Deliberation SAN-2019-005 of May 28, 2019 National Commission for Computing and Liberties Nature of the deliberation: Sanction Legal status: In force Date of publication on Légifrance: Thursday June 06, 2019 Deliberation of the restricted committee no. SAN – 2019-005 of 28 May 2019 pronouncing a pecuniary penalty against the company XLThe National Commission for Computing and Liberties, meeting in its restricted formation composed of Mr. Alexandre LINDEN, Chairman, Mr. Philippe-Pierre CABOURDIN, Vice-Chairman, Ms. Sylvie LEMMET and Mrs 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 the 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 as amended relating to information matic, files and freedoms, in particular its articles 45 and following; Considering the decree n ° 2005-1309 of October 20, 2005 modified taken for the application of the law n ° 78-17 of January 6, 1978 modified relating to the 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. 2018-186C of September 5, 2018 of the President of the National Commission for Computing and Liberties to instruct the Secretary General to carry out or have carried out a verification mission; Having regard to the decision of the President of the National Commission for Computing and Liberties appointing a a rapporteur before the restricted committee, dated February 1, 2019; Having regard to the report of Mr. Éric PÉRÈS, commissioner rapporteur, of February 4, 2019; Having regard to the written observations submitted by company X on March 4, 2019; Having regard to the observations in response from commissioner-rapporteur of March 15, 2019; Having regard to the observations in response submitted by company X on April 2, 2019 as well as the oral observations made during the restricted committee meeting; Having regard to the other documents in the file; of the restricted training of April 11, 2019: Mr. Éric PÉRÈS, statutory auditor, heard in his report;As representatives of company X:[…] The company having the last word;After deliberation, adopted the following decision:Facts and procedure1.Company X (hereinafter the company) specializes in property development, purchase, sale, rental and property management. It employs 486 people and generated revenue of approximately €43 million in 2017.2. For the needs of its activity, the company publishes the website www.[...].com (hereinafter the site) which allows in particular candidates for the rental of a property to download the supporting documents necessary for the constitution of their file.3. On August 12, 2018, the National Commission for Computing and Liberties (hereinafter CNIL or the Commission)

received a complaint from a user of the site. The complainant indicated that a modification of the character X in the URL address composed as follows: https://www.crm.[...].com/documents/upload/eresa/X.pdf , where X represents a number whole, had allowed him to access the supporting documents that he himself had downloaded via the site but also those downloaded by other candidates for rental. In his complaint, the complainant provided several examples of URLs from which he was able to access parts uploaded by third parties. He stated that he had informed the company of these facts as early as March 2018.4. Pursuant to decision no. 2018-186C of September 5, 2018 of the President of the Commission, an online inspection mission then an inspection mission within the company's premises were carried out respectively on September 7 and 13, 2018. The purpose of these missions was to verify compliance with the amended law of January 6, 1978 (hereinafter the Data Protection Act) and Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (hereinafter GDPR or the Regulation) of the processing of personal data accessible from the [...].com domain or relating to personal data collected from the latter.5.During the control mission in online, the delegation found that entering one of the URLs provided by the complainant enabled the downloading of a tax notice issued in a name different from his own. The delegation then proceeded to download 9,446 documents using a script, including copies of identity cards, Vitale cards, tax notices, death certificates, marriage certificates , social security affiliation certificates, certificates issued by the family allowance fund, disability pension certificates, divorce judgments, account statements, bank account statements and rent receipts.6.The company was informed on September 7, by the delegation, of the existence of a security defect on its site and an e-mail containing the type of URL addresses concerned by this security defect was sent to him. On September 13, 2018, during the inspection mission to the company's premises, the CNIL delegation noted that the URL addresses provided by the complainant in his referral still allowed access to the documents in question. The company told the delegation that the supporting documents uploaded by rental applicants are recorded in a dedicated directory. It was clarified that the entire directory had been made accessible by the security flaw. It emerges from the observations made that this directory contained 290,870 files on the day of the inspection. The company further indicated that the documents provided by the candidates were not purged and that they were not reused later, the documents of the candidates who accessed the tenancy being moved to another directory of the company. database.8.The company confirmed to the delegation that a report informing it that documents were freely accessible from the site, without prior authentication, had reached it in March 2018. It specified that at the Following this report, it carried out an initial phase of analysis of the security defect, which gave rise to an action plan implemented from June 2018.

