Deliberation SAN-2018-012 of December 26, 2018 National Commission for Computing and Liberties Legal status: In force Date of publication on Légifrance: Thursday, December 27, 2018 Deliberation of the restricted committee no. SAN-2018-012 of December 26, 2018 pronouncing a sanction pecuniary against the company XLThe 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 Directive 95/46/ EC of the European Parliament and of the Council, of October 24, 1995, relating to the protection of individuals with regard to the processing of personal data and to the free movement of such data; o 78-17 of January 6, 1978 relating to data processing, files and modified freedoms, in particular its articles 45 and following; Having regard to decree no. 17 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. of data processing and freedoms; Having regard to decision no. all the processing of personal data accessible or having been accessible from the domain […]; Having regard to the decision of the President of the National Commission for Computing and Liberties appointing a rapporteur before the restricted committee, in dated October 1, 2018; Having regard to the report of Mr. François PELLEGRINI, rapporteur auditor, notified to company X on October 5, 2018; Having regard to the written observations of the board of company X received on October 31, 2018; Having regard to the rapporteur's response to observations of company X, notified on November 15, 2018 to the board of the company; Having regard to the new written observations of the board of company X received on November 29, 2018 as well as the oral observations made during the restricted training session; Having regard to the other documents in the file; Were present at the restricted training session of December 13, 2018: Mr. François PELLEGRINI, auditor, in his report; As representative of company X:[…] The representatives of company X having spoken last; Adopted the following decision: Facts and procedure Company X is a telecommunications operator French sis […]. 90.5% of the company's capital is held by group Y and 9.5% by group Z. The company has approximately 7,000 employees and 17.8 million customers (14.4 million customers for mobile telephony and 3.4 million box customers). In 2017, it achieved a turnover of more than 5 billion euros, for a net profit of 260 million euros. As part of its commercial activity, it publishes and manages the xxx website and offers its customers, on this platform, the possibility of connecting to a personal space in order, in particular, to edit administrative documents related to their contract, including invoices. On March 2, 2018, the National

Commission for Information Technology and freedoms (hereinafter the CNIL or the commission) has been informed, in the context of a report, of the existence of a security defect on the xxx website. This email reported the possibility of accessing documents containing personal data of the company's customers from several URL addresses with an identical structure. On March 6, 2018, company X notified the CNIL of the breach data using the form made available by the commission. On March 9, 2018, pursuant to decision no. inspection at the premises of company X. During this inspection, the delegation was informed that the company had been notified of the data breach by a message sent to its institutional account on the social network Twitter. of the report, the company's teams reproduced the incident: the URL addresses composed as followsxxxx, where X represents an integer, made it possible to display a customer's subscription contract. From this URL, and by modifying the value of X , it was possible to display the contract of another client. The data concerned by the violation was contained in a table, entitled archived_contract_invoice , composing the MySQL database from the company's website. Of the 2,788,289 rows in the table, the company said the breach only allowed access to data in 2,176,236 rows targeting […] customers, not including X customers or business customers. first series of measures was deployed on March 5, 2018 to prevent access to data, before the technical teams discovered the exact origin of the vulnerability and remedied it. During the on-site check of March 9, 2018, the delegation noted that it was effectively no longer possible to display the contracts and invoices accessible from the aforementioned URLs. The check revealed that entering several URL addresses composed as follows https://www.[...].fr/archived/index/printcontract/archived_id/X returned an error message whether , or not, a user connected to his customer area. The data had therefore effectively been made inaccessible. Asked about the date on which the security flaw had appeared, the company explained that the vulnerability had its origins in the merger of the X and […] brands and the corresponding computer systems, in 2015 A database specific to former customers […] has been kept by the company in order to allow these customers and former customers to access their contracts and invoices. This is the database affected by the data breach. During testing following the merger of these databases, the computer code that required authentication to the xxx website was disabled . Due to human error committed by a person acting on behalf of the company, this code was not reactivated following the tests carried out. appointed Mr. François PELLEGRINI as rapporteur, on October 1, 2018, on the basis of article 46 of the amended law of January 6, 1978 relating to data processing, files and freedoms (hereinafter law of January 6, 1978 1978 amended or Data Protection Act). At the end of his investigation, the rapporteur notified Company X on October 5, 2018 of a report detailing the breaches of the law that he considered constituted in this case and proposed to the

