Deliberation SAN-2019-007 of July 18, 2019 National Commission for Computing and Liberties Nature of the deliberation: Sanction Legal status: In force Date of publication on Légifrance: Thursday July 25, 2019 Deliberation of the restricted committee no. SAN – 2019-007 of 18 July 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. Anne DEBET, Mrs Sylvie LEMMET, 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 the 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 n ° 78-17 of January 6, 1978 mo dified relating to data processing, files and freedoms, in particular its articles 20 and following; Considering the decree n ° 2019-536 of May 29, 2019 taken for the application of the law n ° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms; Having regard to deliberation no. 2013-175 of July 4, 2013 adopting the internal regulations of the National Commission for Data Processing and Freedoms; Having regard to decision no. 2018-136C of 26 June 2018 from the President of the National Commission for Computing and Liberties to instruct the Secretary General to carry out or have carried out a mission to verify any processing accessible from the domain […].fr or relating to personal data collected from the latter; Having regard to the decision of the President of the National Commission for Computing and Liberties appointing a rapporteur to the restricted committee, dated March 8, 2019; Having regard to the report of Mr François PELLEG RINI, commissioner rapporteur, of April 4, 2019; Considering the written observations submitted by company X on May 6, 2019; Considering the observations in response of the commissioner rapporteur of May 16, 2019; Considering the letter from company X of June 11, 2019; Considering the oral observations made during the restricted training session; Considering the other documents in the file; Were present at the restricted training session of June 13, 2019: Mr. François PELLEGRINI, statutory auditor, heard in his report; As representatives of company X: Mr. XMaître Y, lawyer;Maître Z, lawyer;Ms XX;The Restricted Panel heard, pursuant to Article 42 of Decree No. 2019-536 of May 29, 2019, Mr. XY, Technical Director within the company […]. The company that spoke last; After deliberation, adopted the following decision: Facts and procedure Company X (hereinafter the company) is a simplified joint-stock company with an activity as an insurance intermediary, designer and distributor automobile insurance contracts to individuals, for direct sale or online sale. The company employs approximately 160 employees, 150 of whom are located in Madagascar within a branch of the company. In 2018, the

company achieved a turnover of […] euros and a net result of […] euros. Its head office is located […]. For the purposes of its activity, the company publishes the website […], on which people can request quotes or take out motor insurance contracts. The company obtains customers mainly through its website and through car insurance comparators available on other websites. the Commission) was informed by a customer of company X that he had access to the data of other customers without a prior authentication procedure. On June 27, the National Information Systems Security Agency (ANSSI) also notified the CNIL that access to the personal data of users of the company's website was possible without prior control from the engine Duckduckgo research center (https://duckduckgo.com). Pursuant to decision no. 2018-136C of the President of the Commission of June 26, 2018, an online control mission was carried out by a delegation on June 28, 2018 The purpose of this mission was to verify compliance with the provisions of law no. et Libertés) and Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (hereinafter GDPR or Regulation), of any processing accessible from the domain […] or relating to personal data collected from the latter. During this control mission, the delegation noted that a query made within the Duckduckgo search engine using the keywords client.[…] site:client.[…].fr revealed hypertext links allowing free access to certain accounts of the Company's customers, without prior authentication. By clicking on these links, the delegation was able to access customer accounts - including their surname, first name, postal address, e-mail address, telephone number - and download several PDF documents relating to individuals, such as identity documents , quotes, car insurance certificates or even insurance contracts. The delegation also noted that the modification of the identifying number appearing at the end of one of the URL addresses displayed in the search results of the Duckduckgo search engine allowed access to the personal accounts of other customers of the company.8.The company was informed by telephone the same day, by the delegation, of the existence of a security defect on its site. An e-mail containing the type of URLs concerned was also sent to him. The company was asked to take the necessary corrective measures to remedy this as soon as possible in order to avoid any access to personal data by unauthorized third parties. By letter dated July 2, 2018, the company indicated to the Commission, through his counsel, that several steps had been taken to remedy the security defect. It specified that all the links indexed within the various search engines had been secured. In addition, it indicated that the URL address for viewing documents stored in Microsoft Azure storage space was now encrypted and had a limited lifespan of one hour. The company indicated that it had thus taken the necessary measures to make the documents inaccessible to a user who wanted to copy the link and index it in a search engine or on an application. premises of the company, the latter informed the delegation that it had

