Deliberation SAN-2018-009 of September 6, 2018 National Commission for Computing and Liberties Nature of the deliberation: Sanction Legal status: In force Date of publication on Légifrance: Thursday, September 20, 2018 Deliberation of the restricted committee no. SAN-2018-009 of 6 September 2018 pronouncing a pecuniary penalty against company X The National Commission for Computing and Liberties, meeting in its restricted formation composed of Mr. Jean-François CARREZ, Chairman, Mr. Alexandre LINDEN, Vice-Chairman, Ms. Dominique CASTERA, Ms. Marie-Hélène MITJAVILE and Mr. Maurice RONAI, members; Having regard to Convention No. 108 of the Council of Europe of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data ;Having regard to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of these data; Considering the law n° 78-17 of January 6, 1978 modified relating to data processing, the files and freedoms, in particular its articles 45 and following; Considering the decree n° 2005-1309 of October 20, 2005 modified taken for the application of law n ° 78-17 of January 6, 1978 relating to data processing, files and freedoms, modified by decree n ° 2007-451 of March 25, 2007; Having regard to deliberation n ° 2013- 175 of July 4, 2013 adopting the internal regulations of the National Commission for Computing and Liberties; Having regard to decision no. 2016-292C of October 21, 2016 of the President of the National Commission for Computing and Liberties to instruct the Secretary General to carry out or have carried out a verification mission with company X; Having regard to the decision of the President of the Commission no. 2017-049 of July 26, 2017 giving formal notice to company X; Having regard to the decision of the President of the Committee appointing a rapporteur to the r formation restricted, dated April 19, 2018; Having regard to the report of Mrs Marie-France MAZARS, reporting auditor, notified by hand to company X on June 1, 2018; Having regard to the written observations of company X received on July 10, 2018, as well as the oral observations made during the restricted committee meeting; Having regard to the other documents in the file; Were present at the restricted committee meeting of July 12, 2018: Ms. Marie-France MAZARS, Statutory Auditor, in her report; of representatives of company X:[…];[…];As counsel for company X:[…];The representatives of company X who spoke last;Adopted the following decision:Facts and procedureThe company X (hereinafter the company ) is a simplified joint-stock company, whose registered office is located […]. A secondary establishment of the company is located at […]. The company has a remote surveillance activity for elevators and car parks. It employs 14 people, including 13 teleoperators, and achieved a turnover of 816,691 euros in 2017. On June 21, 2015, the National Commission for Computing and Freedoms (hereinafter CNIL or the Commission) was a complaint concerning the

installation of a video surveillance/video protection system in the company's premises located […]. Pursuant to decision no. 2016-292C of the President of the Commission of October 21, 2016, a delegation from the CNIL carried out an inspection mission at the company's premises on November 3, 2016. During the inspection, the delegation observed that a biometric clocking-in device for the purpose of controlling employee schedules was implemented, without authorization from the CNIL. It was also noted that a device for recording telephone calls was put in place without the employees being informed. In addition, it was noted that during an incoming call, the interlocutors were in particular not informed of the identity of the data controller and of the right of opposition they have. In addition, the CNIL delegation noted that the passwords allowing access to the Windows environment and to the software […] containing the data recorded via the biometric device were composed of 9 alphanumeric characters and 4 numeric characters respectively. The delegation noted, on the one hand, that access to the company's management tool called […] is via a password made up of 6 alphabetical characters and, on the other hand, an absence of automatic locking of sessions on certain workstations. Finally, it was informed that the software access password […] had not been changed since 2011. to the company by letter dated November 7, 2016. In view of the breaches noted, the President of the CNIL gave the company formal notice, by decision no. 2017-049 of July 26, 2017, within three months of: not collecting and process only adequate, relevant and non-excessive data with regard to the purposes for which they are collected and their subsequent processing, in particular ceasing to use the biometric fingerprint recognition device to control employee schedules and delete all the data that has been collected by such a device; inform the persons concerned, in accordance with the provisions of article 32 of the law of January 6, 1978 as amended, in particular concerning the call recording device telephone calls: inform employees, in particular bringing to their attention the particulars relating to the identity of the data controller, the purpose of the processing, the recipients of the data from the device, the retention period of the data processed as well as the rights of data subjects, the right to object in this case taking the form of deactivation of the recording or access to a telephone line not connected to the recording system for making personal calls or internal to the company; to inform the interlocutors in the event of outgoing and incoming calls by an oral mention at the beginning of the conversation integrating for example the possibility of opposing the recording as well as a reference to a site internet or to a telephone key for the delivery of all the prescribed information; take all necessary measures to guarantee the security and confidentiality of the personal data processed, in particular by: setting up a rigorous and binding policy imposing strong passwords for access to the Windows environment, the software […], as well as the data management tool company […]: passwords are composed of