restricted formation of the CNIL to pronounce a financial penalty of five hundred thousand (500,000) euros which would be made public. This report was accompanied by a notice of meeting for the restricted training session of December 13, 2018 and invited the company to submit observations in response within one month. On October 31, 2018, the company, through of his adviser, produced written observations to which the rapporteur replied on the following November 15 pursuant to the provisions of article 75 of decree no. 2005-1309 of October 20, 2005 as amended. In his response, the rapporteur proposed to reduce the sanction imposed to an amount of two hundred and fifty thousand (250,000) euros. On November 29, 2018, through his counsel, the company produced new observations in response to those of the rapporteur. She orally reiterated all of her observations before the Restricted Committee on 13 December 2018. Reasons for the decision On the breach of the obligation to ensure the security and confidentiality of data Article 34 of the law of 6 January 1978 as amended, in the version applicable on the day of the findings, 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, 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. As a preliminary point, the company explains that Article 34 of the aforementioned Data Protection Act imposes on the data controller an obligation of means and not of result. It considers that in this case, it has not committed any breach of its obligations insofar as the data breach of which it has been the victim does not result from the insufficiency of the measures it would have taken in terms of security. but from human error. It considers that the rapporteur's reading of Article 34 amounts to making a data controller responsible for any breach of personal data, regardless of the circumstances in which this breach occurred, and places a burden on him an obligation of result in terms of safety. The Restricted Committee recalls that pursuant to the aforementioned Article 34, it is indeed up to the Restricted Committee to decide whether Company X has breached its obligation to take measures sufficient to ensure the security of the personal data contained in its information system, and in particular those of the users of the xxx website. The Restricted Committee notes in this respect that company X does not dispute either the fact that the personal data it processes have been freely accessible through the URL addresses mentioned, or the origin of this data breach. place, on the protection measure put in place, the company considers that it has complied with the rules of the art by setting up, at the time of the merger of its information systems, a mechanism making it necessary to authenticate the user before allowing him to access the data on the website xxx. It considers that a second protective measure, such as making URL addresses unpredictable or difficult to read, is not a practice imposed either by the texts or by the state of the art. On this point,

the Restricted Committee notes that the aforementioned Article 34 is not prescriptive as to the measures to be deployed by data controllers to guarantee the security of processing as long as the obligation is, ultimately, complied with. The Restricted Committee thus considers that although a measure aimed at making URL addresses unpredictable may appear appropriate and proportionate in this case, given the amount of personal data accessible, the need to protect them, and the fragility induced by the existence of predictable URL addresses, this measure is not actually mandatory, other measures can ensure equivalent protection of the data processed. The precautions to be taken to preserve the security of the data are the responsibility of the data controller. The Restricted Committee notes that in this case, company X has chosen not to implement any additional measure to the authentication users of the xxx website. Consequently, the Restricted Committee considers that this choice imposed on the company a particularly reinforced obligation with regard to the vigilance that should be given to this unique security measure. Secondly, on the attention paid to the measurement of protection in place, the company claims to have carried out numerous audits and security tests in order to test the protection of the personal data it processes. These tests were carried out each year, both directly by the company and through external service providers, between 2015 and 2018. It recalls that none of these tests made it possible to discover the vulnerability making the data accessible. explains the lack of effectiveness of these tests due to the method used: it indicates that dummy user accounts are created during these tests in order to simulate the actions that can be performed by a real user, and that these accounts must be regularly generated to adapt the tests to the evolution of the computing environment. The accounts used for the tests carried out therefore proved to be unsuitable for identifying the vulnerability since only customer accounts […] created between July 2011 and December 2014 could reveal the vulnerability here in question. The company also claims that it was materially impossible to effectively carry out a manual review of the […] lines that made up the computer code of its website. from its website, it notes that these tests were not adapted to the specificities of the inherited database and that they could not lead to the discovery of the vulnerability. These tests were therefore ineffective in this case. Similarly, if the Restricted Committee could accept that a manual review of all the code of the company's website may not be proportionate with regard to the number of lines making up this code, the Restricted Committee nevertheless considers that the particular attention to be paid to the authentication mechanism required a manual review of the code relating solely to this critical element. Such a measure does not appear to be disproportionate in this specific case, both with regard to the human and technical resources available to company X and the risks incurred by the more than two million people affected by the violation. The Restricted Committee