It also indicated that an initial action to no longer display URLs as they appeared at the time of the breach had been rolled out days before the September 13 audit. The company then explained that a measure permanently ending the security flaw was to be put into production on September 17, 2018. The minutes of September 7 and 13 were notified to the company on September 17.9. For the purpose of examining these elements, the President of the CNIL appointed, on February 1, 2019, Mr Éric PÉRÈS as rapporteur on the basis of article 47 of the law of January 6, 1978. By letter dated 1 February 2019, the President of the CNIL informed the company of this appointment.10. At the end of his investigation, the rapporteur notified Company X, on February 5, 2019, of a report detailing the breaches relating to Articles 5 and 32 of the GDPR that he considered constituted in this case.11. This report proposed that the CNIL's restricted committee impose a financial penalty of 900,000 euros on company X, which would be made public.12. Also attached to the report was a notice to attend the restricted committee meeting of April 11, 2019. The company had one month to submit its written observations. On February 11, 2019, the company made a request for the session to be held behind closed doors. This request was granted by letter dated February 22, 2019 insofar as certain elements submitted to the proceedings are protected by business secrecy, as provided for by Article L 151-1 of the Commercial Code.13. On March 4, 2019, the company provided written comments on the report. These observations were the subject of a response from the rapporteur on March 15, 2019. On April 2, 2019, the company produced new observations in response to those of the rapporteur.14. All of the observations were reiterated orally by the company and the rapporteur during the restricted training session of April 11, 2019. II. Reasons for the decision On the request for nullity of the findings online of September 7, 201815. The company makes argue that during the online check of September 7, 2018, CNIL agents extracted the files accessible from URL addresses composed as follows: https://www.crm.[...]. com/documents/upload/eresa/X.pdf whereas the provisions of article 44 of the Data Protection Act only authorize CNIL agents to consult data that is freely accessible or made accessible and that they do not make it possible, under no circumstances, to maintain it in an automated data processing system with a view to extracting data by downloading them. contained in the trial -verbal n° 2018-186/1 of September 7, 2018.17.The restricted committee recalls that under the terms of paragraph 3 of III of article 44 of the Data Protection Act, the agents of the Commission may in particular, at from an online public communication service, consult the data freely accessible or made accessible, including through imprudence, negligence or by the act of a third party, where applicable by accessing and maintaining automated data processing for the time necessary for the findings; they can transcribe the data by any appropriate processing into documents that can be used directly for control purposes .18.

By downloading the files from the aforementioned URL addresses, the CNIL agents did indeed proceed to a transcription of the data and not to an extraction, insofar as the files were not moved from the database of the company but have simply been copied. The Restricted Committee considers that by downloading the files made freely accessible by the lack of security, the CNIL agents acted in strict compliance with the provisions of the aforementioned Article 44, which moreover does not exhaustively list the forms that may take transcripts from authorized agents.19. Consequently, the request for nullity will be rejected. On the use of elements from the response of the company Y20. The company notes that in the report notified on February 5, 2019, the rapporteur indicated that he had taken into account information which had been forwarded by its subsidiary, company Y, a separate legal entity from company X, in the context of sanction proceedings previously opened against the latter. Company X argues that neither the report nor the rapporteur's response clearly indicates what information provided by company Y was relied upon by the rapporteur in this proceeding. The company thus indicates that it does not know how the rapporteur took these elements into account in developing its proposal. It therefore asks the Restricted Committee to rule solely on the basis of the observations and documents it has provided and to exclude the information provided by company Y. The Restricted Committee notes first of all that, in its report of 4 February 2019, the rapporteur clearly stated that a first sanction procedure had been initiated against company Y but that the investigations carried out within the framework of this procedure had revealed that Y was not responsible of treatment for which shortcomings could be attributed. The Restricted Committee notes that, moreover, the sanction procedure initiated against company Y was closed on 31 January 2019.22. The Restricted Committee then notes that, in its response to the company's observations, the rapporteur indicated