Deliberation SAN-2019-006 of June 13, 2019 National Commission for Computing and Liberties Nature of the deliberation: Sanction Legal status: In force Date of publication on Légifrance: Tuesday June 18, 2019 Deliberation of the restricted committee no. SAN-2019-006 of 13 June 2019 pronouncing a sanction against the company XLThe National Commission for Computing and Liberties, meeting in its restricted formation composed of Mr. Alexandre LINDEN, Chairman, Mr. Philippe-Pierre CABOURDIN, Vice-Chairman, Ms. Anne DEBET and Mrs Sylvie LEMMET, members; Having regard to Council of Europe Convention No. 108 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 April 27, 2016 relating to the protection of personal data and the free movement of such data; ers and freedoms, in particular its articles 20 and following; Considering the decree n ° 2019-536 of May 29, 2019 taken for the application of the law n ° 78-17 of January 6, 1978 modified relating to data processing, files and to freedoms; Having regard to deliberation no. 2013-175 of July 4, 2013 adopting the internal regulations of the National Commission for Computing and Freedoms; Having regard to decision no. 2018-031C of February 2, 2018 of the President of the Commission National Computing and Liberties to instruct the Secretary General to carry out or have carried out a mission to verify all the processing of personal data implemented by company X; Having regard to the decision of the President of the National Commission for Computing and Liberties appointing a rapporteur to the restricted committee, dated January 29, 2019; Having regard to the report of Mr. Éric PÉRÈS, commissioner rapporteur, of February 11, 2019; Having regard to the written observations submitted by the s company X on March 12, 2019; Having regard to the observations in response of the commissioner-rapporteur of March 26, 2019; Having regard to the observations in response submitted by company X on April 11, 2019 as well as the oral observations made during the restricted training session; the other documents in the file; Were present at the restricted committee meeting of April 18, 2019:- Mr. Éric PÉRÈS, auditor, heard in his report;- As a representative of company X:- […]; - As counsel for Company X:[…]. The company having the last word; After having deliberated, adopted the following decision: I. Facts and procedure1. Company X (hereinafter the company) is a simplified joint-stock company whose registered office is located […]. Its activity is the sworn and free translation of documents (legal, financial, civil status translation). The company employs nine people and achieved a turnover of 885,739 euros in 2017 and a negative net result of 110,844 euros.2. Between 2013 and 2015, the National Commission for Computing and Liberties (hereinafter the CNIL or the Commission) received four complaints concerning the installation of a video surveillance system on the premises of the company. As part of the investigation of these complaints, the CNIL twice, by

letters dated October 18, 2013 and June 2, 2016, drew the company's attention to the rules governing the implementation of a video surveillance and video protection and on the need that the device does not interfere unduly with respect for the privacy of employees in the workplace. The Commission also asked the company to send it additional information on the system put in place. The company confirmed, by letters of February 6, 2014 and July 1, 2016, that this device was justified for the sake of the safety of property and people and that it was not used to monitor the activities of personnel.3. Despite explicit reminders of the legal framework applicable to video surveillance devices, four new complaints were sent to the CNIL in 2017, highlighting the presence of cameras in the workspace of employees, placing them under constant surveillance. 4. Pursuant to decision no. 2018-031C of the President of the Commission of February 2, 2018, a delegation from the CNIL carried out an inspection mission at the company's premises on February 16, 2018.5. During the check, the delegation noted the presence of three cameras in the company's premises, including a camera installed in the translators' office, not accessible to the public. This camera filmed six workstations and a cabinet containing the company's working documents.6. The delegation noted that the video surveillance system was not the subject of any formal information intended for employees. She observed that the camera installed in the translators' office made it possible to view the workstations continuously. The control operation also made it possible to establish that the retention period of the images exceeded that necessary for the purpose indicated by the company and that, moreover, the measures put in place by the company for access to computer stations and the professional mailbox did not ensure the security and confidentiality of the data.7. Report no. 2018-031 drawn up following the on-site inspection was notified to the company by letter dated February 20, 2018.8. Additional information was provided by the company by letter dated March 12, 2018 and email dated March 22, 2018.9. In view of the shortcomings noted after taking into account the additional elements provided, the President of the CNIL gave the company formal notice, by decision no. 2018-029 of July 26, 2018, within two months, to:- modify the video surveillance device so that it is proportionate with regard to the purpose pursued, in accordance with the now applicable provisions of c) of article 5 of Regulation (EU) 2016/679 of 27 April 2016 relating to data protection, and in in particular: o stop placing employees under constant surveillance, for example, by reorienting or moving the cameras or even by proceeding with the implementation of dynamic masks when viewing the images, in particular concerning the camera located in the office of the translators;- implement a retention period policy for personal data that does not exceed the period necessary for the purposes for which they are collected, in accordance with the provisions ons of e) of Article 5 of the aforementioned Regulation now applicable, in particular, not to keep the recordings of

