Deliberation SAN-2018-003 of June 21, 2018 National Commission for Computing and Liberties Legal status: In force Date of publication on Légifrance: Thursday June 28, 2018 Deliberation of the restricted committee no. SAN-2018-003 of June 21, 2018 pronouncing a sanction pecuniary against X The National Commission for Computing and Liberties, 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 the Council of Europe of 28 January 1981 for the protection of individuals with regard to the automatic processing of personal data; Having regard to Law No. 78-17 of January 6, 1978 amended relating to data processing, files and freedoms, in particular its articles 45 and following; Having regard to decree no. 78-17 of January 6, 1978 relating to information technology, files and freedoms of March 25, 2007; 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. 2017- 147C of June 12, 2017 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 all processing of personal data accessible from the domain […]; Having regard to decision no. 2017-157C of the President of the CNIL of June 12, 2017 to instruct the Secretary General to carry out or to have carried out a verification mission with the association XY; Having regard to the decision of the President of the Commission appointing a rapporteur to the restricted committee, dated January 24, 2018; Having regard to the report of Mr François PELLEGRINI, rapporteur commissioner, notified by bearer to association X on February 23, 2018; Having regard to the ob written services from association X received on April 16, 2018, as well as the oral observations made during the restricted training session; Considering the other documents in the file; Were present, during the restricted training session of May 3, 2018 :Mr. François PELLEGRINI, Commissioner, in his report;As representative of the association X: Y;As counsel for the association X: Z;Mr. Michel TEIXEIRA, Deputy Government Commissioner, having made no observations;The representatives of association X having spoken last;Adopted the following decision:Facts and procedureX (hereinafter X or the association) is a private non-profit association created under the law of July 1, 1901. Its mission is to provide accommodation in residences and hostels for people in social difficulty, in particular students, single-parent families and migrant workers. The association employs approximately 270 people and in 2016 achieved a turnover of 37.6 million euros. Its headquarters are located at […]. On June 11, 2017, the National Commission for Computing and Liberties (hereinafter CNIL or the Commission) was alerted to the existence of a security flaw allowing access to tax notices from beneficiaries of association, based on a

search carried out on the Google search engine. Pursuant to decision no. 2017-147C of the President of the Commission of June 12, 2017, a CNIL delegation carried out a online check the following June 15 on the processing implemented by the association. The report n°2017-147/1 drawn up at the end of this mission was sent to the association by e-mail (e-mail) and by post on June 20, 2017. During the inspection, the delegation applied for housing by filling in the form on the association's website […] and found that a change in the path of the URL displayed in the browser allowed access to documents saved by others applicants. In addition, the delegation carried out the following search directly within the Google search engine […] . She found that income tax notices appeared in the displayed results list. On June 15, 2017, the delegation contacted the association by telephone and email to inform them of the existence of this violation. of personal data and ask him to take the necessary corrective measures to remedy it. By email of the following June 19, the Commission informed the association that personal data was still freely accessible on the domain […]. On June 20, 2017, the association informed the CNIL that it had asked its IT department to contact the website host and specified that the Commission would be informed as soon as possible of the corrective measures taken. In application of decision no. 2017-157C of June 12, 2017 of the President of the CNIL, a Commission delegation carried out an inspection mission to the association's premises on June 21, 2017, in particular to verify the corrective measures taken following the disclosure of the data breach. Inspection report no. 2017-157/1 was notified to the association on June 23, 2017. During the on-site inspection, the association informed the delegation that it had contacted the company […], which had developed the website in 2012, so that it could implement the corrective measures. However, it was noted on this occasion that the data of the persons were still accessible on the Internet by a simple modification of the URL. For the purposes of examining these elements, the President of the Commission appointed Mr François PELLEGRINI as rapporteur, on January 24, 2018, on the basis of article 46 of law n° 78-17 of January 6, 1978 as amended relating to data processing, files and freedoms (hereinafter the Data Protection Act or the law of January 6, 1978 amended). At the end of his investigation, the rapporteur notified association X, by hand, on February 23, 2018, of a report detailing the breaches of the law that he considered constituted in this case. This report proposed to the restricted formation of the Commission to pronounce a pecuniary sanction which could not be less than one hundred and fifty thousand (150,000) euros and which would be made public. April 2018 indicating to the association that it had a period of one month to communicate its written observations. session. This request was accepted on March 21, 2018 and the meeting was postponed to the following May 3. The board of the association also requested, by letter of March 14, 2018, the communication of the acts of appointment and authorization of

