Deliberation SAN-2018-011 of December 19, 2018 National Commission for Computing and Liberties Legal status: In force Date of publication on Légifrance: Thursday, December 20, 2018 Deliberation of the restricted committee no. SAN-2018-011 of December 19, 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, Chairman, Mr. Alexandre LINDEN, Vice-Chairman, Ms. Dominique CASTERA, Ms. 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 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data; Having regard to the law no. 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. ° 78-17 of January 6, 1978 relating to data processing, files and freedoms, modified by decree n ° 2007-451 of March 25, 2007; Considering the deliberation n ° 2013-175 of July 4, 2013 adopting the regulation of the National Commission for Computing and Liberties; Having regard to decision no. 2017-279C of 8 December 2017 of the President of the National Commission for Computing and Liberties to instruct the Secretary General to proceed or to to a mission of verification of all the processing of personal data relating, in whole or in part, to data relating to the marketing or use of products or services attached to the brand […]; Having regard to the decision of the President of the National Commission for Information et des libertés appointing a rapporteur before the restricted committee, dated June 13, 2018; Having regard to the report of Mr. François PELLEGRINI, commissioner rapporteur, notified to company X on August 6, 2018 and sent for information to companies Y and Z; Having regard to the written observations of companies X, Y and Z received on September 24, 2018; Having regard to the rapporteur's response to the observations of companies X, Y and Z, notified on October 9, 2018; Having regard to the new written observations of companies X, Y and Z received on October 23, 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 November 8, 2018: Mr. François PELLEGRINI, Statutory Auditor, in his report; As representative of company X:[…] As representative of company Y:[…] As advisor to companies X, Y and Z:[…][…][…][…][…] As interpreter:[…] Mrs. Eve JULLIEN, Deputy Government Commissioner, having made no comments; The representatives of company X having spoken last; Adopted the following decision:Facts and procedureCompany Z, founded in 2009 and whose head office is located at […], has as its main activity the transport of people with driver, known as VTC, via a

web platform and a mobile application. In order to offer this service in other countries, several subsidiaries have been created around the world, including company Y, located at […] and company X, located […]. The company […] has approximately 16,000 employees. In 2017, it achieved a turnover of approximately 6 billion euros. On November 21, 2017, company Z published an article on its website stating that at the end of 2016 , two individuals outside the company had accessed the data of 57 million users of the services […] worldwide. This information was then repeated in numerous press articles, some of which reported that the company had paid the attackers the sum of 100,000 US dollars so that they destroy the data in question and that they do not reveal the existence of this incident. On November 28, 2017, company Y sent a letter to the President of the Article 29 Data Protection Working Party (hereinafter G29) informing her of the circumstances of the breach of data and its willingness to cooperate with all the competent authorities on this case. On November 29, 2017, the G29 Plenary Assembly mandated the creation of a working group called taskforce with the aim of coordinating the investigation procedures of different data protection authorities. This working group is made up of the Dutch, Spanish, French, Belgian, Italian, British and Slovak authorities. Pursuant to decision no. (hereinafter the CNIL or the Commission), a delegation from the CNIL sent on December 22, 2017 to companies Z and Y (hereinafter the company […] or the company ) a questionnaire relating in particular to the circumstances of the violation of data and on the measures taken by the companies to ensure the security of the data processed. On January 22, 2018, the company replied to the questionnaire, explaining that the data breach took place in three stages. First, the company clarified that outsiders have been granted access to a private workspace […] on GitHub. GitHub is a third-party web-based software development platform that was being used by software engineers at […] at the time of the incident to store code for collaboration and development. She mentioned that […] engineers log into GitHub using a username and password set up by themselves. These identifications took the format of a personal email address as a user name and an individual password. She clarified that the platform was used by […] engineers and that there was no process for removing clearances when an engineer leaves the company.Secondly, the company indicated that the attackers used these credentials to connect to the GitHub platform and had found an access key written in the clear in a source code file. This access key related to a service account allowing access to the hosting platform […] where the personal data of users of the services […] are stored. Third, the company explained that the attackers had used this access key to access the company's databases […] stored on the servers […], and thus download a significant amount of personal data. The company explained that the data breach affected 57 million users worldwide, including 1.4 million in France. Among these users were 1.2 million passengers