images from the video surveillance device beyond a period of fifteen days; - inform the persons whose data is processed, in particular with regard to the video surveillance system, in accordance with the provisions of Articles 12 and 13 of Regulation (EU) 2016/679 now applicable, and in particular: o inform any person, for example by posting signs, of the implementation of a video surveillance system, specifying the purpose of the processing, the retention period and the recipients of the data, the identity of the data controller and the procedures for exercising the rights; - take any measures, for all the processing of personal data implemented, making it possible to preserve the security of this data and to prevent unauthorized third parties from having access to it pursuant to art. Article 32 of Regulation (EU) 2016/679 now applicable, in particular: o ensuring that access to employees' computer stations is subject to authentication by each user, for example via an individual identifier and password; o implement a restrictive password management policy, both for the image viewing software installed on the manager's computer station and for the employees' Windows accounts, according to one of the following methods: § the passwords are composed of at least twelve characters, containing at least one uppercase letter, one lowercase letter, one number and one special character; § passwords consist of at least eight characters, containing three of the four character categories (uppercase letters, lowercase letters, numbers and special characters) and are accompanied by an additional measure such as account access timeout 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);§ storage of passwords in hashed form (for example, using the SHA256 algorithm with the use of a salt); in all cases, passwords must be regularly renewed; o implement measures to ensure the traceability of access to the mailbox used, for example by implementing for each employee individualized access and by removing access to the mailbox for employees leaving the company.10. This decision was notified to the company on July 30, 2018.11. The company, by letter dated September 10, 2018, responded to the formal notice on the various breaches of which it was accused. She told the Commission that the camera installed in the translators' office only made it possible to view two employees without the workstations being filmed continuously. She specified that the storage period of the images had been modified and set at fifteen days, the images being automatically destroyed after this period. Nevertheless, it confirmed that access to employees' workstations was without a password so that each employee could have access to the project files of other employees in the event of their absence. It also confirmed that the Windows session of the manager's workstation was accessible without a password, in particular so that the

accountant or the project manager could have access to it. Similarly, it indicated that exchanges between the company and its customers are carried out by means of a generic e-mail address accessible by all employees by means of a shared eight-character password. With regard to informing employees about the existence of the cameras, the company stated that this installation was very visible and that a large panel was displayed at the entrance to the premises, bearing the name and telephone number of the responsible.12. Insofar as the supporting documents produced by the company appeared insufficient, where its statements contradicted the findings made during the on-site inspection of February 16, 2018 and where it had expressed its intention not to take measures to ensure data security , a CNIL delegation carried out a new on-site inspection mission on October 10, 2018, on the basis of the aforementioned decision of the President of the CNIL No. 2018-031C.13. During this mission, the delegation noted that the camera present in the employees' office was constantly filming employees, without modification since the initial inspection of February 16, 2018. It also noted that no material information intended for employees was had been carried out, specifying in particular the purpose of the processing, the retention period, the recipients of the data, the identity of the data controller and the procedures for exercising the rights. Finally, the delegation noted that no password management policy had been implemented with regard to access to employees' computer stations or to the company's electronic messaging system.14. Minutes no. 2018-031-2 of October 10, 2018 were notified to the company on October 19, 2018.15. Following the on-site inspection, the company spontaneously informed the CNIL, by letter dated October 15, 2018, that it had partially obstructed the camera filming the translators' office, with