that the elements which he had taken into account to draw up his report were the information relating to the fact that X had proceeded to the notification of the data breach to the persons concerned, the fact that the number of persons affected by the data breach had been clarified and the fact that the documents submitted by the candidates were kept for pre-litigation and litigation purposes.23. It considers that the information given by the rapporteur enabled the company to identify unambiguously the information in question and the developments in the report containing it.24. Finally, the Restricted Committee stresses that all of the information on which the rapporteur based his proposal for a sanction, whatever the source, was brought to the attention of company X in the context of the procedure and submitted to a contradictory debate. In doing so, the company became aware that this information had been taken into account and was given the opportunity to question the accuracy of the facts developed in the report and to contest their scope.25. Consequently, the company's request not to take

into consideration the elements resulting from the procedure followed against company Y.3 should be rejected. On the absence of prior formal notice26. The company argues that the shortcomings of which it is accused could have been corrected in the context of a formal notice. It therefore considers that the immediate initiation of sanction proceedings, without prior formal notice, deprived it of the possibility of bringing itself into compliance.27.The Restricted Committee notes that it follows from the very letter of the provisions of III of article 45 of the amended law of January 6, 1978, resulting from law no. is not subject to the prior adoption of a formal notice. The decision to appoint a rapporteur and to refer to the restricted committee is a power belonging to the President of the CNIL, who has the opportunity to prosecute and can therefore determine, depending on the circumstances of the case, the action to be taken on investigations by, for example, closing a file, by issuing a formal notice or by seizing the restricted committee with a view to issuing one or more corrective measures.4. On the breach of the obligation to ensure the security and confidentiality of personal data. On the characterization of the breach28. Article 32 (1) of the Regulation provides that: 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, including the degree of probability and seriousness 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: pseudonymization and encryption of personal data; means to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; means to restore the availability of personal data and the access to them within appropriate timeframes in the event of a physical or technical incident; a procedure for regularly testing, analyzing and evaluating the effectiveness of technical and organizational measures to ensure the security of the processing. 29. Article 32 (2) provides that: When assessing the appropriate level of security, particular account shall be taken of the risks posed by the processing, resulting in particular from the destruction, loss, alteration , the unauthorized disclosure of personal data transmitted, stored or otherwise processed, or unauthorized access to such data, accidentally or unlawfully. It is up to the Restricted Committee to determine whether company X has failed in its obligation to ensure the security of the personal data processed and whether, in particular, the company has implemented means to guarantee their confidentiality, in order to prevent that they are accessible to unauthorized third parties, in accordance with the aforementioned Article 32 (1) ii.31.The Restricted Committee notes first of all that the existence of a security defect on the site www.[. ..].com is not contested by the company. It notes that this security defect made possible the breach of personal data insofar as it allowed unauthorized third parties to access this data.32.The

Restricted Committee recalls that when a request to access to a resource is addressed to a server, the latter must first ensure that the sender of this request is authorized to access the requested information. In the present case, both the complainant and the delegation of control were able to freely consult the documents transmitted to the company by a large number of candidates for rental, without any measure restricting this possibility.33. This access to the documents kept by the company reflects a faulty design of the site, characterized in this case by the lack of implementation of a user authentication procedure. The data breach resulting from this security flaw could have been avoided if, for example, the company had implemented a means of authentication to ensure that the people accessing the documents were indeed the ones from whom they originated. download to the directory in question, and that only they could access it. The implementation of such a feature constitutes an essential precaution for use, which would have made it possible to guarantee the confidentiality of the personal data processed, in accordance with Article 32 (1) ii, and to significantly reduce the risk of this occurring. data breach. The Restricted Committee recalls that the exposure of personal data without prior access control is identified as one of the most widespread vulnerabilities and that it has already pronounced numerous public pecuniary sanctions for similar acts. 35.In view of these elements, the Restricted Committee considers that the company has not implemented the appropriate technical and organizational measures to guarantee the security of the personal data processed, in accordance with Article 32 of the Regulation.b. On the scope of the breach36. The company points out that exploiting the vulnerability required special skills, as evidenced by the use of a script by the delegation of control, and that it was only possible with knowledge from the URL address https://www.crm.