Deliberation SAN-2020-003 of July 28, 2020 National Commission for Computing and Liberties Legal status: In force Date of publication on Légifrance: Wednesday August 05, 2020 Deliberation of restricted committee no. SAN-2020-003 of July 28, 2020 concerning the company XThe National Commission for Computing and Liberties, meeting in its restricted formation composed of Messrs Alexandre LINDEN, Chairman, Philippe-Pierre CABOURDIN, Vice-Chairman, and Mesdames Anne DEBET and Christine MAUGÜE, members; Having regard to Convention No. 108 of Council of Europe of 28 January 1981 for the protection of individuals with regard to the automatic processing of personal data; Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 relating to the protection personal data and the free movement of such data; Having regard to law no. 78-17 of 6 January 1978 relating to data processing, files and modified freedoms, in particular its articles s 20 and following; Having regard to decree no. 2019-536 of May 29, 2019 taken for the application of law no. 78-17 of January 6, 1978 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 Computing and Liberties; Having regard to decision no. 2018-076C of March 30, 2018 of the President of the National Commission for Computing and Liberties to instruct the secretary general to carry out or have carried out a mission to verify the processing implemented by this organization or on behalf of company X; Having regard to the decision of the president of the National Commission for Computing and Liberties appointing of a rapporteur before the restricted committee, dated April 29, 2019; Having regard to the report of Mr. Bertrand du MARAIS, reporting commissioner, notified to company X on September 23, 2019; Having regard to the written observations submitted by company X on October 24 2019 Having regard to the rapporteur's response to these observations notified on November 7, 2019 to the board of the company; Having regard to the new written observations of the board of company X received on November 22, 2019 as well as the oral observations made during the session of the restricted committee , November 28, 2019; Having regard to the other documents in the file; Were present at the restricted committee meeting of November 28, 2019: Mr. Bertrand du MARAIS, statutory auditor, heard in his report; As representatives of company X: […];[…];[…];[…];[…];[…]. Company X having the floor last;The Restricted Committee adopted the following decision:I.Facts and procedureCompany X (hereinafter the company) is a simplified joint-stock company created in 2006, specializing in the sales sector distance of shoes, whose head office is located […]. In 2018, company X achieved a net turnover of more than […] euros and a negative net result of almost […] euros. In the same year, Group X, comprising Company X and its subsidiaries, achieved a net turnover of around […] euros and a negative net result of around […] euros. Group X employs

approximately 1,000 people. The company publishes, for the purposes of its activity, sixteen websites in thirteen countries of the European Union, namely France, Spain, Germany, Italy, the Netherlands, Slovakia, Denmark, Poland, Sweden, Finland, Belgium, the Czech Republic and Hungary as well as the United Kingdom. Two other websites (X.eu) and (X.net) are intended for consumers from other countries paying in euros and dollars. On May 31, 2018, pursuant to decision no. 2018-076C of the President , a delegation from the National Commission for Computing and Liberties (hereafter the CNIL or the Commission) carried out an inspection mission on the premises of company X. The purpose of this mission was to verify compliance by this company of all the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 (hereinafter the Regulation or the GDPR) and of Law No. 78-17 of January 6, 1978 as amended relating to data processing, files and freedoms (hereinafter the amended law of 6 January 1978 or the Data Protection Act). The control focused more particularly on the processing of personal data of the company's customers and prospects, as well as on the recording of telephone conversations between customers and the company's customer service employees. During this mission control, the delegation was informed that the company implements processing aimed at combating fraud and unpaid bills during payments made on its websites. When the 3DSecure protocol is not validated, an email is sent to the person placing the order so that they can send proof of address and a scan of the front of their bank card. The company also told the delegation that no retention period for personal data had been defined and that it did not regularly delete data relating to customers and prospects after a defined period. The delegation found that in the context of the recording of telephone conversations between customer advisers and customers, people calling the company could oppose the recording of telephone calls by pressing a key their phone. Finally, the delegation noted that when a user creates an account on the company's website, passwords consisting of six digits, containing a single type of character, were accepted. The company also indicated that account passwords were stored in the production database in hashed form using the MD5 hash function, using a salt present directly in the database field relating to corresponding passwords. In addition, following the check, the company sent the Commission, by email dated June 7, 2018, the additional documents requested and in particular a count made in the database relating to the number of customers and prospects who have not connected, since 2008, to its websites distributed in the various countries in which it is present. The following elements were provided by the company: 118,768 customers whose personal data was present in the database had not connected since May 25, 2008; 682,164 customers had not connected since May 25, 2010; 3,620 401 customers had not connected since May 25, 2013; 5,790,121 customers had not connected since May 25, 2015;