the two CNIL inspectors to carry out inspections, as well as the formal notice sent by the President of the CNIL to the association in accordance with I of article 45 of the law of January 6, 1978 as amended. By letter of 20 March 2018, the secretary general of the CNIL informed the association that the two CNIL agents had been authorized to carry out verification missions by deliberation n° 2017-150 of May 9, 2017 available on the website www. legifrance.gouv.fr and provided the two mission orders requested. In addition, he informed the council of the association that no formal notice had been adopted by the President against the association prior to the sending of the sanction report. In addition, the council of the association requested, by letter of the same day, from the Commission the communication of the appendices and attachments of the minutes of the controls as well as the justification that the controllers had carried out, prior to the online control, any measure guaranteeing the reality of the facts observed and conferring probative force on the findings. June 20, 2017. The association and its counsel were also informed that they could obtain on-site communication of the documents in the file. On April 16, 2018, the association produced written observations on the report, reiterated or also during the restricted committee meeting of the following May 3.Reasons for the decision1. On the grounds for nullity of the procedure raised by the associationIn the first place, the association maintains that the sanction procedure is vitiated by nullity since it disregards I of article 45 of the law of January 6, 1978 as amended by law no. 2016-1321 of October 7, 2016 for a digital Republic.I of article 45 of the amended law of January 6, 1978 provides that:I. - When the data controller does not comply with the obligations arising from this law, the President of the National Commission for Computing and Liberties may give him formal notice to put an end to the observed breach within a period 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 committee declares the procedure closed. contrary, 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, except in cases is implemented by the State; 3° An injunction to cease the processing, when this falls under Article 22, or a withdrawal of the authorization granted in application of Article 25. When the failure observed does not may 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. The association asserts that in application of this provision, she should have received a prior formal notice from the President before sending the sanction report and that in the absence of such a decision, the sanction procedure initiated before the restricted committee is void.The restricted committee notes that it follows from the very wording of Article

45 of the aforementioned law of 6 January 1978 that the pronouncement of a sanction is not subject to the prior systematic adoption of a formal notice. In this regard, it emphasizes that the last paragraph of this article expressly provides that when the breach observed cannot be brought into compliance in the context of a formal notice, the restricted committee may pronounce, without notice prior formal notice and after an adversarial procedure, the penalties provided for in this I . It also recalls that the purpose of the reform introduced by the law for a digital Republic was to widen the range of direct sanctions that it can apply, by authorizing the imposition of a pecuniary sanction without prior formal notice, whereas Previously, the Restricted Committee could only issue a warning in such cases. may by construction have effect only for the future and not for the past), the restricted panel may pronounce the penalties provided for. effect of making it impossible to sanction past offences. It would even constitute a reason for a data controller who has caused or suffered a data breach to refrain from taking any corrective action and to wait for a formal notice to be sent to him, the mere fact of doing so. to comply then obstructing the pronouncement of a sanction. staff for the duration of the security incident) but that the failure could be directly sanctioned, under the last paragraph of I of article 45 of the law of January 6, 1978 modified.Secondly, the association maintains that she received the online report of June 15, 2017, the following June 22, i.e. after the on-site inspection by the CNIL delegation. It maintains that it was only at this stage that it was able to learn about the proceedings in progress, without measuring the penalties incurred and to be able to actually exercise its rights of defense in the context of adversarial proceedings. restricted notes, however, that it appears from the attachments to the report that the minutes of the online check were sent to the association by email on 20 June 2017 and by post on the same day. Although it did receive the minutes in paper format on June 22, 2017, the association was aware on the day of the on-site inspection, June 21, 2017, of the findings made by the Commission during the online inspection. therefore considers that the association was aware as of June 20, 2017, of the nature, day, time and purpose of the inspection carried out by the CNIL delegation on June 15, 2017. In this respect, the Restricted Committee notes that it appears from the minutes drawn up during the on-site inspection that the association indicates that it received the minutes of the online check on June 20, 2017. The Restricted Committee also considers that the rights of the defense n were not disregarded when the association was informed of its right to be assisted or represented by the counsel of its choice, during the on-site inspection of June 21, 2017, and when it formulated, by through its representative, written observations and oral in response to the report made against it. Finally, the Restricted Committee notes that no other ground for nullity results from the investigation before it. Consequently, the pleas alleging the nullity of the sanction procedure

can only be discarded. On the breach of the obligation to ensure data security under article 34 of the law of January 6, 1978 as amended Article 34 of the law of January 6, 1978 as amended provides that: The person in charge of the processing is required to take all useful precautions, with regard to the nature of the data and the risks presented by the processing, to preserve the security of the data and, in particular, to prevent them from being distorted, damaged, or that unauthorized third parties have access. It is up to the Restricted Committee to decide whether association X has failed in its obligation to implement appropriate means to ensure the security of the personal data contained in its information system and, in particular, those users of the website […] so that this data is not accessible to unauthorized third parties. In defence, the association acknowledges the existence of the security incident noted. The Restricted Committee notes that it has been proven that the CNIL services were able to access the documents recorded by the users of the website […]. Firstly, while emphasizing the diligence of the association, which reacted quickly after the revelation of the incident to correct it, the Restricted Committee notes that basic security measures had not been taken prior to the development of its website. Indeed, the Restricted Committee notes that the modification of a word present in the URL of the housing application form such as passport or cni allowed unauthorized third parties to access the documents provided by users from its website. This data breach was made possible by the association's failure to put in place a mechanism to avoid the predictability of URLs. In addition, the Restricted Committee considers that the association should have at least set up a function modifying the name of the files saved by people, when uploading them to its storage directory, in order to prevent a person from identifying the access path to the saved files. committee considers that the association should have put in place such elementary measures which, moreover, did not require major or costly developments. no procedure for identifying or authenticating users of the website has been put in place to protect the information recorded. The Restricted Committee considers that the association should have put in place a restriction of access to the documents made available to customers via a space reserved for each person, accessible using a username and password. The association should have, moreover, if it did not wish to create accounts dedicated to each user, implement a means to ensure that the persons accessing the recorded documents were indeed the origin of the request (for example example using a session identifier cookie). It thus considers that the implementation of such functionalities constitutes an essential precaution for use, the implementation of which would have made it possible to significantly reduce the risk of the occurrence of the observed data breach. Furthermore, the Restricted Committee notes that the association had not taken any measures to protect the directories containing the documents of applicants for housing, directly accessible from the Internet. In