adhesive tape, and that she had redirected the camera to the cupboard containing the documents (order forms and sworn translations) to be protected. It also indicated that it had drawn up an information note for staff relating to the installation of cameras in the premises. The company claimed to have created passwords on all computer workstations respecting the recommended number and character categories.16. For the purpose of investigating these elements, the Chairperson of the Commission appointed Mr Éric PÉRÈS as rapporteur, on January 29, 2019, on the basis of Article 47 of the law of January 6, 1978 amended in the version applicable to the day of designation.17. At the end of his investigation, the rapporteur had company X notified by hand, on February 12, 2019, of a report detailing the breaches of Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 relating to the protection of data (hereinafter the Regulation) which he considered constituted in this case.18. 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), 12, 13 and 32 of the Regulation, accompanied by a penalty payment of 1,000 euros per

day of delay at the end of a period of two days following the notification of the deliberation of the restricted formation as well as an administrative fine of an amount of seventy-five thousand (75,000) euros which would be made public. It also proposed that this decision be made public and anonymised after the expiry of a period of two years from its publication.19. Also attached to the report was a notice to attend the restricted committee meeting of April 18, 2019, indicating to the company that it had one month to submit its written observations.20. On March 8, 2019, the company requested a closed session due to confidentiality related to its translation activity. The Chairman of the Restricted Committee rejected his request by letter dated March 21, 2019.21. On March 12, 2019, the company, through its counsel, filed submissions. The rapporteur replied on 26 March 2019.22. On 11 April 2019, the company produced new observations in response to those of the rapporteur.23. During the restricted training session of April 18, 2019, the company renewed its request for a closed session, in respect of which the chairman of the restricted training confirmed his refusal to grant it, considering that no risk breach of public order or the protection of secrets protected by law was characterized. All of the observations presented during the investigation were reiterated orally by the rapporteur and the company. In view of the information provided by the company, the rapporteur decided to lower the amount initially proposed for the administrative fine and proposed an amount of 50,000 euros.II. Reasons for decision1. On the failure to ensure the adequacy, relevance and non-excessive nature of the data24. Article 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 (data minimization) .25. The company was given formal notice by decision dated July 26, 2018 and notified on July 30, 2018, within two months, to modify the video surveillance system so that it is proportionate with regard to the purpose pursued. In particular, he was asked to stop placing the employees under constant surveillance, for example by reorienting or moving the cameras or even by proceeding with the implementation of dynamic masks when viewing the images, concerning the camera located in the translators office.26. The company stated, in its response letter of September 10, 2018, that the disputed camera only made it possible to partially view two people and that it did not make it possible to continuously film the workstations of employees.27. The delegation noted, during the second check carried out on 10 October 2018, that the video surveillance device installed in the translators' office showed no changes since the initial check on 16 February 2018 and that it still allowed constant and permanent monitoring of six employees.28. By letter of 15 October 2018, the company informed the Commission that it had partially obstructed the camera with adhesive tape and redirected the camera to the cabinet containing the documents to be protected. As the photograph produced established that the camera was

still aimed at at least one workstation, the rapporteur considered that the company had not complied at the end of the period set out in the formal notice.29. In its memorandum of March 12, 2019, the company indicated in defense that it had removed the camera, as established in the bailiff's report of March 8, 2019 and that it had applied the video protection regime in good faith. to the camera installed in the translators' office instead of the one applicable to video surveillance.30. Firstly, with regard to the proportionality of the video surveillance system, the Restricted Committee notes that the company indicated that it had put such a system in place to ensure the safety of persons and property. Three cameras are installed in the company's premises, including one in the translators' office, not accessible to the public, which continuously films the employees present and the cabinet containing the documents to be translated.31. The Restricted Committee considers that the implementation of a video surveillance system must comply with the principle of proportionality and that the collection of personal data carried out via this device must be strictly necessary for the objective pursued.32. Indeed, Article 5 1. c) of Regulation (EU) No 2016/679 of 27 April 2016 on data protection lays