taken measures as of June 29 so that the documents of its customers are no longer accessible to unauthorized third parties. It thus specified that it had modified the source code of the website which does not generate authentication for people to access their customer area, as well as the configuration of the documents stored on the Microsoft Azure service, this being, before the alert of the CNIL, configured in such a way that the files were publicly accessible from the Internet. The delegation also carried out a query using the keywords client.[…].fr site:client.[…].fr in the Bing, Qwant and Yahoo search engines. She found that a list of hyperlinks to customer accounts was still displayed in the search results, but that these returned to the customer area login page or to a ResourceNotFound error message. However, it was found that by clicking on the cached button displayed next to the URL address referenced in the search results, it was still possible to access pages containing customers' personal data. We also found that the passwords for connecting customers to their personal space, whose format is imposed by the company, corresponded to their date of birth and that this format was indicated on the connection forms. It was also noted that, after the creation of their account, the username and the password of connection were transmitted to the customers by email and indicated in clear text in the body of the message.12. For the purpose of investigating these elements, the President of the CNIL appointed, on March 8, 2019, Mr. François PELLEGRINI as rapporteur on the basis of Article 47 of the law of January 6, 1978 as amended, in its wording applicable on the date of the events. By letter of the same day, the president of the CNIL informed the company of this appointment.13. At the end of his investigation, the rapporteur had company X notified by hand, on April 5, 2019, of a report detailing the breach relating to Article 32 of the GDPR that he considered to have been committed in this case.14. This report proposed that the CNIL's restricted committee impose an administrative fine on company X in the amount of 375,000 euros, which would be made public.15. Also attached to the report was a notice to attend the restricted committee meeting of June 13, 2019. The company had one month to submit its written observations.16. On May 6, 2019, the company provided written comments on the report. On this occasion, the company made a request for the meeting to be held behind closed doors. The Chairman of the Restricted Committee rejected this request by letter dated May 10, 2019.17. The company's observations were the subject of a response from the rapporteur on May 16, 2019.18. On June 11, 2019, the company filed submissions. As these were sent after the expiry of the fifteen-day period provided for in the third paragraph of Article 40 of the decree of May 29, 2019, they will be declared inadmissible.19.The company and the rapporteur presented oral observations during of the Restricted Committee meeting of June 13, 2019. II. Reasons for the decision On the absence of prior formal notice The company maintains that the President of the Commission could have sent it a formal notice which

would have more in-depth compliance procedure following the Commission's online inspection. the pronouncement of a sanction is not subject to a prior formal notice. The decision to appoint a rapporteur and to seize the restricted formation is a power belonging to the President of the Commission, who has the opportunity to take legal action and can therefore determine, depending on the circumstances of the case, the action to be taken on investigations by closing a case, for example, by issuing a formal notice or by seizing the restricted committee with a view to issuing one or more corrective measures. On the breach of the obligation to ensure the security and confidentiality of data to personal natureOn the security breach that led to the breach of personal dataa.On the characterization of the breach22. 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 in a timely manner in the event of a physical or technical incident; a procedure aimed at regularly testing, analyzing and evaluating the effectiveness of the measures technical and organizational to ensure the security of the processing.23. Article 32 (2) of the Regulation provides that: When assessing the appropriate level of security, account shall be taken in particular of the risks presented by the processing, resulting in particular from the destruction, loss, alteration , the unauthorized disclosure of personal data transmitted, stored or processed in any other way, or unauthorized access to such data, accidentally or unlawfully. It is up to the restricted party to determine whether the company X has failed in its obligation to ensure the security of the personal data processed and whether, in particular, it has implemented means to guarantee their confidentiality, in order to prevent them from being accessible to third parties not authorized, in accordance with the aforementioned Article 32 (1) ii. In defence, the company does not dispute that a security defect affected the website […] but points out that, after having been informed of the existence of the by services of the Commission, it quickly put in place effective measures to remedy it. Firstly, while emphasizing the diligence of the company, which reacted quickly after the revelation of the incident to correct it, the Restricted Committee notes that the basic security measures had not been taken prior to the development of its website, which made possible the occurrence of the personal data breach. The Restricted Committee notes that, during the inspection of June 28, 2018, the CNIL delegation was able to access the company's