and 163,000 drivers. The company clarified that the attackers had access to the following data: surname, first name, email address, city or country of residence, mobile phone number and user status (driver, passenger or both). Finally, the company explained that following the data breach, it had put in place […] For the purpose of examining these elements, the President of the Commission appointed Mr François PELLEGRINI as rapporteur, the June 13, 2018, on the basis of article 46 of the amended law of January 6, 1978 relating to data processing, files and freedoms (hereinafter amended law of January 6, 1978 or Data Protection Act). At the end of his investigation, the rapporteur notified company X on August 6, 2018, and communicated for information to companies Y and Z, 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 pecuniary sanction of four hundred thousand (400,000) euros which would be made public. This report was accompanied by a notice of meeting for the restricted training session of October 11, 2018 and invited the company to submit observations in response within a period running until September 24, 2018. By letter dated October 2, 2018, the company was informed that the meeting of the Restricted Committee was postponed to November 8 following. provided for by Article 75 of Decree No. 2005-1309 of October 20, 2005 as amended. On October 23, 2018, the company produced new observations in response to those of the rapporteur. Reasons for the decision On the quality of data controller for companies Z and YLe I of article 3 of the modified law of January 6, 1978 provides that the person responsible for the processing of personal data is, unless expressly designated by the legislative provisions. or regulations relating to this processing, the person, public authority, service or body which determines its purposes and means. This provision constitutes the transposition of Article 2 d) of the Directive which defines the data controller. processing as the natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data. Company […] argues that only company Y can be considered as data controller and that company Z acts only as a subcontractor of company Y. It recalls that all the tasks performed by Z in the context of the processing fall within the leeway that this company has, as a processor, in the way the data processing is carried out. It recalls that a subcontracting agreement was concluded between the two companies and that it is as a subcontractor that company Z drew up guidelines concerning data management, that it provides training for new employees of the group, that it has signed contracts with third-party companies and that it has managed the consequences of the data breach. Firstly, the Restricted Committee notes that Y's status as data controller is not not contested.Secondly, the Restricted Committee recalls that according to Opinion No. 1/2010 of the G29 of February 16, 2010 on the notions of controller

and processor, a processor who acquires an important role in the determination of the essential purposes or means of processing is more a (co-)controller than a processor. The opinion of the G29 specifies that the notion of data controller is based on a factual analysis rather than a formal one. It also notes that this opinion states that while the determination of the purpose of the processing would systematically carry the qualification of controller of the processing, the determination of the means would imply liability only when it relates to the essential elements of the means. The Restricted Committee also notes that it appears from the documents in the file that the proposed service constitutes a unique application designed and developed in the United States by company Z, an application which was subsequently offered in other regions of the world, by being, as necessary, simply adapted according to the laws of the States. The restricted committee notes in particular that it is indeed the company Z which managed the consequences of the data breach. In particular, it is the Z teams that […]. Company Y did not intervene during this process even though the data breach concerned in part data relating to users of the application […] located on the territory of the European Union, territory for which the Company Y is however described in the observations as the sole data controller. The Restricted Committee further notes that it is company Z […]. Finally, it is company Z which, through an article published by its general manager, revealed the existence of the breach to the public. The Restricted Committee considers that the management of the consequences of the data breach n t is not a simple technical or organizational question that can entirely fall within the room for maneuver available to a subcontractor. On the contrary, the management of a data breach is a question attached to an essential element of a means of treatment, of which the data controller cannot be removed. To this end, company Z has drafted several key documents relating to the management of the personal data collected, including the directives which are applied by all the entities of the group […]. It is also this entity that is in charge of training new group employees. The Restricted Committee also points out that it is company Z which has entered into contracts with several third-party companies, including […], which provide tools essential to the operation of the service, such as those allowing the management of marketing campaigns. The Restricted Committee considers that the multitude of fields of action in which company Z intervenes testify to the decisive role which it plays in determining the purposes and means of the processing. Consequently, companies Y and Z must be jointly qualified as data controllers. On the applicable law Article 5 I of the amended law of 6 January 1978 provides that the processing of personal data is subject to this law. : 1° Whose manager is established on French territory. The data controller who carries out an activity on French territory within the framework of an installation, whatever its legal form, is considered to be established there. This article constitutes the