down the principle of data minimization, i.e. the data to be personal character collected must be limited to what is necessary in relation to the purposes for which they are processed.33. In this respect, when a video surveillance device is likely to target members of staff, the number, location, orientation, periods of operation of the cameras or the nature of the tasks performed by the persons concerned, are so many elements to take into account when installing the system.34. It follows that, while the surveillance of sensitive areas can be justified by security imperatives, the placement under permanent surveillance of employees, infringing on their privacy, can only take place in exceptional circumstances relating, for example, to the nature of the task to be performed. This is the case when an employee handles objects of great value or when the data controller is able to justify the theft or damage committed in these areas. Moreover, Article L. 1121-1 of the Labor Code provides that no one may place restrictions on the rights of persons and individual and collective freedoms that are not justified by the nature of the task to be performed or proportionate to the aim. wanted .35. In this case, the Restricted Committee notes that no exceptional circumstances justifying placing the translators, who are sworn translators, under permanent surveillance has been demonstrated by the company. The latter invokes the need to protect translated documents. However, if the nature of the documents can justify the implementation of specific protection measures, it is advisable to consider, prior to the use of a video surveillance device leading to constant filming of the employees, alternative processes such as as securing access to the workplace. However, such alternative procedures had not been considered by the company, which moreover did not report any theft or damage to its premises, which could justify the establishment of such a system.36.

Under these conditions, the use of a video surveillance device leading to placing employees under permanent surveillance does not appear justified and must be considered manifestly disproportionate and excessive in relation to the declared purpose.37. Secondly, with regard to the lack of compliance within the time limit set by the formal notice, the Restricted Committee notes that two letters from the CNIL, addressed to the company within the framework of the investigation of the complaints October 18, 2013 and June 2, 2016, expressly reminded him of the need to set up a video surveillance system proportionate to the purposes implemented. These letters specifically indicated that this mechanism could not have the effect of placing under constant surveillance an employee or a group of employees at their workstations, except in exceptional circumstances related to the sensitivity of the position occupied. Despite these letters and the formal notice from the President of the CNIL of July 26, 2018, it appears from the findings made by the Commission delegation on October 10, 2018 that the video surveillance system set up in the translators' office still made it possible to constantly filming employees, contrary to the company's assertions that the employees were not continuously filmed.38. The Restricted Committee also notes that if the company took a measure on October 15, 2018 consisting of the affixing of adhesive tape to the camera, this summary process did not make it possible to achieve compliance, since it appears from the documents file that at least one employee was still filmed continuously at his workstation.39. The Restricted Committee then holds that the company withdrew the disputed camera on March 8, 2019, as appears from the bailiff's report produced in defence. It notes that this compliance came late, insofar as it was only upon notification of the report that the company took measures to stop filming employees' workstations on a permanent basis, whereas he had been asked to do so since October 18, 2013.40. The Restricted Committee holds, in any event, that the company did not comply at the end of the period set in the formal notice of July 26, 2018.41. On the basis of these elements, the Restricted Committee considers that the breach of Article 5 1. c) of the Rules is established.2. On the breach of the obligation to inform people42. Article 12 of the Regulation provides: 1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 as well as to carry out any communication under Articles 15 to 22 and Article 34 in concerning the processing to the data subject in a concise, transparent, comprehensible and easily accessible manner, in clear and simple terms, in particular for any information intended specifically for a child. Information is provided in writing or by other means including, where appropriate, electronically .43. Article 13 of the Regulation provides that: 1. When personal data relating to a data subject is collected from that person, the controller shall provide him, at the time the data in question is obtained, with all of the following information a) the identity and contact details of the controller and, where