25,911,675 prospects had been inactive since May 25, 2015. It also emerged from this count that company X held more than […] customer accounts and more than […] prospects. web.In accordance with article 56 of the GDPR, the CNIL informed on July 27, 2018 all the European supervisory authorities of its competence to act as lead supervisory authority concerning the cross-border processing carried out by the company and opening the procedure on the statement of the authorities concerned on this case. For the purposes of examining these elements, the President of the Commission appointed Mr Bertrand du MARAIS as rapporteur, on April 18, 2019, on the basis of Article 47 of the law of January 6, 1978 amended in the version applicable on the day of appointment. ° 2005-1309 of October 20, 2005 amended. At the end of his investigation, the rapporteur had a bailiff notify company X, on September 23, 2019, of a report detailing the breaches of the GDPR that he considered constituted in case. This report proposed that the restricted committee of the Commission issue an injunction to bring the processing into compliance with the provisions of Articles 5-1-c), 5-1 e), 13, 32 and 35-1 of the Payment, accompanied by a penalty payment at the end of a period of three months following prior to notification of the deliberation of the Restricted Committee, as well as an administrative fine. It also proposed that this decision be made public and no longer allow the company to be identified by name after the expiry of a period of two years from its publication. of November 28, 2019 indicating to the company that it had one month to submit its written observations. On October 23, 2019, through its counsel, the company produced observations. The rapporteur replied on the following November 7. On November 22, the company produced new observations in response to those of the rapporteur. The company and the rapporteur presented oral observations during the restricted training session of November 28, 2019 The draft decision adopted by the Restricted Committee was sent to the relevant European supervisory authorities on February 16, 2020, in accordance with Article 60.4 of the General Data Protection Regulation (GDPR). The Restricted Committee ruled, in its draft decision, on the breaches proposed by the rapporteur and discussed by the parties in the context of compliance with the adversarial principle, namely the breaches of Articles 5-1-c), 5 -1 e), 13, 32 and 35-1 of the GDPR; no breach of Article 6 of the GDPR and of Directive 2002/58/EC of the Parliament and of the Council known as the ePrivacy Directive having been raised by the rapporteur. On the following 13 and 17 March, the Italian, Portuguese and of Lower Saxony have formulated relevant and reasoned objections to the draft decision. The Restricted Committee decided to modify its draft decision in order to take these objections into account. Since they did not propose to deviate from the draft decision by taking into account a new factual circumstance, to add a breach or to aggravate the nature of the corrective measure initially proposed, the Restricted Committee decided not to

communicate them to the rapporteur or to company X. The revised draft decision was submitted to the supervisory authorities concerned on June 25, 2020. II. Grounds for the decision A. On the breach of the principle of data minimization (obligation to ensuring the adequacy, relevance and non-excessive nature of the data)1. Recording of telephone callsArticle 5-1 c) of the Regulation provides that personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (minimization of data). Firstly, the rapporteur maintains that the complete and permanent recording of telephone calls received by customer service employees appears excessive with regard to the purpose of evaluating them by the company. The company maintains that the telephone recordings do not are neither permanent nor systematic insofar as customers have the possibility of opposing the recording of the call. It also considers that the full recording of telephone conversations is proportionate to the employee evaluation and training objectives pursued by the company. Lastly, it maintains that the rapporteur is wrong to assert that the recording of telephone calls would be excessive on the grounds that the person responsible for carrying out the training generally only listens to one recording per week, per employee, whereas this average would be, according to the company, likely to evolve according to the needs of the company. It specifies that the number of recordings that the trainer must be able to listen to must be greater than the number of recordings that he actually listens to. The restricted training notes, first of all, that if certain customers oppose the recording of the telephone call made, the company implements a process allowing the recording of all the telephone conversations of its employees, without the latter having the possibility of opposing it. Next, it considers that the company does not justify the need to record all of the telephone conversations made by customer service, with regard to the purpose of the processing, namely the training of employees. The Restricted Committee notes that the company indicated, during the hearing of June 19, 2019, that the person in charge of this training generally only listens to one recording per week and per employee. Moreover, if the company stated, during the meeting of November 28, 2019, that the rate of recording of telephone conversations fell from 100% to 30%, it does not produce any supporting documents on this point. he recordings may vary according to each employee and the circumstances, in particular the latter's training needs, the Restricted Committee considers that the company has not demonstrated that it has put in place, for the past and the future, a recording of the telephone conversations of employees limited to what is necessary with regard to the purpose pursued. However, a data controller cannot set up a processing of personal data without ensuring that it is necessary for his needs, a fortiori when it is based on a particularly intrusive device for employees. Restricted training therefore considers, in view of these elements, that a breach of Article