transposition into domestic law of Article 4-1-a) of Directive 95/46/EC of 24 October 1995 on applicable national law which provides that: 1. Each Member State applies the national provisions that it stops pursuant to this Directive to the processing of personal data when: a) the processing is carried out within the framework of the activities of an establishment of the controller on the territory of the Member State; if the same controller is established in the territory of several Member States, he must take the necessary measures to ensure that each of his establishments complies with the obligations provided for by the applicable national law. With regard to these provisions, the applicable law of a Member State depends on two cumulative conditions: the existence of an establishment of the controller on the territory of a Member State and the implementation of the data processing in the framework of the activities of this establishment. With regard to the first criterion, the Restricted Committee recalls that in its judgment Weltimmo, of October 1, 2015, the Court of Justice of the European Union specified that the notion of establishment, within the meaning of Directive 95/46, extends to any real and effective activity, even minimal, carried out by means of a stable installation, the criterion of stability of the installation being examined with regard to the presence of human and technical means necessary to the provision of specific services in question (paragraphs 30 and 31 of the judgment). In this case, the Restricted Committee notes first of all that the status of establishment of company X is not disputed. It then notes that this company has stable premises located in France within which its employees are in particular in charge of support activities for drivers and the realization of the group's marketing campaigns on French territory. Restricted training therefore considers, in the light of these elements and in the light of the case law of the Court of Justice of the European Union on the subject, that company X has a stable establishment on French territory by means of which it exercises real and effective activity thanks to the human and technical resources necessary in particular for the provision of the services of companies Y and Z. With regard to the second criterion, the Restricted Committee recalls that in its Costeja judgment of 13 May 2014, the Court of Justice of the European Union has clarified that processing of personal data is carried out in the context of the activities of an establishment when the latter is intended to carry out the activity promotion and sale of advertising space for the needs of a company located in a third country. It notes that in the present case, company X carries out marketing campaigns to promote the services of the company […] and provides a support service to customers and drivers. Consequently, the processing in question must be regarded as being carried out within the framework of the activities of an establishment of the data controllers, which are companies Y and Z. The Restricted Committee concludes that the two criteria provided for in Article 4.1 a) of the directive and article 5. I.1° of the Data Protection Act being fulfilled, French law

applies, including the possibility for the CNIL to pronounce a pecuniary sanction. On the recipient of the measure The company […] considers that the CNIL can only impose a sanction on a data controller and not on a simple establishment to which breaches of the Data Protection Act cannot be attributed. It recalls that in this case, the occurrence of the data breach is solely attributable to Y as controller. It therefore considers that pronouncing a sanction against company X would constitute a manifest violation of the principle of individuality of sentences. The Restricted Committee recalls that the Court of Justice of the European Union ruled in its judgment -Holstein GmbH of 5 June 2018 that when a company established outside the Union has several establishments in different Member States, the supervisory authority of a Member State is empowered to exercise the powers conferred on it by Article 28, paragraph 3, of this directive with regard to an establishment of this undertaking located on the territory of this Member State even though, by virtue of the distribution of tasks within the group, on the one hand, this establishment is solely responsible for the sale of advertising space and other marketing activities in the territory of the said Member State and, on the other hand, the exclusive responsibility for the collection and processing of personal data. personal data is the responsibility, for the entire territory of the Union, of an establishment located in another Member