Deliberation SAN-2021-020 of December 28, 2021Commission Nationale de l'Informatique et des LibertésNature of the deliberation: SanctionLegal status: In force Date of publication on Légifrance: Thursday, December 30, 2021Deliberation of the restricted committee n°SAN-2021-020 of 28 December 2021 concerning the company SLIMPAYThe National Commission for Computing and Liberties, meeting in its restricted formation composed of Mr. Alexandre LINDEN, President, Mr. Philippe-Pierre CABOURDIN, Vice-President, Mrs. Christine MAUGÜÉ, Mr. Bertrand du MARAIS and Mr. Alain DRU, members; 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; Having regard to Law No. 78-17 of January 6, 1978 amended relating to data processing, files and freedoms, in particular its articles 20 and following; Considering the decree n ° 2019-536 of May 29, 2019 taken for the application of the Law 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 Data Processing and Freedoms Having regard to decision no. 2020-107C of the President of the CNIL of May 12, 2020 to instruct the Secretary General to carry out or to have carried out a verification mission with the company SLIMPAY; Having regard to the decision of the President of the Commission National Computing and Freedoms appointing a rapporteur before the restricted committee, dated April 12, 2021; Having regard to the report of Mrs Valérie PEUGEOT, reporting commissioner, notified to SLIMPAY on June 23, 2021; Having regard to the observations written submissions submitted by SLIMPAY on July 23, 2021; Having regard to the oral observations made during the restricted training session; Considering the other documents in the file; Were present, during the restricted training session of 16 September 2021:- Mrs. Valérie PEUGEOT, statutory auditor, heard in her report;As representatives of the SLIMPAY company:- […];The SLIMPAY company having had the floor last;After deliberating, the restricted committee adopted the following decision:I. Facts and procedure1. SLIMPAY (hereinafter the "company") is a public limited company, registered with the Paris Trade and Companies Register, whose business is consulting in computer systems and software. Its workforce is 83 employees.2. The company is an approved payment institution, which offers recurring payment services in the Single Euro Payments Area (SEPA). It offers its customers, "merchants" who are legal persons, solutions for managing subscriptions and recurring payments.3. As part of the services provided by the company to its merchants, the personal data processed are those of the debtors who are natural persons of the merchants. As of September 1, 2020, SLIMPAY had […] natural person debtors of merchants in its databases.4. In 2019, the company achieved a turnover of […] euros and presented a net result amounting to […] euros. In

2020, its turnover amounted to […] euros and it presented a net result of […] euros. The company also raised funds of […] euros in 2015.5. During the summer of 2015, during an internal research project on an anti-fraud mechanism, the company reused personal data contained in its databases for test purposes. She thus imported debtors' personal data onto a server. When the research project ended in July 2016, the data remained stored on this server, which was not subject to any particular security procedure and which was freely accessible from the Internet.6. On February 14, 2020, one of the company's customer merchants informed him of these elements. SLIMPAY then immediately proceeded to isolate the server and sequester the data, in order to put an end to the personal data breach.7. On February 17, 2020, the company notified the data breach to the Commission Nationale de l'Informatique et des Libertés (hereinafter the "Commission" or the "CNIL").8. On February 26, 2020, the company made an additional data breach notification to the CNIL, giving more details on the security incident, in particular on the measures implemented by the company, the number of people and the type of personal data affected by the data breach.9. Debtor data from […] merchants, corresponding to approximately twelve million unique debtors, were affected by this breach. The personal data concerned by the breach are civil status data (title, surname, first name), postal, electronic and telephone contact details, and banking information ("Bank Identifier Code" - BIC/ "International Bank Account Number " - IBAN).10. The elements transmitted by the company having made it possible to establish the cross-border nature of the processing concerned, the CNIL informed on February 27, 2020, in accordance with Article 56 of the GDPR, all the European supervisory authorities of its competence to act in as lead supervisory authority and thus opened the procedure for the declaration of the authorities concerned on this case.11. Pursuant to Decision No. 2020-107C of the President of the Commission of May 12, 2020, the CNIL carried out a documentary inspection mission to the company, in order to verify compliance by the latter with all the provisions of the modified law n° 78-17 of January 6, 1978 relating to data processing, files and freedoms (hereinafter the "modified law of January 6, 1978" or "Data Protection Act") and of the regulation (EU ) 2016/679 of the European Parliament and of the Council of April 27, 2016 (hereinafter the "GDPR"). This mission was carried out by sending a questionnaire to the company, sent by registered letter with acknowledgment of receipt on July 31, 2020.12. By email of August 5, 2020, the company's data protection officer requested an extension from the CNIL delegation.13. By email of August 6, 2020, an extension was granted to the company until September 11, 2020.14. On September 11, 2020, the company sent response elements to the CNIL, by secure dematerialized means.15. By emails of October 21 and December 2, 2020, the CNIL delegation requested additional information from the company, in particular to find out whether the company