5-1-c) of the GDPR has been established.Secondly, the rapporteur criticizes the company for not having put in place a measure to avoid the registration of customers' bank details during telephone calls made with the company. It also considers that the measure proposed by the company, following the hearing, consisting of eliminating calls every day in connection with orders placed by telephone with payment by credit card, remains unsatisfactory in that the processing of data banking for one day is not justified with regard to the purpose of the processing, which is the evaluation of the employees. He recalls that the processing of bank details is aimed at making the payment and that such data does not have to be recorded by the company, even for a single day, once the payment has been validated. The company maintains that the erasure of the data records recorded during telephone conversations, every day, put in place following the hearing of June 19, 2019, ensures data retention in accordance with the principle of minimization. It specifies that the implementation of a measure making it possible to interrupt a recording when a customer's bank details are communicated would require the development of complex technical tools and would entail a particularly heavy financial and human cost. Restricted training observes that the company has, at least until June 19, 2019, recorded on the occasion of the recording of employee conversations for training purposes, the bank details of customers who placed orders by telephone and kept such data in its database, in plain text, for fifteen days. It notes that bank details are data which, given their nature and the associated risks of fraud, must be subject to enhanced protection by data controllers. Indeed, as noted by the rapporteur, their use by unauthorized third parties, in the context of fraudulent payment, is likely to cause harm to the persons concerned. The Restricted Committee notes that the company recorded and kept data of which it had no use with regard to the purpose pursued by the processing in question, namely the training of employees. It therefore considers, in view of these elements, that a breach of Article 5-1-c) of the GDPR is constituted. The data collected in the context of the fight against fraudFirstly, the rapporteur maintains that the company disregards the principle of data minimization when it keeps, in the context of the fight against fraud , supporting documents sent by customers such as a copy of the national identity card, which are not required. The company maintains that the retention of a document transmitted spontaneously by a person is not excessive. It considers that it can keep copies of the national identity card of persons transmitted spontaneously insofar as the CNIL indicates in its practical guide for online purchases that a data controller can request proof of identity and/or or domicile to ensure the identity of the holder. The Restricted Committee notes that the company informed the CNIL, during the hearing of June 19, 2019, that it was asking customers located in France, for the purposes of fight against fraud, providing a copy of proof of address and a scan of their bank card. However, she told the

Commission that even if she does not ask for a copy of the identity card, it happens that people provide her with such a document and that in such a case, she keeps this document for six months. , in the same way as the other supporting documents sent to it. The Restricted Committee notes that the copy of the identity card can constitute relevant proof in the context of the fight against fraud. Consequently, in view of the purpose of the processing implemented by the company and the residual nature of the number of copies of identity cards processed by the company, it considers that there is no reason to retain, in l species, the alleged breach. Secondly, the rapporteur pointed out in his report that the company collected, in Italy, within the framework of the fight against fraud, the copy of the health card (tessera sanitaria) and the health card. valid identity. He criticized the company for not having been able to indicate during the hearing why the collection of this document is necessary in the context of the fight against fraud. Subsequently, the rapporteur took note of the information provided by the company by virtue of which it indicated that its statements made during the hearing of June 19, 2019 were false and that it was in fact only asking customers to communicate their identity card to the exclusion of any other proof. It also indicated that following a communication error, the company's sales department asked, between June 27 and July 18, 2019, customers to send a copy of this health card, but that this practice has ceased and that the documents thus collected have been suppressed. The rapporteur therefore considered that there was no longer any need to take this fact into account in support of the aforementioned breach. The Restricted Committee notes that the Italian health card contains a large amount of information about its holder, know his surname, first name, gender, tax code, place of birth corresponding for citizens born in Italy to the municipality of birth and for foreigners to the country of birth. It can also be deduced from the expiry date of the card that the person has a residence permit in Italy. It considers that the communication of two documents making it possible to prove the identity of the person for the purposes of against fraud, namely the health card and the identity document, was excessive and not relevant under Article 5-1 c) of the GDPR. It appears that only the collection of the identity card was relevant with regard to the purpose of the processing implemented. In this case, the collection of the health card containing more information than the identity card, irrelevant in the context of the fight against fraud, was excessive. In this regard, the Restricted Committee notes that the company acknowledges that such collection was not necessary, as it ceased in July 2019. The Restricted Committee considers that even if the company would have collected such a document only for a limited period of three weeks, such elements constitute a breach of the obligation for the data controller to process only adequate, relevant and limited data to what is necessary in relation to the purposes for which they are processed, under the principle of data minimization. The

