspection of the February 5, 2018 then a second time during the online check of February 23, 2018. It was not until March 2, 2018 that the association informed the CNIL that the data breach had been definitively put to an end. place, the Restricted Committee considers that the seriousness of the breach is characterized, in particular with regard to the

elementary nature of the security incident constituted by the absence of authentication measures for the persons accessing the documents and by the foreseeable nature of the URL addresses allowing to download them. With regard to the elements developed above, the facts observed and the failure constituted in article 34 of the law of January 6, 1978 as amended justify the imposition of a sanction of one amount of 30,000 (thirty thousand) euros. Finally, the Restricted Committee considers that, given the seriousness of the aforementioned breach, the current context in which security incidents are multiplying and the need to raise awareness among data controllers and Internet users as to the risks weighing on data security, its decision should be made public.FOR THESE REASONSThe Restricted Committee of the CNIL, after having deliberated, decides: of an amount of thirty thousand (30,000) euros; to make its deliberation public, which will be anonymized at the end of a period of two years from its publication. The President Jean-François CARREZ This decision is likely to make the object of an appeal before the Council of State within two months of its notification.