customer data by performing a search using the keywords client.[…].fr site:client.[…].fr within the Duckduckgo search engine. Hypertext links appearing in search engine results allowed direct access to customer accounts containing their personal information and supporting documents, without prior checking. In addition, the delegation noted that the data was also accessible by modifying the URL address displayed in the navigation bar, such an operation being able to be carried out by a customer of the company connected to his personal space – who could thus access other 'personal accounts other than his own - or by anyone who saw the URL addresses referring to the accounts of the company's customers appear in the results of the Duckduckgo search engine. Furthermore, during the on-site inspection of the following July 12, the delegation noted that customer data and supporting documents were also accessible from the cache of the Bing, Qwant and Yahoo search engines.28 The Restricted Committee recalls that when hen a request to access a resource is sent to a server, the latter must first verify that its sender is authorized to access the requested information. However, in the present case, both the complainant, who had reported this security defect to the Commission's services, and the delegation of control, were able to freely consult the documents of the customers registered by the company, without any restrictive measure prevent it. The Restricted Committee considers that the breach of personal data resulting from this security defect could have been avoided if, for example, the company had implemented an authentication measure and a management of access rights to ensure that each user wishing to access a document was authorized to consult it. had not put in place the appropriate and elementary security measures. from the company's website, have been indexed by Duckduckgo, Bing, Qwant and Yahoo search engines. This indexing was made possible when the company had not put in place measures to limit it by search engines, by means, for example, of a robot.txt file. Furthermore, the Restricted Committee considers that the company should have implemented these elementary measures which did not require significant technical developments. It also recalls that data controllers are regularly alerted, in particular through its deliberations pronouncing administrative fines, on the importance of implementing this type of measure in order to protect personal data.Secondly, the company maintains that the identification of the security defect of its website required specific technical computer skills, which the complainant who made the report to the CNIL had, because of his profession. It considers that a natural person not educated in the field of computer development could not have identified this security defect and that the complainant's findings are the work of a specialist and that they are not representative of the activity on the Internet by an uninitiated natural person. The Restricted Committee considers, however, that access to the data of the company's customers was possible from a simple manipulation consisting of a modification of the

number appearing in the URL address displayed in the Navigator. Such a modification does not require any complex operation or any particular technical expertise in computer matters. This simple modification of the number appearing in the URL address is within the reach of any user of a browser as soon as this address appears in the browser of any customer of the company connecting to his account. The same manipulation could also be carried out by anyone who, from a search carried out within the Duckduckgo, Bing, Qwant and Yahoo search engines, saw displayed in their browser the URL addresses referring to the accounts of the company's customers .The Restricted Committee recalls, moreover, that it is regularly confronted with such a problem and that it has indicated, in several deliberations, that such manipulation does not require any particular technical skill. It also notes that the exposure of resources without prior access control is one of the ten security breaches most to monitor according to the 2017 guide to good practices from the Open Web Application Security Project, the reference professional association in terms of security of web companies. Verification of URL parameters is also part of all web security audits, insofar as it is an attack known to the web developer profession for a long time.36.In view of these elements, the restricted training 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 breachThe company explains that it only became aware of the security defect on June 28, 2018, following the information from the Commission services, and that it took the corrective measures that were imposed immediately after this alert. It specifies that it quickly delisted all the links indexed by the Duckduckgo.com search engine, which the delegation took note of by email of July 4. The company indicates that it also called on the company […] in order to carry out a complete audit of its IT system and bring its processing operations into compliance with the regulations. It states that it subsequently regularly informed the Commission's services of the progress of its compliance. Finally, it states, in its defense, that it set up a plan remediation, dated April 2019, defining the actions to be taken. The technical director of this company also specified, during the meeting of June 13, that the security measures concerning personal data had all been taken. Firstly, the Restricted Committee notes that the company has put in place the corrective measures necessary to secure personal data and acknowledges the fact that a more general remediation plan, making it possible to ensure its compliance with the regulations, has been determined. However, the Restricted Committee notes that the resolution of the security defect could only be carried out thanks to a report from a customer of the company who tried in vain to inform it in May 2018. In addition, the basic measures necessary to secure the data of its customers were put in place by the company only after the report and then the intervention of the