Restricted Committee therefore considers that a breach of Article 5-1 c) of the GDPR is constituted for these facts. B. On the breach of the obligation to limit the data retention periodArticle 5-1 e) of the Regulation provides that personal data must be kept in a form allowing the identification of the persons concerned for a period not not exceeding that necessary with regard to the purposes for which they are processed; personal data may be stored for longer periods insofar as they will be processed exclusively for archival purposes in the public interest, for scientific or historical research purposes or for statistical purposes in accordance with Article 89 , paragraph 1, provided that the appropriate technical and organizational measures required by this Regulation are implemented in order to guarantee the rights and freedoms of the data subject (limitation of storage). Firstly, the rapporteur noted that during the inspection of May 31, 2018, the company informed the CNIL that no retention period for customer and prospect data had been determined and that it did not carry out any regular deletion or no archiving of such data after a defined period. During the hearing of June 19, 2019, the company informed the rapporteur that it had set a retention period for this data of five years, on an active basis, from the date of the last activity of customers and prospects, which may correspond for example , to a connection to the customer account, to a click in a newsletter or even to the opening of this one. For the determination of the number of customers and prospects to be taken into consideration, it is necessary to include those located in the United Kingdom. United since this State was a member of the European Union at the time of the facts in question, the GDPR is applicable. Moreover, under the withdrawal agreement between the European Union and the United Kingdom, a transitional period has been agreed during which Union law continues to apply to the United Kingdom. by the company, at the request of the delegation of control, made it possible to establish that the company kept the data of 118,768 customers who had not connected to their account since May 25, 2008, those of 682,164 customers who had not not connected to their account since May 25, 2010 and the data of 3,620,401 customers who have not connected to their account since May 25, 2013. The Restricted Committee deduces from this that at least until the count carried out on June 7 2018 in the database, the company kept a particularly large amount of data concerning its customers who had not connected to their account for more than ten years. In addition, the fact, alleged by the company, that only the legal manager has access to customer data stored ées is in any case devoid of scope, the retention period being independent of access. With regard to prospects, the rapporteur considers that the company does not justify the need to apply a retention period for their data for five years from the last contact from them. The company maintains that the five-year retention period for such data is adequate given the specificity of its general e-commerce platform. It would, moreover, be established that certain prospects connect to

look at the offers offered after a period of inactivity of four years. The Restricted Committee notes that the company kept in June 2018, with regard to the various countries of the European Union where the company does business and from the UK, with data from over 25 million prospects who have had no activity since May 25, 2015, more than three years. In addition, by way of significant example, the data of 4,801,596 prospects with no activity for more than three years were kept, concerning Spain, those of 5,616,503 prospects concerning Italy and those of more than 12 million prospects concerning France. The Restricted Committee notes that after having indicated to the CNIL services that the data was kept indefinitely, the company indicated, during the hearing, that it now keeps this data for five years from the last contact. , even though she maintains that she no longer relaunch them after a period of inactivity of two years. The Restricted Committee considers that the company has not established how the retention of the data of prospects, who are people who have never placed an order on the company's site or former customers whose data is used for prospecting purposes after the end of the commercial relationship, is necessary beyond the period of two years during which it carries out its prospecting operations. The company has indeed indicated that it only sends messages promoting its products or containing commercial offers to its prospects for a period of two years. On this point, the Restricted Committee considers that in this case, the duration of two years appears proportionate in view of the purpose of the processing. This duration responds to the company's desire to promote, like any merchant, its products to its former customers and to people who have not opposed the receipt of such messages. The company further specifies that a mechanism allows people to unsubscribe at any time to no longer receive prospecting messages. On the other hand, the retention period set up by the company with regard to the data of prospects, namely five years, exceeds that necessary with regard to the purposes for which they are processed. The Restricted Committee therefore considers that the company has disregarded the provisions of Article 5-1 e) of the GDPR.Secondly, the rapporteur criticizes the company for determining as the starting point the retention period for prospects' data, in particular the opening of a prospecting email.The training Restricted notes that prospect data allows a data controller to send messages, for example by e-mail, to people who show an interest in its products or services. The Commission considers in this respect that when the starting point of the data retention period is the last contact from the prospect, it must be an event that demonstrates the person's interest in the message received, such as a click on a hypertext link contained in an e-mail. However, the mere opening of an e-mail cannot be considered as a contact from the prospect, insofar as it may be opened involuntarily due to the operating methods of the e-mail software used or by mistake. The Restricted Committee considers therefore that the company cannot, without