[...].com/documents/upload/eresa/X.pdf . The company also notes that all the documents contained in the directory could not have been downloaded by the delegation of control. It also argues that no site user has reported to it that its personal data has been misused. constitution of the file, in particular to assess their solvency, and that it does not ask candidates for any other document than those referred to in decree no. and his surety.38. It also recalls that it has no control over the documents spontaneously downloaded by the candidates although they do not appear in the aforementioned decree. In the same way, the company considers that it cannot be held responsible for the fact that certain candidates download their Vitale card as proof of identity or that the registration number in the directory (NIR) appears on documents issued by social organisms transmitted by people.39. Finally, the company explains that following the data breach, it planned the patching of the vulnerability over several months, which resulted in the release of a patch on September 17, 2018 to permanently put a end to vulnerability. The company states that these delays are explained by the strong demand for rentals in the summer

period and by the difficulty of suspending its activities during this period.40. Firstly, the Restricted Committee observes that the exploitation of the vulnerability did not require any particular technical mastery in computer matters. Indeed, the simple modification of the value of X in the URL address https://www.crm.[...].com/documents/upload/eresa/X.pdf allowed anyone with knowledge of the aforementioned URL to download the documents in question, without the prior creation of an account on the site being necessary, and without this requiring more complicated handling than the simple modification of the value X , which corresponds to a number. Moreover, the Restricted Training considers that the use of a script does not require any advanced skills to exploit this vulnerability. The use of a script by the delegation of control had the sole purpose of automating a manual process consisting in modifying the value of X at the end of the URL address in question, to download the documents one after the other from faster way.41. Secondly, with regard to the number of files affected by the security flaw, the Restricted Committee observes that it was the CNIL delegation which, on its own initiative, interrupted the execution of the script in order not to overload the server hosting the website. It then emerges from the information transmitted by the company to the delegation during the inspection of September 13, 2018, and from the findings made, that all of the documents contained in the directory in question, i.e. 290,870 files, were made accessible by this security flaw. The files which according to the company could not have been downloaded corresponded to numbers to which no files were attached as the company agreed at the hearing. The panel notes that, in its observations, the company further indicated that the number of persons concerned was 29,440.42. Thirdly, the Restricted Committee considers that the breach of the security obligation is aggravated with regard to the nature of the personal data made accessible. Indeed, as explained above, the documents transmitted by candidates for rental are of a very diverse nature and included, among the documents in question, marriage certificates, divorce judgments, employment contracts, documents relating to social benefits or tax notices. These documents contain not only identification data, such as surname, first name and contact details, but also a great deal of information liable to reveal some of the most intimate aspects of people's lives, such as the judgments of divorce.43.The Restricted Committee does not call into question the need for company X to have most of these documents. It nevertheless recalls that Article 32 of the Regulation requires the data controller to implement security measures adapted to the risks induced by the processing for the rights and freedoms of individuals, risks resulting in particular from unauthorized access to personal data. processed. In addition, insofar as company X processes documents containing very specific information on certain aspects of the private life of individuals, the need to put in place proportionate security measures, making it possible to guarantee their confidentiality, was all the more more important.

