Deliberation SAN-2018-008 of July 24, 2018 National Commission for Computing and Liberties Legal status: In force Date of publication on Légifrance: Thursday August 02, 2018 Deliberation of the restricted committee no. SAN-2018-008 of July 24, 2018 pronouncing a sanction compensation against the company xThe National Commission for Computing and Liberties, meeting in its restricted formation composed of Mr. Jean-François CARREZ, Chairman, Mr. Alexandre LINDEN, Vice-Chairman, Ms. Dominique CASTERA and Mr. Maurice RONAI, members; Having regard to Convention No. 108 of the Council of Europe of January 28, 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 relating to data processing, files and freedoms, modified by law n° 2011-334 of March 29, 2011, in particular its articles 45 and following; Considering decree n° 2005-1309 of October 20, 2005 taken for application of Law No. 78-17 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. 2013-175 of July 4, 2013 adopting the internal regulations of the National Commission Information Technology and Liberties; Having regard to Decision No. 2016-357C of December 8, 2016 of the President of the National Commission for Informatics and Liberties to instruct the Secretary General to carry out or have carried out a verification mission with company X: Having regard to the decision of the President of the National Commission for Computing and Liberties appointing a rapporteur to the restricted committee, dated May 9, 2017; Having regard to the report of Mr. François PELLEGRINI, commissioner-rapporteur, notified to company X on April 24, 2018; Having regard to the request for a closed session presented by company X on June 5, 2018 which, by letter of June 11, 2018, was not granted; Having regard to the observations letters from company X received l on June 5, 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 June 14, 2018: Mr. François PELLEGRINI, Statutory Auditor, in his report; As representatives of company X:[…];[…];[…];As counsel for company X:[…];[…]. Mrs. Nacima BELKACEM, Government Commissioner, having made no observations;The representatives of company X having spoken last;Adopted the following decision:Facts and procedureOn-site inspection procedureCompany X (hereinafter the company ) is a public limited company located […], which offers a platform for hosting video content created by users. Between 260 and 300 million users visit this platform each month and the content posted online enjoys around 3 billion monthly views. In 2016, it achieved a turnover of 58,809,200 euros. passwords of users of the company's video sharing platform. On December 15, 2016, pursuant to decision no. the CNIL or the Commission), a delegation from the Commission carried out an inspection mission within the premises of the company. On the

occasion of this inspection, the company indicated to the delegation that it had been alerted to the existence of the data breach by an email addressed to the Deputy Chief Executive Officer of the company on December 5, 2016. It also confirmed that the data breach affected 82.5 million account addresses as well as 18.3 million encrypted passwords extracted from user tables (users) and user_password (users password) from the company's database. The company said it identified the data breach on December 6, 2016, following its disclosure by the website [… ] . She told the delegation that the attack was due to the execution of a SELECT-type SQL query; that this query was executed on the user and user_passwords tables; that the data was retrieved from a machine with an IP located on American territory; […] The company also indicated that given that the volume of data downloaded was low in proportion to the capacities of the bandwidth, no alerts were raised during the extraction of data. It specified that in response to this attack, it had immediately put in place several measures to strengthen the security of its information system, in particular […]. The delegation was told that it had not put in place a complex password policy for marketing reasons and that, apart from cases where a request to delete an account is made, the retention period user data was not limited. The company also explained that it used the services of the platform […] in order to improve the security of its processing and that security audits were carried out every quarter. Finally, the company indicated that it did not had not been the victim of a particular blackmail linked to this vulnerability, that the value on the internet of the database attacked would be 11 euros and that all users had been informed of the incident. these elements, the President of the Commission appointed Mr. François PELLEGRINI as rapporteur, on May 9, 2017, on the basis of Article 46 of Law No. 78-17 of January 6, 1978, as amended, relating to information technology , 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 Company X on July 3, 2017 of a report detailing the breaches of the law that he considered constituted in this case and proposed to the restricted committee to impose a pecuniary 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 committee meeting of September 21, 2017 and invited the company to submit observations in response within a period running until September 7, 2017. Following receipt of this report, the company sent observations in response by letter dated September 6, 2017. These observations brought to light many new elements as to the course of the alleged acts, in particular on the fact that the security incident was not the result of a SQL injection, contrary to what had been initially indicated to the delegation of control. , which was accepted. The company was informed of this report by letter of the same day.Additional investigations.As part of his additional investigations, the rapporteur, on October