disregarding the principle of limiting the retention period of data, consider that the simple opening of a prospecting email by a person allows the starting point of the retention period for the data of the prospects and thus keep such data even though the prospects have not demonstrated, by a clear act, an interest in the company's products or services for several years.Thirdly, the rapporteur maintains that at the end of the expiration of the customer data retention period, the company does not delete all of the retained data, but retains the customer's email address as well as their passwords, in a pseudonymized form, which would not make it possible to respect the principle of limitation of data retention. The company maintains that the anonymization of the electronic addresses of former customers is carried out using a process based on SHA-256 technology and that the decryption of hashed data with this function requires very advanced technical skills. It therefore considers that the data of inactive customers is indecipherable and therefore anonymous. The training notes that at the end of a customer's period of inactivity, the company deletes certain data, namely the name, first name and date of birth of the latter, but retains others such as his email address and its password which are hashed by an algorithm and transferred to another table. The company thus wishes to allow a customer to reconnect to his account with the same identifier and the same password as those used when creating his account, at the end of the data retention period set up. The Restricted Committee considers that the data of its former customers, even if hashed, is not anonymized, but pseudonymized, and would make it possible to re-identify people. The company maintains that the email addresses and passwords of its former customers are hashed using a SHA-256 algorithm which is particularly robust and which would make the data anonymous. The Restricted Committee notes that the SHA-256 algorithm is a hash function ensuring the integrity of the personal data processed by the company. If it is, to date, a function that cannot be reversed and is therefore considered by the National Agency for the Security of Information Systems (ANSSI) and the CNIL as guaranteeing a sufficient level of security of data, this does not make it possible to anonymize data and therefore to justify their indefinite retention by a data controller. Consequently, the Restricted Committee considers that the company retains the data in question for a period exceeding that necessary for the with regard to the purposes for which they are processed. It notes in this regard that the company itself indicates that the purpose of implementing such a measure is to allow its customers to reconnect to their account, even though the data is supposed to have been deleted. . The personal data of former customers must be permanently deleted at the end of the retention period for them in the active database or in the archive database, once the legal obligations have expired and cannot be kept for hypothetical future use. .The Restricted Committee therefore considers that the company has, here again, disregarded the

provisions of Article 5-1 e) of the GDPR.C.On the breach of the obligation to inform personsArticle 13 of the GDPR requires the controller that he provides, at the time the data is collected, information relating to his identity and contact details, those of the data protection officer, the purposes of the processing and its legal basis, the recipients of the personal data personal data, where applicable the transfers of personal data, the retention period of personal data, the rights enjoyed by individuals as well as the right of file a complaint with a supervisory authority. As far as customers are concerned, the rapporteur criticized the company for not informing them, within the data privacy policy, accessible on the company's website as well as via a link on the account creation form, that their data is transferred to Madagascar, in the context of telephone calls. He also criticized the company for citing in these documents only one legal basis for all its processing, namely consent, while certain processing was based on a different legal basis. The rapporteur noted, in his observations of 7 November 2019, that despite the company's claims, the privacy policy had not been corrected to include the transfer of data to Madagascar. Regarding the legal bases of the processing, the company claimed that it based its processing on the consent of the people, which, according to it, could not be blamed insofar as this legal basis is more protective for the people and that consequently a failure to inform the people could not be retained against it with regard to these facts. e them, namely, for example, the fight against fraud or those implemented in the context of purchases made on the company's website, cannot be based on the consent of individuals, but, as indicated the rapporteur, on the contract or the legitimate interests pursued by the company. Recalling that recital 41 of the GDPR requires that the legal basis of the processing be clear and precise, it considers that the company cannot only target within its data privacy policy the legal basis of consent for all the processing carried out. Therefore, if the company has effectively, as the texts require, integrated information on the legal basis and had the concern to retain the most protective basis, according to it, of the rights of the people, the restricted committee recalls that GDPR Article 13 requires granular information about the legal basis for each processing operation. It can therefore only note that the company has not fully complied with the provisions of this article by refraining from indicating, for each processing operation implemented, the corresponding legal basis in its privacy policy. elsewhere, the Restricted Committee takes note of the changes made to its website, with regard to the transfer of data to Madagascar. However, it considers that a breach of Article 13 of the GDPR existed until November 18, 2019, the date on which the company indicates that it made changes to its website. As regards employees, the rapporteur criticizes the company not to inform them individually of the recording of their telephone calls. The company maintains that employees are informed of the recording of telephone calls made with customers, thanks to several