The Restricted Committee recalls on this point that recital 83 of the Regulation provides that […] These measures should ensure an appropriate level of security, including confidentiality, taking into account the state of knowledge and the costs of implementation compared to the risks and the nature of the personal data to be protected.44. Finally, the Restricted Committee notes that the existence of the vulnerability on the www.[...].com site was brought to the attention of the company on March 8, 2018 and was only resolved in September 2018. Users' personal data was therefore accessible for at least six months even though company X was aware of it. If the restricted committee admits that the correction of the vulnerability could require phases of analysis and technical developments, it considers that emergency measures not having the objective of correcting the vulnerability but of reducing the extent of the violation were technically simple to set up and could have been quickly deployed. For example, the files contained in the directory made accessible by the vulnerability could have been moved to a temporary directory or a URL filtering measure could have been implemented to prevent access to the documents. Moreover, it appears that the company, aware of the increase in its activities from the month of May, due to the strong demand for rentals, has chosen to favor the stability of its information system during this period. to the correction of the vulnerability of the personal data that it contained. Consequently, insofar as the security defect was brought to its attention on March 8, 2018, and since the company knew that a peak in activities would occur from May, it was up to it to anticipate this difficulty and to take at least all the necessary measures as soon as this vulnerability is known.5. On the breach of the obligation to retain the data for a proportionate period45. Article 5-1-e) of the Regulation provides that: 1. Personal data must be:[…]e) kept in a form allowing the identification of the persons concerned for a period not exceeding that necessary for the with regard to the purposes for which they are processed; personal data may be stored for longer periods insofar as they will be processed exclusively for archival purposes in the public interest, for scientific or historical research purposes or for statistical purposes in accordance with Article 89 , paragraph 1, provided that the appropriate technical and organizational measures required by these Regulations are implemented in order to guarantee the rights and freedoms of the data subject (limitation of storage) .46. The rapporteur criticizes company X for keeping the documents transmitted by the candidates who have not accessed the rental beyond the time necessary to achieve the purpose for which the personal data were collected and processed – namely rental of real estate - and this without this conservation being framed by appropriate guarantees.47. In defence, the company recalls first of all that these people are likely to seize the Defender of Rights alleging discrimination and, as such, the Defender of Rights can demand from the company the transmission of all of the file submitted by the candidate. The company specifies

that the limitation period applicable to acts of discrimination being six years, the documents are kept for this period. It adds that the delegation of control did not note the presence in the directory affected by the vulnerability of any document prior to 2012. The company underlines in its writings that no document in the file proves the absence of intermediate archiving of the data and management of access authorizations to documents.48.The Restricted Committee recalls that the retention period for personal data must be determined according to the purpose pursued by the processing. When this purpose is achieved, the data must either be deleted or be subject to intermediate archiving when their retention is necessary for compliance with legal obligations or for pre-litigation or litigation purposes. These data must then be placed in intermediate archiving, for a period not exceeding that necessary for the purposes for which they are kept, in accordance with the provisions in force. Thus, after sorting the relevant data to be archived, the data controller must provide, for this purpose, a dedicated archive database or a logical separation in the active database. This logical separation is ensured by the implementation of technical and organizational measures guaranteeing that only persons having an interest in processing the data due to their functions, such as persons from the legal department, can access it. Beyond these retention periods for data placed in intermediate archives, personal data must be deleted.49. In this case, the Restricted Committee recalls that the purpose of the collection by company X of the personal data of candidates is to allocate housing. Once this purpose is achieved, the personal data of candidates who have not accessed the rental can no longer be kept for more than three months, within the active database and beyond that be subject to logical separation or even intermediate archiving.50. However, the Restricted Committee observes that the company indicated to the CNIL delegation during the control mission of September 13, 2018 that the documents transmitted by the candidates who did not have access to the rental, that is to say those for which continued processing was no longer justified were not deleted and no purge was implemented in the database. It further notes that, in its observations in defence, the company produced a document from which it appears that its policy on the retention of customer and prospect data was only formalized in November 2018. Finally, during the session of April 11, 2019, the company indicated that the implementation of an archiving solution for the documents in question was in progress. 51. It appears from these various elements that company X kept the data of a personal nature of candidates who have not accessed the rental for a period exceeding in significant proportions that necessary to achieve the purpose of the processing, namely the allocation of accommodation, without any intermediate archiving solution n has been put in place.52.In view of all of these elements, the Restricted Committee considers that a breach of the obligation to retain data, as provided for in Article 5 of the Regulation, is established.