applicable, of the controller's representative; b) where applicable, the contact details of the data protection officer; c) the purposes of the processing for which intended the personal data as well as the legal basis for the processing; d) where the processing is based on Article 6, paragraph 1, point f), the legitimate interests pursued by the controller or by a third party; the recipients or categories of recipients of the personal data, if they exist; andf) where applicable, the fact that the controller intends to transfer personal data to a third country or to an international organization (…);2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject, at the time the personal data is obtained, with the following additional information which is necessary to ensure fair and transparent processing: a) the duration of retention of personal data or, where this is not possible, the criteria used to determine this duration; b) the existence of the right to request from the controller access to personal data, rectification or erasure thereof, or restriction of processing relating to the data subject, or the right to object to processing and the right to data portability; c) where the processing is based on Article 6, paragraph 1, point a), or on Article 9, paragraph 2, point a), the existence of the right to withdraw consent at any time, without prejudice to the lawfulness of the processing based on the consent and made before its withdrawal; d) the right to lodge a complaint with a supervisory authority; e) information on whether the requirement to provide personal data is of a regulatory nature or contractual or if it conditions the conclusion of a contract and if the person concerned is obliged to provide the personal data, as well as on the possible consequences of the non-provision of these data; f) the existence of a automated decision-making, including profiling, referred to in Article 22(1) and (4), and, at least in such cases, meaningful information about the underlying logic, as well as the significance and intended consequences of this processing for the data subject (…).44. The company was given formal notice to proceed with informing the persons whose data were processed, in particular with regard to the video surveillance device placed in the translators' office, in accordance with the aforementioned Articles 12 and 13, the formal notice citing various possible forms of information.45. During the second inspection of October 10, 2018, the delegation noted that no formal information intended for employees, including the elements provided for in Article 13 of the Regulations, had been implemented. She was, however, informed that the company had undertaken to draft an information note for employees on the video surveillance system.46. The rapporteur criticizes the company for not having complied with the injunctions formulated in the formal notice within the time limit and for having initiated measures relating to the information of employees about the video surveillance system only at the outcome of the second check.47. In defence, the company argues, on the one hand, that it was due to confusion between the regimes applicable to video protection and video

surveillance devices that it was able to provide information which was not satisfactory with regard to of the provisions of Article 13 of the Rules and, secondly, that the video-surveillance device having been removed, it no longer had to provide information relating to the installation of such a device.48. The Restricted Committee notes that the camera having been removed from the translators' office, the company no longer effectively has, to date, to issue information to employees relating to this device. It notes, however, that the withdrawal came late, since it was only at the sanctioning stage that the measure was taken, almost six months after the expiry of the time limit set in the formal notice.49. The Restricted Committee also considers that, as of the on-site inspection of February 16, 2018, the manager of the company was questioned by the delegation on the establishment of formal information for employees on the video surveillance system placed in the translators office. It was therefore reminded of the need for specific information intended for employees in February 2018. The company was also given formal notice to provide information intended for employees, in accordance with the provisions of Articles 12 and 13 of the Regulations .50. Although the company has partially completed the information panel present in the reception hall within the time limit set by the formal notice, the Restricted Committee notes that it is a panel relating to video protection, intended for visitors, which does not include the elements referred to in Article 13 of the Regulation. The specific information measures, indicated in the formal notice, which were to be taken for the employees had not been carried out since the restricted committee notes that on the day of the second inspection, October 10, 2018, no formal information to intended for employees had not been implemented.51. The Restricted Committee notes that the company established, after this inspection, as it had indicated to the delegation, an information note intended for employees which remains however incomplete with regard to the requirements of Article 13 of the Regulation. 52. The company, despite the good faith invoked, had all the information required regarding the elements to be brought to the attention of the employees. It was therefore still not in compliance at the end of the formal notice period, nor during the second inspection carried out on October 10, 2018.53. On the basis of these elements, the Restricted Committee considers that the breach of Articles 12 and 13 of the Rules is constituted.3. On the breach of the obligation to ensure the security and confidentiality of data54. Under the terms of Article 32 of Regulation (EU) No 2016/679 of April 27, 2016: (…) the controller and the processor implement the appropriate technical and organizational measures to guarantee a level of security appropriate to the risk, including inter alia, as required: a) pseudonymization and encryption of personal data; b) means to ensure the ongoing confidentiality, integrity, availability and resilience of systems and processing services;c) the means to restore the availability of personal data and access to them in a timely manner in the event of a physical or technical incident;d)