at least 12 characters, containing at least one uppercase letter, one lowercase letter, a number and a special character or passwords are composed of at least 8 characters, containing 3 of the 4 categories of characters (uppercase letters, lowercase letters, numbers and special characters) and are accompanied by an additional measure such as for example the delay in access to the account after several failures (temporary suspension of access whose duration increases with attempts), the implementation of a mechanism to guard against automated and intensive submissions of attempts (e.g. captcha) and/or the blocking of the account after several authentication attempts unsuccessful ication (maximum 10). In all cases, the passwords of the company's personnel must be regularly renewed; establishing an automatic locking by default of computer workstation sessions in the event of prolonged inactivity (after 10 minutes, for example); justify to the CNIL that all of the aforementioned requests have been complied with, and this within the time limit. This decision was notified to the company on July 31, 2017. In the absence of a response by the deadline for the formal notice, a follow-up letter was sent to the company on October 20, 2017, which received it on October 24, 2017. following October. By letter dated October 20, 2017, the company responded to the formal notice from the Chairman. It specified that the code clocking device was no longer operational and that the recorded data was purged regularly. However, the President of the CNIL again asked the company, by letter of November 21, 2017, to stop having use of a fingerprint recognition clocking device (and not a code clocking device). It also reminded him that it was required to inform people about the device for recording telephone calls as well as the security of the data processed. On 1 December 2017, the company sent back to the Commission its answer dated of the previous October 20, explaining that this and the reminder letter from the CNIL dated the same day had crossed paths. Considering that this letter did not respond to the request for additional information of November 21, 2017, the President of the CNIL sent a follow-up letter to the company on January 12, 2018, received the following January 17. On January 24, 2018, the company informed the President that the biometric clocking device was no longer operational. She specified that a memo informing employees of the implementation of a telephone call recording device had been posted on an information board and that an automatic locking of computer workstation sessions had been put in place. in place. In order to verify whether the measures announced by the company had been put in place, a delegation from the CNIL carried out an on-site inspection mission on March 29, 2018, pursuant to the decision of the President of the CNIL no. ° 2016-292C cited above. The delegation noted that the biometric device allowing the control of employees' schedules was still installed and that no security measures had been put in place at the employees' workstations. In addition, the delegation noted that were recorded within the software […], traces of clocking by fingerprint

between August 30, 2011 and March 28, 2018. Moreover, with regard to the recording of calls, the delegation found that while a note informed employees of the identity of the data controller, the time of registration, the duration of data retention and the purpose pursued by the processing, it did not contain any information relating to the rights of persons. With regard to the information of the company's interlocutors, the delegation noted that an information message was broadcast for incoming calls but that it may be truncated when the operator took the call before it ends. In addition, it was found that no information message relating to the recording of calls was delivered by the operators to the interlocutors in the event of outgoing calls. Minutes No. 2016-292/2 of 29 March 2018 was sent to the company by post, received on the following April 4. Subsequently, the company informed the CNIL, by letter dated April 13, 2018, that it had appointed a data protection officer and implemented implemented several measures to meet the requirements of the formal notice. It specified in particular that the biometric fingerprint recognition box for checking employee schedules had been dismantled and that automatic locking of workstations had been put in place. She also indicated that measures had been taken to ensure that the information message delivered for incoming calls was not truncated. the Commission appointed Mrs Marie-France MAZARS as rapporteur, on April 19, 2018, on the basis of Article 46 of the amended law of January 6, 1978 relating to data processing, files and freedoms (hereinafter Data-processing law and Freedoms or law of January 6, 1978 modified). At the end of his investigation, the rapporteur notified Company X, on June 1, 2018, by bearer, of a report detailing the breaches of the law that he considered constituted in this case. This report proposed to the restricted formation of the Commission to pronounce a pecuniary sanction which could not be less than fifty thousand (50,000) euros and which would be made public. 