State. This therefore implies that, when a power which a supervisory authority of a Member State wishes to use falls within the scope of this article, it may be exercised with regard to the establishment of the controller located within the territory of that Member State, regardless of the type of power envisaged.Article 28(3) of Directive 95/46/EC of 24 October 1995 on data protection provides that: Each supervisory has in particular: powers of investigation, such as the power to access the data being processed and to collect all the information necessary for the accomplishment of its mission of control, effective powers of intervention, such as, for example, to issue opinions prior to the implementation of processing, in accordance with Article 20, and to ensure appropriate publication of these opinions or to order the blocking, erasure or destruction of data, or i temporarily or permanently prohibit processing, or to issue a warning or admonishment to the controller or to seize national parliaments or other political institutions, […] The scope of the powers available to the supervisory authorities in application of Article 28(3) of the Directive was clarified by the Court of Justice of the European Union in particular in its aforementioned Weltimmo decision. Indeed, in point 49 of its decision, the Court indicated that non-exhaustive nature of the powers thus enumerated and of the type of powers of intervention mentioned in this provision as well as of the room for maneuver available to the Member States for the transposition of Directive 95/46, it must be considered that these powers intervention may include sanctioning the data controller by inflicting, where appropriate, a fine. In domestic law, the possibility for the restricted formation of the CNIL to

pronounce a pecuniary penalty is expressly provided for by article 45 of the Data Protection Act (in the version applicable at the time of the facts) which constitutes the transposition of the provisions of the Article 28(3) of the Directive. The Restricted Committee therefore considers that, insofar as the power to impose a financial penalty falls within the scope provided for by Article 28(3) of the Directive, that this possibility is offered by article 45 of the Data Protection Act and that company X constitutes an establishment of companies Z. and Y, data controllers, it follows from these provisions, as clarified by the case law of the Court of Justice of the European Union, that the power to impose a pecuniary penalty can be exercised against company X. Given, moreover, the nature of the links between company X and those responsible s of the processing, which implement their processing operations within the framework of the specific activities of their French establishment, the pronouncement of a pecuniary sanction against the latter cannot be regarded as disregarding the principle of personality of the sentences. On the breach of the obligation to ensure the security and confidentiality of data the risks presented by the processing, to preserve the security of the data and, in particular, to prevent them from being distorted, damaged, or from unauthorized third parties having access to them. It is up to the Restricted Committee to decide whether the company […] has failed in its obligation to implement appropriate means to ensure the security of the personal data processed and, in particular, those of the users of the service […], in particular so that this data is not accessible to unauthorized third parties. In defence, the company considers that it has not committed any breach of its obligations insofar as, prior to the occurrence of the violation, it had put in put in place sufficient security measures. First of all, with regard to securing access to the GitHub platform, the company believes that it was not negligent in allowing its engineers to use personal identifiers to connect to GitHub. It specifies that this practice is also a recommendation issued by the GitHub platform relating to good practices in project development. She explains that the implementation of a multi-factor authentication measure on GitHub was not mandatory insofar as this platform was not used as an internal tool for the company on which personal data was kept. The Restricted Committee notes that the GitHub platform, being used by […], was a central working tool in the development of the company's activities, access to which should have been governed by adequate security rules. In this case, notwithstanding the recommendation of the GitHub platform, it was up to the company, as data controller, to adopt rules capable of guaranteeing the security of the information stored on GitHub which, if they did not constitute in themselves personal data (these were the access keys to the servers […]), on the other hand allowed direct access to a large quantity of data relating to the users of the service […], since these data was stored on the servers […]. The Restricted Committee notes that the possibility of