a procedure for testing, analyzing and to regularly assess the effectiveness of the technical and organizational measures to ensure the security of the processing (…).55. The company has been given formal notice to remedy the security flaws relating to access to employee computer stations so that they are subject to authentication by each user. The formal notice also ordered the company to put in place a binding password management policy for the image viewing software installed on the manager's computer station and for the employees' Windows accounts, as well as to implement measures to ensure the traceability of access to the generic professional mailbox and to remove access to this mailbox for employees leaving the company.56. By letter dated September 10, 2018, the company confirmed that access to employee workstations and to the Windows session of the manager's workstation is without a password. It specified that access to generic professional messaging for exchanges with customers and the company is carried out by means of a generic messaging address accessible by all employees via a shared password, made up of eight characters.57. During the inspection of October 10, 2018, the delegation confirmed the findings made during the first inspection, namely that all employees continued to use a unique and shared username and password to access professional email and that access to employee computer workstations was still not subject to authentication. The company nevertheless informed the delegation that it planned to bring the employees together in order to find a solution to the implementation of a policy for managing the passwords of computer workstations compatible with the operation of the company.58. The delegation noted that on the day of the inspection of 10 October 2018, no binding password management policy had been put in place for computer workstations and that no measure had been taken to ensure traceability to access to professional email.59. The company was thus criticized for not having complied, with regard to the measures to be taken to ensure the security and confidentiality of the data.60. In its brief of April 11, 2019, the company argues that each employee now has a personal identifier and a password that meets the recommendations of the CNIL, as defined in its deliberation No. 2017-012 of January 19 2017, as appears from the bailiff's report of April 10, 2019.61. The Restricted Committee notes that while the company complied during the investigation, with regard to the authentication of each user when accessing the employees' computer stations and the implementation of a restrictive password policy, it had not done so at the end of the period of formal notice, nor during the second check of October 10, 2018. It did so only after the end of the initiation of sanction proceedings.62. The Restricted Committee also notes that the company has not provided any response regarding the measures to be implemented in order to ensure the traceability of access to the generic professional mailbox. It notes, however, that the company undertakes to revoke access in the event of

the permanent departure of an employee.63. On the basis of all of these elements, the Restricted Committee considers that the breach of Article 32 of the Rules is established.4. On the penalty and publicity64. Article 20-III of the amended law of January 6, 1978 provides: When the data controller or its processor does not comply with the obligations resulting from Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016 mentioned above or of this law, the president of the National Commission for Computing 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 an update 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 of this Law or of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 mentioned above (…), which may be accompanied, except in cases where the processing is implemented by the State, d a penalty payment, the amount of which cannot t exceed €100,000 per day of delay from the date set by the restricted committee; (…) 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 the European Parliament and of the Council of April 27, 2016 mentioned above, these ceilings are increased, respectively, to 20 million euros and 4% of said turnover. The restricted committee takes into account, in determining the amount of the fine, the criteria specified in the same section 83.65. Article 83 of the GDPR provides: Each supervisory authority shall ensure that administrative fines imposed under this Article for breaches of this Regulation referred to in paragraphs 4, 5 and 6 are, in each case, effective, proportionate and dissuasive . Depending on the specific characteristics of each case, administrative fines are imposed in addition to or instead of the measures referred to in points (a) to (h) and (j) of Article 58(2). In deciding whether to impose an administrative fine and in deciding the amount of the administrative fine, due account shall be taken in each individual case of the following elements: (a) the nature, gravity and the duration of the breach, taking into account the nature, scope or purpose of the processing concerned, as well as the number of data subjects affected and the level of damage they have suffered; b) whether the breach was committed willfully or negligently; (c) any action taken by the controller or processor to mitigate the damage suffered by data subjects; (d) the degree of responsibility of the controller or processor, taking into account the technical and organizational measures they have implemented pursuant to Articles 25 and 32; (e) any relevant breach previously committed