documents, such as a certificate of presence telephone tap dated January 14, 2016, a document from May 2014 as well as performance evaluation sheets dated 2017. The company also provided certificates from three customer advisers stating that they had read the document dated January 14 2016, that they understood the purpose of these wiretaps and that they can contact the legal department for additional information. recalls that informing employees of the implementation of devices for listening to and recording telephone conversations in the workplace is fundamental and is linked to the fair and transparent nature of any processing implemented by a data controller . As stated in recital 39 of the GDPR, the principle of transparency requires that any information and communication relating to the processing of such personal data be easily accessible, easy to understand, and formulated in clear and simple terms . The obligation of transparency obliges the company to provide information relating to such a system to each employee, which cannot be satisfied with a single piece of information, as in this case in 2016, which would not be provided to new employees. employees thereafter. Moreover, the Restricted Committee also notes that Article L. 1222-4 of the Labor Code provides that no information concerning an employee personally may be collected by a device that has not been worn beforehand. to his knowledge. In addition, the Commission has reiterated on several occasions, and in particular in a guide for employers and employees available on its website as well as in recommendation no. 2014-474 of 27 November 2014 relating to the recording of calls on the place of work, that employees must be provided with a certain amount of information regarding the processing implemented by employers. Finally, the Restricted Committee notes that the documents produced by the company do not allow employees to be provided with a information relating to the purposes pursued by the processing, the legal basis of the device, the recipients of the data from the device, the retention period of the data, their rights in particular of access to the data concerning them as well as the possibility of file a complaint with the CNIL, guaranteeing complete information for employees in accordance with article 13 of the GDPR. The restricted training therefore considers, in view of these elements, that a breach of Article 13 of the GDPR is constituted.D.A breach of the obligation to ensure data security1. The lack of security relating to passwords for accessing customer accountsArticle 32-1 of the Regulation provides: Given the state of knowledge, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risks, the degree of probability and severity of which varies, for the rights and freedoms of natural persons, the controller and the processor implement the appropriate technical and organizational measures in order to guarantee a level of security appropriate to the risk and in particular the means to guarantee the constant confidentiality, integrity, availability and resilience of the processing systems and services . The

controller must therefore, in accordance with Article 32-2 of the GDPR, take into account the risks presented by the processing, resulting in particular from the destruction, loss, alteration, unauthorized disclosure of data to personal nature transmitted, stored or processed in another way, or unauthorized access to such data, accidentally or unlawfully. The CNIL delegation noted, during the inspection of May 31, 2018, that the persons wishing to create a user account on the company's website could create a six-character password with a single character category. During the hearing on June 19, 2019, the company specified that, since the CNIL's control, a one-minute account blocking measure was put in place, after 19 unsuccessful attempts to access an account at from the same IP address in less than a minute. In defense, the company argues that it has changed the rules for creating account passwords and now requires its customers to create passwords composed of at least eight characters. It also calls into question the CNIL's recommendations in this area and maintains that the technical recommendations in terms of securing passwords resulting from Commission deliberation no. 2017-190 of 22 June 2017 are the subject of disputes by cybersecurity experts. Maintaining that overly complex rules have led to a standardization of passwords, she preferred to opt for the imposition of short and simpler passwords, these being less predictable for a possible attacker, the hazard being based on a human logic. The rapporteur maintains that passwords, made up of six or eight characters, with no complexity criteria, are not sufficiently robust and do not ensure the security of the data processed by the company. He considers that such passwords do not make it possible to prevent brute force attacks which consist in successively and systematically testing numerous passwords and can thus lead to a compromise of the associated accounts and personal data that they contain. The Restricted Committee considers that, contrary to what society maintains, the length and complexity of a password remain basic criteria for assessing its strength. It recalls that, in order to ensure a sufficient level of security and meet the robustness 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 at least one uppercase letter, one lowercase letter, one number and one 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 timeout access to the account after several failures (temporary suspension of access, the duration of which increases as attempts are made), the establishment of a mechanism to guard against automated and intensive submissions of attempts (e.g. captcha) and/or the blocking of the account after several unsuccessful authentication attempts. The Restricted Committee notes that the need for a strong password is equal underlined by the ANSSI, which indicates that a good password is above all a strong

password, i.e. 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 this case, it considers that the robustness of a password made up of eight characters and only one category of characters is very low and that the company does not demonstrate at any time how a short and simple password would be more likely to resist a brute force attack than a password made up of more characters as well as several categories of characters. The Restricted Committee therefore considers that the passwords put in place by the company to access the accounts created on its website do not correspond to the required requirements in terms of robustness. as part of the fight against fraud, to send him by email a scan of the bank card used when ordering. For its customers in France, an email specifying on the 16 digits of the front face, please let appear at least the first 4 and the last 4, the date of validity and the name of the holder must appear clearly is then sent to the people. E-mails making such a request are also sent to people placing orders on the Italian, Spanish, Hungarian, Slovak, Danish and Greek sites. it was found that the company kept the bank card scans unobstructed. The rapporteur thus considers that the company's e-mail addressed to people, particularly French people, encourages them to provide a full copy of the payment card instead of inviting customers to hide a minimum number of their bank card numbers. It has also been noted that bank card scans are kept by the company in the clear for six months from the registration of the documents, in the event of a dispute. letter of June 28, 2019, the company indicated that an online platform dedicated to sending supporting documents would be set up at the end of August 2019. In addition, the company maintains that it has been authorized by the CNIL to implement implements processing for the purpose of combating fraud and that it can validly collect the expiry dates and truncated bank card numbers. First, the Restricted Committee notes that the company té was indeed authorized by deliberation of the CNIL of July 2, 2009 to process the truncated bank card number as well as the date of expiry, within the framework of the implementation of a processing whose purpose is to fight against the fraud. However, it is established that the company processed copies of customers' bank cards containing all the numbers, while it was only authorized to process a truncated part of them. The Restricted Committee therefore considers that the authorization issued by the CNIL cannot justify the processing of all of the customers' bank card numbers. Secondly, the Restricted Committee notes that it has been noted by the CNIL delegation that the system put in place by the company allowed customers to send in plain text, by unencrypted e-mail from their electronic inbox, photographs or scans of their bank card containing the full number of