26, 2017, sent the company a questionnaire relating to the data breach, to which the company responded by letter dated November 23, 2017. Then, the rapporteur interviewed the company's representatives at the CNIL premises on February 15, 2018. During these investigations, the company explained that the security incident resulted from a multi-stage attack, carried out by experienced computer criminals, after a coordinated approach over several months and likely by several people. She specified that this attack was the result of the combination of six factors , namely: fraudulent access to the company's source code; the identification of a maliciously exploitable bug within the platform's hundreds of thousands of lines of code e X; the development of an understanding of the architecture of the platform allowing to identify the necessary and sufficient conditions for the malicious exploitation of the bug; the development of a specific exploitation code capable of triggering and pulling advantage of the bug; the ability to hijack an administration account to exploit the identified bug; the propagation of the intrusion from the web servers to data while masking its real identity by a set of bounces to servers rented specifically for these purposes. The company clarified that the source code stored within the Github platform contained a service account with administrative privileges and that it was used to perform non-regression tests.[…] Finally, it indicated that as of February 15, 2018, none of its users had reported any damage following the security incident. In view of the information provided by the company to the rapporteur, the latter has prepared a new report, replacing its initial report, proposing that the restricted committee pronounce a pecuniary sanction which may not be less than one hundred thousand (100,000) euros and which would be made public. This report was notified to the company on April 25, 2018 and was accompanied by a notice to attend the restricted training session of June 14, 2018, indicating to the company that it had one month to communicate its written observations. By letter dated June 5, 2018, company X produced written observations on the report, reiterated orally during the restricted committee session of June 14, 2018. Reasons for the decision On the breach of the obligation to ensure the security and confidentiality of data. Article 34 of the amended law of January 6, 1978 provides that the controller is required to take all necessary 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, prevent them from being distorted, 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 the present case, it has not committed any breach of its obligations insofar as the fraudulent extraction of the data of which it was the victim does not result from the inadequacy of the measures it would have taken in terms of security but a particularly sophisticated attack. 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 technical circumstances in which this breach occurred. considers that the aforementioned Article 34 places the responsibility of the data controller to implement appropriate means to ensure the security of the personal data contained in its information system and in particular those concerning the users of its web platform, in particular so that this data is not accessible to unauthorized third parties. It is therefore up to the restricted committee to decide whether company X has breached its obligation to take sufficient measures. the presence of the password within the source code, the company explains that it relates to a service account with particular functions. eras. The company said that this service account was intended to simulate an administrator in order to test the validity of administrative features. She explains that these tests would not have been possible by writing the password in the source code in a hashed form, because the password must necessarily be written in the clear in the source code so that the service account can to log in. It therefore considers that the presence of this password in the source code is not contrary to the state of the art. The Restricted Committee considers that in terms of authentication, it is important to ensure that a password allowing authentication on a system cannot be disclosed. Thus, it is imperative that it not be stored in an unprotected file. If it were necessary, for the proper conduct of tests relating to the service account, that the password associated with this account be entered clearly in the source code, this circumstance cannot, however, justify, according to the Restricted Committee, the constant presence of the password in the source code. Since it was impossible for the company to keep the password in the source code in a hashed form, it was up to them to find another solution so as not to make it accessible, for example, by storing it within its internal network and by ensuring that it was injected in real time into the source code, only during the test phases and then deleted once the test was completed. external to the administration of the information system, the company explains that from its creation, the X platform was designed to allow users outside the internal network, in this case the company's partners, to have access rights. administration in order to be able to add or remove content. In this regard, the company has indicated that the data extracted from its server was transmitted to an external server with an IP address located on the territory of the United States of America. The Restricted Committee considers that when employees are required to connect remotely to the internal computer network of a company, securing this connection is an elementary precaution in order to preserve the integrity of said network. This security can, for example, be based at least on the implementation of an IP address filtering measure so that only requests from identified and authorized IP addresses are executed or by the use of a VPN, which makes it possible to avoid any illicit connection, by