2018 indicating to the company that it had one month to submit its written observations. On July 10, 2018, the company produced written observations on the report, through its counsel, reiterated orally during of the Restricted Committee meeting of the following July 12. Reasons for the decision1. On the breach of the obligation to ensure the adequacy, relevance and non-excessive nature of the dataThe 3° of article 6 of the law of January 6, 1978 as amended, in the version applicable on the day of the facts, provides that the personal data are adequate, relevant and not excessive in relation to the purposes for which they are collected and their subsequent processing. The company was given formal notice on July 26, 2017 to stop using the biometric fingerprint recognition device to monitor employee schedules and to delete all data collected by the employee. that the biometric clocking device was no longer operational and that a regular purge of the recorded data was carried out, the delegation noted, during the second CNIL check of March 29, 2018, that the biometric box had not been uninstalled, that some employees continued to use it and that biometric

data was kept for the period from August 30, 2011 to March 28, 2018. The rapporteur maintains that until the day of the inspection of March 29, 2018, carried out after the formal notice of the President of the CNIL, the company had always used the biometric device for the purpose of checking the hours of the employees and that no exceptional circumstances requiring the use of the b iometry for this purpose is not invoked by the company. In defence, the company indicates that the biometric device in question was acquired in 2011, by the former manager. It specifies that it had not been used since March 2017 and that if the fingerprints of the former employees were still recognized by the device, they no longer pointed. In addition, the company maintains that the system in question has been dismantled. and destroyed since the second inspection by the Commission. Firstly, the Restricted Committee notes that the company had set up a biometric device whose purpose was to manage employees' schedules without authorization from the CNIL, as noted by the delegation of the CNIL on November 3, 2016. In this regard, the Restricted Committee notes that despite the formal notice from the President of the CNIL of July 26, 2017 and the letter of October 20, 2017 asking the company to stop using the biometric device in question, it appears from the findings made by the Commission delegation on 29 March 2018 that it was still installed and that the data recorded in the software […], since 30 August 201 1, had not been purged. Although the Restricted Committee notes that, according to the company, the data collected by the biometric device was no longer used by the payroll department, it is nevertheless established that certain employees continued to use and therefore that biometric data of employees were recorded and stored. Moreover, there is nothing to establish, as the company maintains, that the biometric device was used by the employees in disregard of the directives given by it, the company having produced no document attesting to such instructions.Secondly, the restricted formation recalls that biometric data have the particularity of being unique and therefore make it possible to identify an individual based on their physical or biological characteristics. As such, they benefit from a particularly protective regime. The Restricted Committee recalls that, since 2012, the Commission has excluded the use of any biometric device for the purpose of managing employee schedules. If the use of a biometric device, for such a purpose, can be the subject of a request for authorization on the basis of 8° of I of article 25 of the law of January 6, 1978 as amended, the person in charge of the processing must nevertheless demonstrate that there are exceptional circumstances based on a specific security imperative. employees. It follows from the foregoing that the company has collected excessive data with regard to the purposes for which they were collected. On the basis of these elements, the Restricted Committee considers that the breach of 3° of Article 6 of the amended law of January 6, 1978 is constituted, the company not having complied with the decision of the President of the

CNIL n° 2017-049 of July 26, 2017 within the time limit. ion to inform people Article 32 of the amended law of January 6, 1978, in the version applicable on the day of the events, provides that: I.- The person from whom personal data concerning him/her are collected is informed, unless it has been previously, by the controller or his representative: 1° The identity of the controller and, where applicable, that of his representative; 2° The purpose pursued by the processing to whom the data is intended; 3° The mandatory or optional nature of the answers; 4° The possible consequences, with regard to him, of a lack of answer; 5° The recipients or categories of recipients of the data; 6° The rights that it derives from the provisions of section 2 of this chapter, including that of defining directives relating to the fate of its personal data after its death; 7° Where applicable, transfers of personal data envisaged to a Statenot a member of the European Community; 8° The retention period of the categories of data processed or, if this is not possible, the criteria used to determine this period. When such data is collected by means of