III .On sanctions and publicityArticle 45-III 7° of the law of January 6, 1978 provides: When the data controller or its subcontractor does not comply with the obligations resulting from Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 mentioned above or of 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, as the case where appropriate in addition to a formal notice provided for in II, seize the restricted formation of the committee with a view to the pronouncement, after adversarial procedure, of one or more of the following measures:[…]: 7° With the exception in 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 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 the European Parliament and of the Council of April 27, 2016 mentioned above, 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. Article 83 of the GDPR provides that Each supervisory authority shall ensure that the administrative fines imposed under this Article for infringements of this Regulation referred to in paragraphs 4, 5 and 6 are, in each case, effective, proportionate and dissuasive. 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) 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 under Article 40 or certification mechanisms approved under Article 42; and (k) any other aggravating or mitigating circumstances applicable to the circumstances of the case, such as financial benefits obtained or losses avoided, directly or indirectly, as a result of the violation.54.The company considers that an administrative fine of 900 000 euros is disproportionate taking into account the criteria set by Article 83 of the Rules, his financial capacity and the sanctions previously imposed by the Restricted Committee. It then recalls that neither the GDPR nor the Data Protection Act provide for rules regarding the maximum amount of the fine that may be imposed by the supervisory authority when the shortcomings identified are punished for one, a fine of up to 10 million euros or 2% of the worldwide annual turnover and, for the other, a fine of up to 20 million euros or 4% of worldwide annual turnover.55. First of all, the Restricted Committee considers that in the present case, the aforementioned breaches justify the imposition of an administrative fine on the company for the following reasons.56. On the one hand, it recalls that faced with the risks represented by personal data breaches, the European legislator has intended to strengthen the obligations of data controllers in terms of processing security. Thus, according to recital 83 of the GDPR, In order to guarantee security and to prevent any processing carried out in violation of this Regulation, it is important that the controller or the processor assesses the risks inherent in the processing and implements measures. to mitigate them, such as encryption. These measures should ensure an appropriate level of security, including confidentiality, taking into account the state of knowledge and the costs of implementation in relation to the risks and the nature of the personal data to be protected. As part of the data security risk assessment, account should be taken of the risks posed by the processing of personal data, such as destruction, loss or alteration, unauthorized disclosure of personal data transmitted, stored or processed in any other way or unauthorized access to such data, accidentally or unlawfully, which is likely to cause physical or material damage or moral damage. However, the Restricted Committee observes that the security defect which made the data breach possible originated in a faulty design of its site by company X. The implementation of an authentication procedure on the site was a elementary measure to be taken, which would have made it possible to avoid the violation of personal data.57. On the other hand, the Restricted Committee notes that company X lacked diligence in correcting the vulnerability, whereas in the presence of a data breach, the GDPR requires a rapid reaction. It is thus provided in recital 85 that A breach of personal data risks, if one does not intervene in time and in an appropriate manner, to cause the natural persons concerned physical, material or moral damage […] . Even though no natural person has, to date, reported having suffered damage as a result of the data breach, the company's lack of promptness in correcting the vulnerability, for a period of

at least six months , has had the effect of prolonging the risk of such damage occurring. Then, the seriousness of the breaches must also be assessed with regard to the categories of data concerned. In this respect, the Restricted Committee recalls that the data processed by the company in the context of the management of the files of candidate tenants contains particularly precise information on certain aspects of their private life. As soon as it receives this type of data, the company must pay particular attention to the preservation of their confidentiality and their storage methods; however, it did not provide for an intermediate database and kept this data for a manifestly excessive period of time. total amount of the fine cannot exceed the amount set for the most serious violation. In this case, insofar as the company is accused of a breach of Article 5 of the Regulations, which may be subject to a fine of up to 20 million euros or 4% annual worldwide turnover, it is this maximum amount that should be taken into consideration. GDPR and the financial situation of the company, considers that an administrative fine of 400,000 euros is justified and proportionate, as well as an additional sanction of publicity for the same reasons.FOR THESE REASONSThe restricted formation of the CNIL, after having deliberated, decides: to reject the request for nullity raised by company X; to reject the request of company X not to take into consideration the elements resulting from the procedure followed against company Y; to rule against of company X, an administrative fine in the amount of 400,000 (four hundred thousand) euros; to make public, on the CNIL website and on the Légifrance website, its deliberation which will be anonymized at the end of a period of two years from its publication. The President Alexandre LINDEN This decision may be appealed to the Council of State within two months of its notification.