implementing a multi-factor authentication measure was set out in the same recommendation as that referenced by the company. […] Finally, the Restricted Committee considers that the absence of a process relating to the withdrawal of authorizations from former engineers constitutes significant negligence since the company was unable to guarantee that people who left the company did not continue to access to projects developed on Github. Next, with regard to the presence in plain text of server access identifiers […] in the source code stored on the GitHub platform, the company explains that this was an incident isolated due to human error. She specifies that at the time of the incident […]. The Restricted Committee recalls that in terms of authentication, it is important to ensure that identifiers allowing secure connection to servers containing a large amount of personal data cannot be disclosed. It is therefore imperative that such identifiers are not stored in an unprotected file. Moreover, the Restricted Committee notes that the company […] itself recommends that users of its services […] not store identifiers directly in code files. The Restricted Committee considers that the company's decision [… ] demonstrates that it was aware, on the one hand, that access identifiers were potentially present in its source code and, on the other hand, that the presence of such information within GitHub was a source of risk. with regard to the lack of secure access to the servers, the company explains […] The Restricted Committee notes that if a measure […]. Finally, the company explains that the implementation of a filtering measure of the IP addresses authorized to access the servers […]. The Restricted Committee considers that when employees are required to connect remotely to the servers used by a company, securing this connection constitutes an elementary precaution in order to preserve the confidentiality of the data processed. This security can, for example, be based at least on the implementation of an IP address filtering measure so that only requests from identified IP addresses are executed, which makes it possible to avoid any illicit connection, by securing exchanges of data and by authenticating users. It considers that, given the very large number of people whose personal data is stored on the servers […], the establishment of an IP address filtering system, even if it required a long development, constituted a necessary effort which should have been planned from the beginning of the use of the services […].[…]. In view of these elements, the Restricted Committee notes that the company was negligent in not implementing certain basic security measures. This general lack of precaution is evident in that the success of the attack carried out by the hackers resulted from a chain of negligence, illustrated by the three stages of the attack. The Restricted Committee therefore considers that the company has not taken all the necessary precautions to prevent unauthorized third parties from having access to the data processed and that the breach of Article 34 of the amended law of January 6, 1978 constitutes .On the penalty and publicityThe Restricted Committee recalls

that this decision concerns a continuous breach which continued after October 7, 2016, the date of entry into force of the Law for a Digital Republic, and which was noted at the occasion of data breach facts. Consequently, the breaches alleged against the company […] must be assessed under the influence of this law, which ensures the transposition into domestic law of Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 (here -after the directive) and which was applicable at the material time.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 person responsible for processing does not 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 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 implemented by the State; 3° An injunction to cease the processing, when it falls under Article 22, or a withdrawal of the authorization granted pursuant to Article 25. When the observed breach 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 The 1st and 2nd paragraphs 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 the benefits derived from this breach. 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 400,000 euros is not justified since 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 it communicated the existence of the violation to the public, that the violation did not cause any prejudice to the persons concerned and that it cooperated with the CNIL. The Restricted Committee recalls that the fact that the data accessible 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 data controller to ensure the security of the data that he treats. It also points out that the data breach affected 1.4 million users, i.e. a very large number of people, and identifying data such as surname, first name, e-mail address, city or country of residence and the mobile telephone number. Furthermore, if no damage suffered by the persons as a result of the data breach has been reported to date, the proof of the total absence of damage cannot be invoked by the society. Moreover, it is established that the attackers seized the data thus leaving them the possibility, although the company maintains, of a subsequent use. article 34 of the amended law of January 6, 1978 justifies the imposition of a sanction in the amount of 400,000 (four hundred thousand) euros. in which security incidents are on the increase and of the need to raise the awareness of data controllers and Internet users of 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. FOR THESE REASONS The Restricted Committee of the CNIL, after having deliberated, decides: to pronounce against company X, acting as an establishment of companies Z and Y, a pec union of an amount of 400,000 (four hundred thousand) euros; to make public its deliberation on the CNIL website and on the Légifrance website, 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.