questionnaires, these must mention the prescriptions appearing in 1°, 2°, 3° and 6°. The company was given formal notice to inform people about the implementation of a device for recording telephone calls, in accordance with the aforementioned article 32. During the second inspection on March 29, 2018, the delegation noted that the information message broadcast for incoming calls could be truncated when the operator takes the call before the end of its broadcast. It also noted that no information message relating to the recording of calls is delivered by the operators to the interlocutors in the event of outgoing calls. Finally, it was noted that the information note entitled Recording of telephone communications, intended for the company's employees, does not contain any information relating to their rights. The rapporteur noted that the company had not provided any evidence that the note information intended for employees had been completed and that the message broadcast for incoming calls could not be truncated. He therefore specified that he was not assured that the persons were duly informed of the implementation of such a system, of its purpose, of the identity of the data controller and of their right to oppose it. In defence, the company maintains that the recordings of incoming telephone calls are managed by an external service provider and that it cannot be held responsible for the failure relating to the failure to inform people about incoming calls. It specifies that it informed the latter of the problems encountered by letter dated April 5, 2018 and that it only obtained satisfaction from it on the following July 5. The restricted committee notes that, contrary to the company's assertions, it is up to it as head of processing, including when it uses a service provider, to ensure compliance with the obligations and rights provided for by the Data Protection Act and in particular that complete information relating to the implementation of processing is provided to data subjects, in accordance with Article 32 of the aforementioned law. the CNIL. The company had therefore

not taken steps with its service provider within the time limit set by the formal notice. Finally, the Restricted Committee notes that the company has not provided any evidence that the information note for employees has been completed. regarding the rights they hold under the Data Protection Act. On the basis of these elements, the Restricted Committee considers that the breach of Article 32 of the amended law of January 6, 1978 has been constituted, the company not having complied with the decision of the President of the CNIL No. 2017 -049 of July 26, 2017 within the time limit. On the breach of the obligation to ensure the security and confidentiality of data that: The controller is required to take all useful precautions, with regard to the nature of the data and the risks presented by the processing, to preserve the security of the data and, in particular, to prevent them from being distorted, damaged, or unauthorized third parties have access to it. The company has been put on notice to put in place a rigorous and restrictive policy imposing strong passwords for access to the Windows environment, the […] software, as well as the […] tool and introduce an automatic default locking of computer workstation sessions in the event of prolonged inactivity. In a letter dated January 24, 2018, the company specified that an automatic locking of workstation sessions after four of inactivity had been put in place. During the second inspection of March 29, 2018, the CNIL delegation noted that the workstation with the software […] was accessible from an office open to the entire staff and that it was not locked automatically in the event of prolonged inactivity. It was also found that the password used to display the history of events recorded in this software was made up of 4 digits. In addition, the delegation noted that the operator session access passwords were made up of 6 characters and that the telephone recordings were accessible to all telephone operators from the call management software. finally noted that the workstations of the employees were not locked automatically in the event of inactivity. The rapporteur maintains that the insufficient robustness of the passwords and the absence of automatic locking of the sessions of the workstations do not to ensure the security of the data processed by the company and to prevent unauthorized third parties such as teleoperators, but also persons called upon to intervene on the premises, from having access to said personal data. In defence, the company does not dispute the facts found but minimizes the risk relating to the personal data it processes. It maintains in particular that this data is neither exposed on the Internet nor accessible to unauthorized third parties since its premises are secure and do not receive the public. It also indicates that the data processed is neither sensitive data nor confidential information. The Restricted Committee notes that it is up to company X to implement security measures intended to ensure the security of personal data personnel it deals with. The restricted training reminds that the workstations of the agents must be configured so that they lock automatically beyond a period of inactivity and must be