the bank card and that such data was kept, in the same way as the supporting documents requested in the context of the fight against fraud, for six months, unencrypted in the database. Under these conditions, the Restricted Committee considers that the company did not put in place, at least until August 2019, security measures to guarantee the security of its customers' banking data. Based on all of these elements, the restricted training co n considers that the breach of Article 32 of the Regulation is established.E. On corrective measures and their publication Under the terms of III of Article 20 of the law of January 6, 1978 as amended: When the data controller or its subcontractor does not comply with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or from 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: […] 2° An injunction to bring the processing into compliance with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or from this law or to satisfy the requests presented by the person concerned with a view to exercising their rights, which may be accompanied, except in cases where the processing is implemented by the State, with a penalty payment the amount of which may not exceed €100,000 per day of delay from the date set by the restricted body; […] 7° With the exception of cases where the processing is implemented by the State, an administrative fine not exceeding 10 million euros or, in the case of a company, 2% of the turnover total worldwide annual business for the previous fiscal year, whichever is greater. In the cases mentioned in 5 and 6 of Article 83 of Regulation (EU) 2016/679 of April 27, 2016, 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:1. 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.2. 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) the fact that the breach has was committed willfully or negligently; c) any action taken by the controller or processor to mitigate the harm

suffered by data subjects; d) the degree of liability 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 control in with a view to remedying the breach and mitigating its possible negative effects; g) the categories of personal data concerned by the breach; h) the manner in which the supervisory authority became aware of the breach, in particular if, 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 processor for the same purpose, compliance with these measures; j) the application of codes of conduct approved pursuant to Article 40 or certification mechanisms approved pursuant to Article 42; andk) any other aggravating or mitigating circumstance applicable to the circumstances of the case, such as the financial benefits obtained or the losses avoided, directly or indirectly, as a result of the violation. Firstly, concerning the fine proposed by the rapporteur, the company maintains that it has never been condemned by the CNIL, that it had few repositories before the entry into force of the GDPR and that the Commission had announced a period of tolerance with regard to new breaches of the GDPR, such as the minimization or pseudonymization of data. The Restricted Committee considers that, in the present case, the aforementioned breaches justify the imposition of an administrative fine against the company for the following reasons. firstly, it notes that, contrary to what the company maintains, the shortcomings retained relate, essentially, to obligations that law no. 78-17 of January 6, 1978 as amended already imposed to data controllers and which are not born of the GDPR, including with regard to the principle of minimization and limitation of the duration of data retention. It also recalls that questions relating to the pseudonymization of data were raised well before the entry into force of the GDPR. Next, it notes that several of these breaches concern employees and in particular their right to benefit from information on the processing of their personal data. Here again, the Restricted Committee recalls that this is not a novelty introduced following the entry into force of the GDPR. Finally, it emphasizes that bank data is data that must be subject to particular vigilance by data controllers and that the Commission has not stopped supporting them on this subject for many years.Secondly, the company emphasizes its cooperation with the rapporteur and the measures put in place, as well as certain sanctions previously pronounced by the Restricted Committee. It also considers that it cannot be blamed for a lack of promptness when the hearing took place one year after the inspection carried out on its premises and when no formal notice was served on it within this period of time. restricted formation notes that while several measures have been put in place by the company to remedy certain shortcomings