services of the Commission with it. The Restricted Committee therefore considers that the company did not place the he security of its customers' data at the heart of its concerns only after the intervention of the Commission services. Secondly, with regard to the number of people affected by the security breach, the Restricted Committee notes that the delegation noted, during the on-site check, that the database contained 148,359 separate telephone numbers and 144,057 separate e-mail addresses relating to customers. The company specified, on this occasion, that the personal data and supporting documents relating to all the contracts concluded by the company, terminated or not, were freely accessible due to the security defect noted. The Restricted Committee further notes that each customer of the company must provide several documents concerning him within the framework of the conclusion of a contract. Consequently, a large number of documents were made accessible due to the lack of security affecting the company's website, namely 144,890 copies of vehicle registration documents, 137,776 copies of driving licenses, 119,940 bank identity statements , 119,517 quotes or 36,068 copies of declarations of transfer of a vehicle. In addition, each document contains, by its nature, multiple information on the person concerned such as his surname, first name, postal address, e-mail address, date and place of birth, bank details, vehicle registration or even elements relating to the suspension of the driving license and the reasons for termination of the guarantee on the part of the company. Consequently, the security defect concerned a particularly large number import of personal data and documents concerning the company's customers. In addition, the Restricted Committee notes that the security breach concerned documents containing t elements that reveal particularly precise information about individuals. It was thus possible to have access to the history of customers in terms of automobile insurance and thus to know if a person had been the subject of a termination or cancellation of contract for false declaration or for non- payment of a bonus, or even if she had had her license revoked or committed a hit and run or a refusal to comply. On this last point, the Restricted Committee notes that the data in question relate offenses committed by the persons and the follow-up given to them. It recalls that recital 83 of the GDPR provides that the measures to mitigate the risks inherent in the processing must ensure an appropriate level of security, including confidentiality, taking into account the state of knowledge and the costs of implementation by in relation to the risks and the nature of the personal data to be protected. Consequently, such data, considered to be special data, must be subject to enhanced vigilance and protection by data controllers, which was not the case in this case. .On the lack of robustness of the passwords for accessing the company's customer accountsThe CNIL delegation noted, during the inspection of July 12, 2018, that customers had to connect to their personal space accessible online via their customer number and their date of birth, this

second piece of information being equivalent to a password. The company informed the delegation that no additional measures for the authentication of persons, such as a limitation of the number of attempts in the event of incorrect passwords, had been put in place. The rapporteur maintains that the insufficient robustness of the passwords does not ensure the security of the data processed by the company and to prevent brute force attacks which consist in successively and systematically testing numerous passwords and thus lead to a compromise associated accounts and the personal data they contain. In defence, the company does not dispute the facts found, but maintains that its choice as to the complexity of the passwords was guided by the desire to facilitate the diligence of its customers in order to that they can easily access their personal file and communicate in user-friendly and practical conditions with their broker. The company had thus indicated, during the on-site inspection, that it had wished to facilitate the procedures of the policyholders, some of whom had difficulty reading and writing. Subsequently, the company informed the CNIL that it had imposed on its customers, on July 26, 2018, a modification of their password during a new connection to their space. The Restricted Committee notes that it belongs to company X to implement security measures intended to ensure the security of all the personal data it processes, including in particular those of vulnerable populations. In this regard, it notes that recommendations are put forward by the Commission and ANSSI to help anyone create a complex and easy-to-remember password. The Restricted Committee therefore considers that the company has the means enabling it to fulfill its obligations in terms of security, even though some of its customers may have difficulty reading and writing. The Restricted Committee recalls that, to ensure a level of security sufficient and meet the strength requirements for passwords, when authentication is based solely on a username and a password, the password must contain at least twelve characters - containing at least one uppercase letter, one lowercase letter, one number and a special character - or the password must contain at least eight characters - containing three of these four categories of characters - and be accompanied by an additional measure such as, for example, the delay in accessing the account after several failures (suspension temporary access, the duration of which increases as attempts are made), the establishment of a mechanism to guard against the automated and intensive submissions of attempts (e.g. captcha) and/or blocking of the account after several unsuccessful authentication attempts. The Restricted Committee notes that the need for a strong password is also underlined by ANSSI, which indicates that a good password is above all a strong password, ie difficult to find even using automated tools. The strength of a password depends on its length and the number of possibilities existing for each character composing it. Indeed, a password consisting of lowercase letters, uppercase letters, special characters and numbers is technically more