by the Controller or Processor; (f) the degree of cooperation established with the supervisory authority with a view to remedying the breach and mitigating its possible negative effects; (g) the categories of personal data affected by the breach; (h) how the supervisory authority became aware of the breach, including whether and to what extent the controller or processor notified the breach; (i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned for the same purpose, compliance with those measures; (j) the application of codes of conduct approved under Article 40 or certification mechanisms approved under Article 42; and (k) any other aggravating or mitigating circumstance applicable to the circumstances of the case, such as financial benefits obtained or losses avoided, directly or indirectly, as a result of the breach.66. Firstly, with regard to the injunction to bring the processing into compliance with the provisions of Articles 5 1 c), 12, 13 and 32 of the Rules, the Restricted Committee notes that the company has removed the camera placed in the translators office. It therefore considers that there is no longer any reason to maintain the injunction to modify the video surveillance system so that the employees are no longer placed under constant surveillance.67. The Restricted Committee also considers that, since the video surveillance device has been removed, the company no longer has to provide information relating to the implementation of such a device. Consequently, there is no longer any reason to maintain the injunction relating to the failure to inform the persons concerned.68. On the other hand, the Restricted Committee finds that the company has not put in place measures to ensure the traceability of individual access to the shared professional mailbox. Indeed, in order to ensure the security and confidentiality of personal data or to determine the origin of a security incident, it is necessary to determine the persons authorized to access the data and to trace the actions carried out on the computer system with a view in particular to identifying illicit access and the risks of breaching the integrity of the data. This is achieved by ensuring that users are authenticated with individual accounts before accessing data and that such generic email access is logged. 69. As the company failed to fully comply with this breach, the injunction should be maintained.70. Secondly, the company maintains that an administrative fine of 75,000 euros would be disproportionate taking into account the criteria set by Article 83 of the Rules, its financial capacities and the sanctions previously imposed by the restricted committee. It highlights the measures taken to mitigate the damage suffered by its employees, its degree of cooperation with the Commission, its confusion between the video protection and video surveillance systems and the serious financial difficulties it has been encountering for three years.71. First of all, the Restricted Committee considers that, in the present case, the aforementioned breaches justify the imposition of an administrative fine on the company for the following reasons.72. The

Restricted Committee recalls that the breaches of Articles 5 1 c), 12, 13 and 32 of the Rules persisted beyond the time limit set by the formal notice from the President of the Commission and that it was only at the notification of the sanction report that the company has taken steps to achieve partial compliance. The company thus did not, contrary to what it maintains, actively cooperate with the Commission's departments until the initiation of the sanction procedure.73. More specifically, with regard to the breach relating to the video surveillance system, the Restricted Committee points out that the company placed the company's translators under constant surveillance for several years without valid reason and without any measure being taken in this regard. following the letters sent to the company by the CNIL in 2013 and 2016, the on-site inspection of February 16, 2018, the formal notice sent to the company on July 26, 2018 and the second on-site inspection carried out on October 10, 2018 In addition, the Restricted Committee notes that the company provided responses that contradicted the findings established during the inspection operations. In any case, it was only in March 2019 that the company withdrew the disputed camera, once the sanction procedure had been initiated. The company cannot therefore claim to have put in place means aimed at limiting the harm suffered by the employees, since the camera was removed very late, several months after the expiry of the period of formal notice. Nor can it rely on any confusion of the applicable legal framework in view of the exchanges which took place between the company and the Commission's departments, ordering