in whole or in part, these were only adopted following the CNIL's inspection on May 31, 2018, with regard to the establishment of retention periods for customer and prospect data and that following the hearing of June 19, 2019, and the report, with regard to the deletion of records containing bank details of customers and the information of people on the website relating to the transfer of their data outside the European Union. Next, the Restricted Committee considers that the seriousness of certain breaches is characterized. More particularly with regard to the breach relating to the recording of telephone conversations, the Restricted Committee notes that the company recorded all the telephone conversations of its employees for several years, even though it had none usefulness and that such processing can amount to constant monitoring. It also notes that employee information about the implementation of the call recording system is particularly flawed, being either incomplete before 2016 or non-existent for employees hired by the company subsequently. seriousness of the breaches is characterized in view of the particular category of personal data processed by the company, namely bank data which is considered to be data exposing people to a risk of fraud, and therefore of prejudice, and must, this fact, be the subject of particular vigilance. Finally, the Restricted Committee also considers that the seriousness is characterized by the number of people affected by the breaches, particularly with regard to the data retention periods, this having affected several thousand people. The company then claims to be a medium-sized company and operate in a particularly competitive sector. It considers that a high administrative fine would affect its financial health and its commercial position. On this subject, the Restricted Committee considers that the company is an established player in e-commerce, and that, created well before the entry into force of the GDPR, it could not ignore the basic rules of the protection of personal data.Then, the Restricted Committee recalls that § 3 of Article 83 of the Regulation provides that in the event of multiple violations, as is the case in this case, since four breaches are identified, the total amount of the fine cannot exceed the amount set for the most serious violation. Insofar as the company is accused of breaching Articles 5 and 12 of the Regulations, the maximum amount of the fine that may be retained is 20 million euros or 4% of the annual worldwide turnover, the highest amount being retained. However, the Restricted Committee also takes into account, in determining the fine imposed, the measures that the company has taken during the sanction procedure to bring itself partially into compliance as well as the cooperation with the services of the Commission.Thirdly, concerning the need to issue an injunction, the company considers that a formal notice without penalty would be more appropriate given the speed already observed in bringing itself into compliance with several breaches.Without ignoring the company's steps to comply with the GDPR, the Restricted Committee considers that the company has not demonstrated, on the day of the closing of the

investigation, full compliance with the processing that it implements in Articles 5-1-c), 5-1 e) 13 and 32 of the Regulations. injunction.Fourthly, the Restricted Committee considers that the publication of the sanction is justified in view of the importance of the issues raised concerning the employees, as well as the nature of the data in question, while the company is a major player in the sector in which it operates. It follows from all of the above and from taking into account the criteria set out in Article 83 of the GDPR that an administrative fine of 250,000 euros, an injunction accompanied by a penalty payment as well as additional sanction of publication for a period of two years are justified and proportionate. with the obligations resulting from articles 5-1 c), article 5-1 e), 13 and 32 of regulation no. personal data: justify the end of non-punctual and non-random recordings of telephone conversations of advisers when the purpose pursued is their training or their evaluation; with regard to the breach of the principle of limitation of the duration of data retention, define and implement a retention period policy for data relating to customers and prospects which does not exceed the period necessary for the purposes for which they are collected and processed, and in particular: justify the intermediate data archiving procedure of a personal nature of customers put in place, after having operated a sorting of the relevant data to be archived and a deletion of the irrelevant data, as well as e of the starting point of this archiving; justify the restriction of employee access to personal data present in the active database to only people who need to know it; stop processing the data of prospects beyond the deadline at the end of which the company no longer contacts them (in this case two years) and stop taking into account, as the last point of contact from them, the simple opening of an email; stop keeping the email addresses and passwords of former customers at the end of the fixed period of inactivity and proceed with the purge of such data kept by the company until the date of the deliberation of the restricted formation; justify the deletion of data concerning customers at the - beyond the defined period of inactivity, which it will be up to the company to justify, and concerning prospects beyond two years of inactivity; with regard to the breach of the obligation to inform people: to inform employees about the implementation of a system for recording telephone conversations, in particular concerning the purposes pursued, the legal basis of the system, the recipients of the data from the system, the data retention period, the rights of employees, in particular access to data concerning them, the possibility of lodging a complaint with the CNIL; to provide complete information to customers, by providing information relating to the different legal bases of the processing implemented by the company; with regard to the breach of the obligation to ensure the security of personal data, take all measures, for all the processing of personal data implemented, to preserve the security of this data and to prevent unauthorized third parties from having access to it pursuant to Article 32 of the GDPR, in particular: implement a password

management policy against painful, with regard to customer accounts according to one of the following methods; passwords are composed of at least twelve characters, containing at least one uppercase letter, one lowercase letter, one number and one special character; password are composed of at least eight characters, containing three of the four categories of characters (uppercase letters, lowercase letters, numbers and special characters) and are accompanied by an additional measure such as the delay of access to the account after several failures (temporary suspension of access, the duration of which increases as attempts are made), the establishment of a mechanism to guard against automated and intensive submissions of attempts (e.g. captcha) and/or the blocking of the account after several unsuccessful authentication attempts (maximum ten); subject the injunction to a penalty payment of 250 (two hundred and fifty) euros per day of delay at the end of a period of 3 (three) months following the notification of this deliberation, the supporting documents of compliance must be sent to the restricted committee within this period; for breaches of Articles 5-1 c), 5-1 e), 13 and 32 of the GDPR, pronounce on against company X an administrative fine of 250,000 (two hundred and fifty thousand) euros; make public, on the CNIL website and on the Légifrance website, its deliberation, which will no longer identify the company at the end of a period of two years from its publication. Chairman Alexandre LINDEN This decision may be appealed to the Council of State within two months of its publication. notification.