Deliberation SAN-2022-008 of March 31, 2022 National Commission for Computing and Liberties Nature of the deliberation: Sanction Legal status: In force Date of publication on Légifrance: Wednesday April 06, 2022 Deliberation of the restricted committee n°SAN-2022-008 of 31 March 2022 relating to the injunction issued against company X by deliberation no. SAN-2020-003 of July 28, 2020

The National Commission for Computing and Liberties, meeting in its restricted formation composed of Messrs Alexandre LINDEN, president, Philippe-Pierre CABOURDIN, vice-president, of Mesdames Anne DEBET and Christine MAUGÜE, and of Mr Alain DRU, members; 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 no. 78-17 of January 6, 1978 as amended relating to information technology, files and freedoms, in particular its articles 20 and following; Considering decree no. 2019-536 of May 29, 2019 taken for the application of the law

no. 78-17 of January 6, 1978 as amended 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; deliberation no SAN-2020-003 of July 28, 2020 pronouncing a sanction against company X; Having regard to the elements transmitted by company X on November 5, 2020, April 7 and December 16, 2021 and February 2, 2022; Having regard to the other documents in the file; After deliberating at its meeting of February 10, 2022, adopted the following decision: I. Facts and procedure Company X (hereinafter "the company"), specializes in the distance selling of shoes. By its deliberation no. 2020-003 of July 28, 2020, notified on August 4, 2020, the Restricted Committee, among other provisions, issued an injunction to bring the processing into compliance with the obligations resulting from Articles 5-1 c), 5- 1 e), 13 and 32 of Regulation No. 2016/679 of April 27, 2016 on data protection (hereinafter GDPR) The injunction was formulated in these terms: with regard to the breach of the principle of minimization of data to personal nature: justify the end of non-punctual and non-random recordings of the 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 put implements 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 archiving procedure of the personal data of the 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 the starting point of this archiving; justify the the restriction of employee access to personal data present in the

active database to only those who need to know it; to stop processing the data of prospects beyond the period after which the company no longer contacts them (in two years) and stop taking into account, as the last point of contact from the latter, the simple opening of an e-mail; stop keeping the e-mail addresses and hashed passwords of former customers at the end of the period of fixed inactivity and proceed with the purging of such data kept by the company until the date of the deliberation of the restricted formation; justify the deletion of data concerning the ients 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 persons: inform employees about the implementation of a device for recording telephone conversations, in particular concerning the purposes pursued, the legal basis of the device, the recipients of the data from the device, the retention period of the data, 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 put in place implementation, making it possible 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: implementing a binding password management policy, as regards 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; passwords 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 in accessing the account after several failures (temporary suspension of the access whose duration increases as attempts are made), the implementation of a mechanism to guard against automated and intensive submissions of attempts (e.g.: "captcha") and/or the b locking of the account after several unsuccessful authentication attempts (a maximum of ten); This injunction was accompanied by a penalty payment of 250 euros per day of delay at the end of a period of three months following the notification of the proof of compliance must be sent to the restricted training within this period. ) a letter in which it presented the measures put in place to comply with the injunction. By letter dated February 2, 2021, the chairman of the Restricted Committee asked the company for additional information, in particular concerning the procedures for the retention by the company of data relating to its customers. The company responded to this request on April 7, 2021 and then supplemented its response with additional mailings on

December 16, 2021 and February 2, 2022.II.Reasons for the decisionA.On the measures taken in connection with data minimizationThe restricted committee is concerned that the responses and supporting documents provided by the company show that it has ceased to record, for the purposes of training its employees, all the telephone calls received by the employees of its customer service department and that it has reduced by substantially the proportion of the recordings it carries out. Consequently, the Restricted Committee considers that the company has complied with this aspect of the injunction. B. On the measures taken in connection with the retention of data Firstly, if concerning the management of employee access to the personal data necessary for the performance of their duties, it appears from the answers and supporting documents provided by the company that only the three people, whose functions within the company justify it, now have access to the data (for example, to carry out research and analyzes in the event of fraud, complaint or judicial requisition). The Restricted Committee considers that these measures satisfy this part of the injunction.Secondly, with regard to the retention of data for prospecting purposes, the Restricted Committee notes that in its response to the injunction, the company indicated that it had changed the starting point from which the period allowing to determine the inactivity of a prospect was calculated, to no longer take into account the simple opening of an email but for example the last order or the last connection to the account. In addition, the company has justified having deleted the data which was retained pursuant to its former retention period policy. The Restricted Committee considers that, under these conditions, the appropriate measures have been put in place to comply with the injunction and it observes that keeping prospects' data for three years from these identified starting points to calculate the duration of inactivity of prospects is not excessive within the meaning of Article 5(1)(e) of the GDPR.Thirdly, with regard to the retention of data beyond a period of three years from the inactivity of the users in a form that no longer allows the identification of the persons to whom they relate, the Restricted Committee notes that during the investigation of the follow-up to the injunction, the company gradually changed the storage methods envisaged so that the stored data no longer made it possible to re-identify the s people. In this sense, the company has in particular: reduced the number of fields kept in its database; stopped keeping the internal identifier assigned to each customer; divided the data kept into three separate tables, in which the data relating to a same person are paid at different times, so that it is not possible to make the link between the data relating to the same person between the three tables. The Restricted Committee considers that the measures taken by the company are such as to no longer allow people to be re-identified. Finally, with regard to keeping the email addresses and passwords of former customers in hashed form in order to allow them to reconnect to their account, the company indicated stop offering this

functionality and therefore end the retention of this information for this purpose. Consequently, the Restricted Committee considers the company has satisfied this section of the injunction.C.On the measures taken with regard to the information of personsIn the first place, with regard to the information of employees regarding the recording of telephone calls, it appears from the answers and supporting documents provided by the company that the latter has had each of its employees sign an information note, containing all the information referred to in Article 13 of the GDPR.Secondly, the Restricted Committee notes that the company has completed the confidentiality policy accessible on its website in order to include a description of the legal bases on which its processing is based. Consequently, the Restricted Committee considers that the company has complied with this aspect of the injunction. D. On the measures taken in link with the security of the processingThe company has produced supporting documents from which it appears that the passwords allowing access to customer accounts must now be composed of at least 8 characters, including at least minus one lowercase, uppercase, number or special character. It explains that it also implemented a measure to delay access to accounts. The Restricted Committee considers that these measures satisfy this part of the injunction. Consequently, the Restricted Committee considers that Company X has satisfied all of of the injunction. This decision will be made public as was deliberation no. SAN 2020-003 of July 28, 2020. FOR THESE REASONS there is no need to liquidate the penalty; to make public, on the CNIL website and on the Légifrance website, its deliberation, which will no longer identify company X by name as of August 5, 2022. Chairman Alexandre LINDEN