it to cease placing its employees under constant surveillance.74. In addition, the restricted training highlights the particular sensitivity of the video surveillance system for employees in their workplace. It recalls that the CNIL's first on-site inspection was decided following the filing of eight complaints between 2013 and 2017 relating to the video surveillance system and that the purpose of the processing invoked - the security of goods with regard to the protection of confidential documents to be translated – does not require sworn translators to be filmed continuously. A reorientation of the camera or the installation of dynamic masks were, for example, possible.75. With regard to the breach relating to the information of persons, the Restricted Committee emphasizes that the company was put in a position, thanks to the injunction formulated in the formal notice, to understand the need to inform the employees of the installation of a video surveillance device and the required particulars which had been expressly listed therein. However, it must be noted that satisfactory information was not given to the persons within the time limit set by the formal notice.76. With regard to the breach relating to the security and confidentiality of data, the Restricted Committee notes that the company has not remedied the lack of secure access to employees' computer workstations at the end of the period set by the notice. It was only on April 10, 2019, as evidenced by the court bailiff's report produced by the company, that

it came into compliance by setting up a personal identifier and a password for each employee for access to computer workstations as well as to the manager's Windows session. The Restricted Committee notes that the steps taken by the company to ensure data security were taken belatedly.77. Finally, the company has not complied, as of the date of this deliberation, in order to ensure the traceability of individual access to the generic professional mailbox.78. Next, the Restricted Committee recalls that § 3 of Article 83 of the Rules provides that in the event of multiple violations, as is the case here since three breaches are identified, the total amount of the fine does not may exceed the amount set for the most serious breach. Insofar as the company is accused of a breach of Article 5 of the Regulations, the maximum amount of the fine that may be withheld is 20 million euros or 4% of the annual worldwide turnover, the highest amount being retained. In this respect, if the company asserts, by way of comparison, the amount of the pecuniary penalties previously pronounced by the restricted committee, this is irrelevant. These are pecuniary penalties pronounced before the entry into force of the Regulation and for some, before Law No. 2016-1321 of October 7, 2016 for a Digital Republic. The maximum ceiling for the amount of penalties was, in the case of the decisions cited by the company, 150,000 euros under the influence of law no. 2011-334 of March 29, 2011 then 3 million euros under the influence of the law for a digital Republic.79. The Restricted Committee emphasizes the plurality of breaches in question as well as their persistence and seriousness, in particular with regard to the disproportionate nature of the video surveillance system. It takes particular account of the number of complaints at the origin of the formal notice procedure and the duration of these breaches. It also notes the company's reluctance to take account of the legislation applicable to the protection of personal data and its lack of diligence in remedying the shortcomings noted, despite the exchanges carried out with the Commission's services for several years.80. However, the restricted committee takes into account the measures that the company has taken during the investigation of the sanction procedure to bring itself into compliance, the fact that it is a micro-enterprise and its financial situation, in order to to determine the amount of a fair and proportionate administrative fine which must also be dissuasive.81. It follows from all of the above and from consideration of the criteria set out in Article 83 of the GDPR that an administrative fine of 20,000 euros is justified and proportionate, as well as an additional sanction of publication for a period of one year.FOR THESE REASONSThe Restricted Committee of the CNIL, after having deliberated, decides to:- issue an injunction to bring the processing into compliance with the provisions of Article 32 of Regulation (EU) No 2016/679 of April 27, 2016 relating to data protection, in particular to put in place measures to ensure that only authorized persons can access the mailbox and that the operations carried out are traced. To this end, users

connecting to the mailbox must be authenticated beforehand with an individual account and access to generic messaging must be logged in order to guarantee their traceability, accompanied by an as payment of 200 euros per day of delay at the end of a period of two months following the notification of this deliberation, the supporting documents of compliance must be sent to the restricted committee within this period; against company X an administrative fine of 20,000 (twenty thousand) euros; - make public, on the CNIL website and on the Légifrance website, its deliberation which will be anonymized at the end of a period of one year from its publication. President Alexandre LINDEN This decision may be appealed to the Council of State within two months of its notification.