notes in besides that the commented code specifically included the indication that it should be deleted at the end of the test phase. A manual review of these lines would thus have immediately allowed the discovery of the error at the origin of the vulnerability. The Restricted Committee therefore considers that, if forgetting to reactivate the code making it necessary to authenticate users on the site the company's website is indeed a human error, from which the company cannot completely protect itself, the fact of not having implemented, for more than two years, effective measures to discover this error constitutes a violation of the obligations imposed by Article 34 referred to above. Automated code review measures adapted to the specificities of the inherited information system and a manual review of the part of the code in charge of authentication would have made it possible to discover the vulnerability and to remedy it. The Restricted Committee therefore considers , that the company has not paid the necessary attention to the database in question to ensure the security of the personal data processed. On the sanction and publicity Under the terms of I of article 45 of the law of January 6, 1978 as amended, 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 National Commission for Computing and Liberties may give him formal notice to put an end to the breach noted 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 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 company considers that the amount of 250,000 euros proposed by the rapporteur is not justified insofar as the data concerned by the breach are not sensitive data, that it reacted promptly by taking the necessary measures to limit the impact of the violation, that the violation did not cause any harm to the persons concerned and that it cooperated with the CNIL. The Restricted Committee notes that company X was very responsive in setting up a unit crisis and the deployment of measures aimed at making the personal data concerned inaccessible. The speed of the correction is necessarily taken into account by the restricted committee to moderate the amount of the sanction, although moreover, it also demonstrates the simplicity of the vulnerability at the origin of the data breach.The restricted committee also notes that the company has implemented a large number of measures to minimize the impact of a possible data breach for its customers, in particular the reminder of good practices and the provision of sheets containing advice for its customers , the fight against phishing, the monitoring of the dark web and the training of its employees.Nevertheless, the Restricted Committee considers that the seriousness of the violation is characterized by the number of data and persons concerned by the violation as well as by reason for its duration. It points out that the data breach affected more than two million users, a very large number of people, and data. identifiers such as surname, first name, date of birth, e-mail address, physical address, mobile phone number. It also notes that the period during which, due to a lack of appropriate vigilance, the data was freely accessible and without control was particularly long (more than two years and three months). It then recalls that the fact that the accessible data does not contain any data that can be qualified as sensitive, within the meaning of Article 8 of the Data Protection Act, has no influence on the characterization of the breach of the obligation incumbent on a responsible processing to ensure the security of the data it processes. In view of the elements developed above, the facts observed and the breach constituted in article 34 of the law of January 6, 1978 as amended justify the imposition of a sanction of an amount of 250,000 (two hundred and fifty 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 those responsible of processing and Internet users as to the risks weighing on data security, it is necessary to make its decision public, in accordance with article 46 of the law of January 6, 1978. BY THESE REASONSThe Restricted Committee of the CNIL, after having deliberated, decides:to pronounce against company X a pecuniary penalty in the amount of 250,000 (two hundred and fifty thousand) euros;to make public its deliberation on the CNIL site and on the Légifrance site, which will be anonymized at the end of a period of two years from its publication. President Jean-François CARREZ This decision may be

subject to appeal before the Council of State within two months of its notification.