difficult to discover than a password consisting only of lowercase letters. In addition, it appears from the findings made by the delegation of control that the form for connecting customers to their personal space expressly indicated the format of the connection passwords, namely the person's date of birth, which considerably facilitated an attack. by brute force, especially since the format of the passwords was indicated on the customer account connection form. The Restricted Committee also notes that customers wishing to strengthen the security of their data and change their password were prevented from doing so by the company which had imposed the format relating to the date of birth. The Restricted Committee therefore considers that the words put in place by the company to access customer accounts did not meet the required requirements in terms of robustness. of the account, the Restricted Committee notes that such a procedure does not make it possible to ensure the security of the data, since the sending of an unencrypted email may lead to its interception by any person listening to the network and to the taking knowledge of the information it contains. The Restricted Committee notes that the company did not dispute, in its response or during the meeting, the existence of such a breach. The Committee Restricted infers that the company has disregarded an elementary security measure recommended by the CNIL, whereas the transmission of passwords in clear text in an email makes it accessible to any third party likely to access the electronic mail of the person concerned. Based on all of these elements, the Restricted Committee considers that the breach of Article 32 of the Rules has been established.3. On penalties and publicityArticle 20-III of the amended law of 6 January 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 April 27, 2016 mentioned above or of this law, the president of the National Commission for Data Processing and Liberties may also, if necessary after having sent him the warning provided for in I of this article or, if necessary in addition to a formal notice provided for in II, seize the restricted formation of the commission with a view to the pronouncement, after adversarial procedure, of one or more of the following measures:[…]: 7° With the exception of cases where the processing is implemented by the State, an administrative fine not to exceed 10 million euros or, in the case of a company, 2% of the total worldwide annual turnover of the preceding financial year, the the highest amount being retained. 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: Each supervisory authority shall ensure that administrative fines imposed under this Article

for breaches 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 breach. 63. The company considers that the amount proposed in the report penalty is disproportionate when it is equivalent to 3.5% of its turnover, as well as in view of its responsiveness and the measures put in place after the discovery of the security defect. The company estimates that such elements must be taken into account by the Restricted Committee when determining the amount of the administrative fine, as has been done in previous proceedings. During the meeting of June 13, the company insisted on the fact that its size and its financial capacity must be taken into account in determining the amount of the penalty and that the amount proposed by the rapporteur is disproportionate in view of the penalties imposed. against companies with higher financial capacity and more employees. on-site inspection and argues that none of its customers informed it of the existence of damage, following the notification of the personal data breach to them.66. 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.67. 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 company did not measure, before being alerted by the services of the CNIL, the importance of securing the personal data contained in its information systems, despite the nature of the data processed. .Then, the Restricted Committee considers that the seriousness of the breach is characterized in this case.This is characterized by the nature of the personal data concerned, the company processing particularly identifying data, as well as data relating to offenses . The Restricted Committee also considers that the seriousness of the breach is characterized by the number of documents and persons concerned by the security defect, which affected the accounts of several thousand customers and persons who terminated their contract with the company .The Restricted Committee recalls, moreover, that the security defect is due to a defective design of its website by the company, developed in 2014, and that it therefore persisted for several years. In addition, the implementation of an authentication procedure on the site as well as that of a directive limiting the indexing by search engines of certain parts of the website were elementary measures. that the sanction decisions invoked by the company were adopted under the Data Protection Act as amended by law no. 2016-1321 of October 7, 2016 for a Digital Republic, which provided that the amount of sanctions that could be pronounced by the restricted committee could not exceed 3 million euros. The facts of the case were observed when the GDPR had entered into force and the violation observed is likely to give rise to a fine of up to 10,000,000 euros or, in the case of company, up to 2% of the total worldwide annual turnover of the previous financial year, whichever is higher. The Restricted Committee notes, however, that the company reacted quickly after learning of the data breach by implementing corrective measures twenty-four hours after being alerted by the CNIL services. It also notes that the company has cooperated with the CNIL in the context of the various exchanges maintained with its services following the

checks and its good faith in the resolution of the security defect. Finally, it notes that the company informed its customers of the occurrence of the safety defect and that no damage concerning them has been brought to its attention. 83 of the GDPR, considers that an administrative fine of 180,000 euros is justified and proportionate, as well as an additional publicity sanction for the same reasons. FOR THESE REASONS The restricted formation of the CNIL, after deliberation, decides: to declare inadmissible the observations of company X produced on June 11, 2019; to impose an administrative fine on company X in the amount of 180,000 (one hundred and eighty thousand) euros; to make public, on them ite of the CNIL and on the Légifrance site, its deliberation, which will no longer identify the company by name at the end of a period of two years from its publication. The Chairman Alexandre LINDEN This decision may be subject to appeal to the Council of State within two months of its notification.