protected by a sufficiently strong password. These provisions are likely to limit the risks of fraudulent use of an application, in the event of the agent's absence from his workstation. a recommendation relating to passwords, the Commission recommends, when authentication is based solely on an identifier and a password, that the password contains at least 12 characters containing at least one uppercase letter, one lowercase letter, one number and a special character or contains at least 8 characters, containing 3 of these 4 categories of characters and is accompanied by an additional measure such as for example the delay in access to the account after several failures, (temporary suspension of access whose the duration increases as attempts are made), the implementation of a mechanism to guard against automated and intensive submissions of attempts (eg captcha) and/or the blocking of the account after several their unsuccessful authentication attempts. The Restricted Committee notes that while the company indicates that it has implemented strong passwords on all workstations, it does not provide proof of this. It also notes that the automatic locking of workstations was not put in place until April 2018, i.e. five months after the expiry of the compliance period granted to it. Finally, it recalls that the obligation security referred to in Article 34 of the Data Protection Act concerns all personal data and not only so-called sensitive data. On the basis of all of these elements, the Restricted Committee considers that the breach of Article 34 of the amended law of January 6, 1978 has been established, the company not having complied with the decision of the Chairman of the CNIL n° 2017-049 of July 26, 2017 within the time limit.On penalties and publicityUnder the terms of I of article 45 of the amended law of January 6, 1978, in the version applicable on the day of the facts: When the person responsible processing does not comply with the obligations arising from this law, the President of the National Commission for Computing and Liberties may give him formal notice to put an end to the observed breach within a period that he sets. In the event of extreme urgency, this period may be reduced to twenty-four hours. If the data controller complies with the formal notice addressed to him, the chairman of the commission declares the procedure closed. Otherwise, the restricted committee may pronounce, after a contradictory procedure, the following sanctions: 1° A warning; 2° A pecuniary sanction, under the conditions provided for in Article 47, with the exception of where the processing is carried out by the State; 3° An injunction to cease the processing, when this falls under Article 22, or a withdrawal of the authorization granted pursuant to Article 25. When the breach found cannot be brought into compliance within the framework of a formal notice, the restricted committee may pronounce, without prior formal notice, and after an adversarial procedure, the sanctions provided for in this I. paragraphs 1 and 2 of article 47 of the aforementioned law, in the version applicable on the day of the facts, specify that: The amount of the financial penalty provided for in I of article 45 is

proportionate to the seriousness of the breach committed and to the benefits derived from this failure. The restricted formation of the Commission Nationale de l'Informatique et des Libertés takes into account in particular the intentional or negligent nature of the breach, the measures taken by the data controller to mitigate the damage suffered by the persons concerned, the degree of cooperation with the commission in order to remedy the breach and mitigate its possible negative effects, the categories of personal data concerned and the manner in which the breach was brought to the attention of the commission. The amount of the penalty may not exceed 3 million euros. The company maintains that the restricted training must take into account, in determining the sanction, the specificity of its activity and its financial difficulties but also the reaction times of its various service providers preventing it from complying. demonstrated that the breaches of Articles 6-3°, 32 and 34 of the law of January 6, 1978, as amended, persisted beyond the time limit set by the formal notice from the President of the Commission. The Restricted Committee considers that the seriousness breaches is characterized in view of the special category of personal data processed by the company. Biometric data insofar as they relate in particular to physical and biological characteristics - allowing the identification or unique authentication of a natural person - benefit from a particularly protective regime. given, but also taking into account the company's partial compliance with the law, on the day the restricted committee rules, and the company's financial situation, the restricted committee considers that the facts of the case justify the issuance of a financial penalty in the amount of 10,000 (ten thousand) euros. In addition, in view of the established breaches, their persistence for 15 months, despite the numerous diligences carried out with regard to it by the services of the CNIL, the restricted committee decides to make its decision public. It considers it necessary to make data controllers aware of the rights and obligations arising from the Data Protection Act , in particular, to the importance of responding to the requests of the President of the Commission and of effectively implementing the required measures.FOR THESE REASONSThe Restricted Committee of the CNIL, after deliberation, decides to: against company X a pecuniary penalty in the amount of 10,000 (ten thousand) euros; make its decision public, which will be anonymized at the end of a period of two years from its publication. The Chairman Jean-François CARREZ This decision may be appealed to the Council of State within two months of its notification.