this respect, the Restricted Committee notes that it was only after the Commission intervened with the association that measures were taken to protect the documents concerned by the incident and make them inaccessible to third parties unauthorized by moving them to a private folder. Secondly, the Restricted Committee notes that the exploitation of the data breach did not require any particular technical skills. She recalls that to access the documents of other clients, it was enough to modify the path of the URLs of the request forms which contained the name of the document registered by the person. Thus, it was particularly easy for a person to enter in a URL the name of a document that he wanted to see displayed, such as a pay slip or an identity card. The Restricted Committee also recalls that the data was freely accessible by performing a search within the Google search engine, thus increasing the risk that the incident will be exploited by unauthorized third parties. The Restricted Committee also recalls that, in general , the exposure of personal data without prior access control, is identified as being part of the security breaches for which special monitoring is required and must, therefore, be the subject of checks, in particular within the framework of security audits. In this respect, the Restricted Committee stresses the importance of carrying out a complete test protocol before the production of a website. It also appears that the association did not carry out, after the deployment of the websites, the regular checks which were its responsibility with regard to the security measures put in place. The Restricted Committee therefore considers that the association did not not taken all the necessary precautions to prevent unauthorized third parties from having access to the data processed. Thirdly, the association specifies that the incident did not concern all the housing application files made online, but only documents provided by people who have not finalized their procedure on the website. She explains that this is the reason why access to certain documents was not secure. The Restricted Committee considers that such an explanation, in addition to demonstrating the retention of personal data for an unjustified period, has no impact on the characterization of the breach since the association was required to ensure the security of all the personal data processed, even those concerning people who did not validate their request for accommodation. On the basis of these elements, it considers that the breach of article 34 of the amended law of January 6, 1978 is established.III. On the penalty and publicityUnder the terms of the 1st and 2nd paragraphs of article 47 of the amended law of 6 January 1978, 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 failure. 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 maintains that the sanction which would be pronounced against it should only be symbolic. She argues that a penalty of 150,000 euros proposed by the rapporteur would be disproportionate to the criteria set out in article 47 of the amended law of 6 January 1978 since she indicates that she cooperated with the delegation of control of the CNIL and to have put in place rapid measures to correct the incident. Firstly, the Restricted Committee considers that the seriousness of the violation is characterized by the nature of the data concerned. Indeed, the violation has rendered accessible official documents, in their entirety, such as proof of identity (passports, residence permits and identity cards), pay slips, tax notices or even payment certificates from the Caisse d' Family allowances. In addition, these documents contain a multitude of data identifying users of the website such as surnames, first names, dates of birth, postal address, registration number in the national directory of identification of natural persons or IBAN. , moreover, that certain accessible information is a matter of private life since the documents make it possible to know the salary of the persons, their reference tax income, their marital status or their number of children and to know whether they receive the aid personalized housing. The Restricted Committee considers that it was up to the association, given the quantity and nature of the data processed, to be particularly vigilant about their security. Secondly, the Restricted Committee considers that the seriousness of the breach is also characterized by the number of documents and persons concerned by the breach. The Restricted Committee notes that it is rt of the documents in the file that on the date of the security incident, 42,652 documents were stored on the hard drive of the association with the application forms completed by the users. The control delegation was able to download a sample of 385 documents, after deduplication, hosted in the directories of the association. It is established that the security breach allowed the delegation of control to access the documents stored in these directories. It therefore appears that the incident made a large number of documents accessible and concerned a large number of people. The Restricted Committee notes, however, that the association reacted quickly after learning of the data breach by putting in place corrective measures within a reasonable time after being alerted by the CNIL. on-site inspections. With regard to the elements developed above, the facts observed and the failure to comply with Article 34 of the law of January 6, 1978 as amended justify the imposition of a pecuniary penalty in the amount of seventy-five thousand (75,000) euros.Finally, the Restricted Committee considers that, with regard to the aforementioned elements on the nature of the data in question, the current context in which incidents of

security and the need to make data controllers and internet users aware of the risks to data security, its decision should be made public. FOR THESE REASONS :pronounce against X a pecuniary penalty in the amount of 75,000 (seventy-five thousand) euros;make public its decision, which will be anonymized at the end of a period of two years from its publication.The President Jean-François CARREZ This decision may be appealed to the Council of State within two months of its notification.