securing data exchanges and authenticating users. The Restricted Committee notes that in this case, the company deployed a measure to secure access to its information system after the discovery of the attack […]. However, the implementation of this measure from the design of the platform would have prevented the attacker from having access to the administration interface from the Internet. combination of several factors, some of which are not attributable to the company, it nevertheless considers that this attack could not have succeeded if at least one of the two measures detailed above had been taken by the company. Finally, the company points out that the principle of the legality of offenses and penalties requires that the constituent elements of an offense be defined in sufficiently clear and precise terms. It considers that in this case, Article 34 of the Data Protection Act is incomplete as regards the type of measures to be taken by the data controller. The Restricted Committee recalls that the legislator has entrusted the data controller with the choice of specific measures to be put in place to comply with the general obligation drawn from the aforementioned article 34. Consequently, the text is not prescriptive as to the measures to be deployed to guarantee the security of processing, as long as the obligation is ultimately respected. On the basis of these elements, the Restricted Committee considers that the breach in article 34 of the amended law of January 6, 1978 is constituted when the company has not taken all the necessary precautions to prevent unauthorized third parties from having access to the data processed. under the terms of I of article 45 of the amended law of 6 January 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 National Commission IT and Liberties may put him on notice to put an end to the observed breach within a time limit that he sets. In cases of extreme urgency, this period may be reduced to twenty-four hours. If the data controller complies with the formal notice sent 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 reports, specify that: The amount of the financial penalty provided for in I of article 45 is proportionate to the gravity 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 with regard to the criteria set by article 47 of the amended law of January 6, 1978, the amount of 100,000 euros proposed by the rapporteur is disproportionate. It recalls that the attack of which it was the victim is not not the result of negligence on its part, that it immediately took measures to mitigate the negative effects, that it cooperated fully with the services of the CNIL and that the only personal data concerned are e-mail addresses, some of which are not identifying because they are not associated with natural persons but with test accounts or the names of partner companies. It also recalls that it did not derive any advantage from the breach and that it received no complaints from its users. The Restricted Committee notes that in certain aspects, the attack suffered by the company can be qualified of sophisticated. It also notes that the reduced number of categories of data extracted, in this case, e-mail addresses and encrypted passwords, is likely to reduce the risk of invasion of the privacy of the persons concerned. In addition, it notes that the company has shown cooperation with the services of the CNIL. However, the Restricted Committee considers that the company has been negligent in that certain elementary security measures have not been taken, allowing thus the success of the attack. Furthermore, notwithstanding the categories of data concerned, the Restricted Committee notes that the company does not provide any element allowing it to significantly minimize the number of 82.5 million e-mail addresses. It therefore considers that the volume of data impacted by the breach is considerable. With regard to the elements developed above, the facts found and the failure to comply with Article 34 of the law of January 6, 1978 as amended justify the imposition of a penalty in the amount of 50,000 (fifty thousand) euros. Finally, the Restricted Committee considers that in view of the very large amount of data in question, the current context in which security incidents are on the increase and the need to make Internet users aware of the risks weighing on the security of their data, it there is reason to make its decision public. FOR THESE REASONS The Restricted Committee of the CNIL, after having deliberated, decides: financial penalty of fifty thousand (50,000) 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 subject to appeal before the Council of State in a period of two months from its notification.