had carried out a public communication or another similar action to inform the persons concerned by the data breach and whether the research and development work she was working on for fraud enforcement required the use of real, non-anonymized data. These elements were transmitted respectively on October 29 and December 10, 2020.16. For the purposes of examining this file, the President of the Commission, on April 12, 2021, appointed Mrs Valérie PEUGEOT as rapporteur on the basis of Article 39 of Decree No. 2019-536 of May 29, 2019 taken as the application of the amended law of January 6, 1978.17. At the end of her investigation, the rapporteur, on June 23, 2021, notified SLIMPAY of a report detailing the breaches of the GDPR that she considered constituted in this case. A letter was also given to him, informing him that the file was on the agenda of the restricted training of September 16, 2021.18. This report proposed that the restricted committee of the Commission impose an administrative fine on the company, with regard to the breaches of Articles 28 paragraphs 3 and 4, 32 and 34 of the GDPR. It also proposed that the sanction decision be made public, but that it would no longer be possible to identify the company by name after the expiry of a period of two years from its publication.19. On July 23, 2021, the company filed observations in response.20. The company and the rapporteur presented oral observations during the meeting of September 16, 2021. II. Reasons for decision21. According to Article 56(1) of the Regulation, "the supervisory authority of the main establishment or single establishment of the controller or processor is competent to act as the chief supervisory authority of file concerning the cross-border processing carried out by this controller or processor, in accordance with the procedure provided for in Article 60 ".22. In this case, the Restricted Committee notes that the registered office of the company, the sole establishment of the company SLIMPAY, is located in France and that it has been registered in the trade and companies register in France from the outset, which leads to making the CNIL the competent lead supervisory authority concerning the cross-border processing carried out by this company, in accordance with Article 56 paragraph 1 of the Regulation.23. Applying the cooperation and consistency mechanism provided for in Chapter VII of the GDPR, the CNIL informed, on February 27, 2020, all the European supervisory authorities of its competence to act as lead supervisory authority concerning the cross-border processing carried out by the company, thus opening the procedure for the declaration of the authorities concerned on this case. The supervisory authorities of the following countries have declared themselves concerned by this procedure: Germany, Spain, Italy and the Netherlands.24. Pursuant to Article 60(3) of the GDPR, the draft decision adopted by the Restricted Committee was sent to these supervisory authorities on November 25, 2021.25. As of 24 December 2021, none of the supervisory authorities concerned had raised a relevant and reasoned objection to this draft decision, so

that, pursuant to Article 60(6) of the GDPR, these latter are deemed to have approved it.A. On the status of the company in terms of processing responsibility26. According to Article 4 of the GDPR, the controller is defined as "the natural or legal person, public authority, service or other body which, alone or jointly with others, determines the purposes and means of processing" (point 7) and the processor is "the natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller" (point 8 ).27. Article 28-10 of the GDPR provides that "without prejudice to Articles 82, 83 and 84, if, in violation of this Regulation, a processor determines the purposes and means of the processing, he is considered to be a controller with respect to this processing ".28. The rapporteur notes that the company SLIMPAY acts as the data controller concerned by the data breach and as a subcontractor for the processing implemented in the context of the services provided to merchants, data controllers.29. In defence, the company does not dispute the rapporteur's analysis on this point.30. The Restricted Committee considers that the notion of data controller must be the subject of a concrete assessment taking into account all the elements making it possible to attribute this quality to an entity. In this respect, it notes that it appears from the elements communicated to the CNIL that the company SLIMPAY acts as a subcontractor for the processing carried out within the framework of the services provided to merchants, data controllers, insofar as the company does not determine the purposes of data processing. These services constitute the bulk of its activity (recurring payment services, SEPA mandates, etc.).31. The Restricted Committee also notes that the company itself uses, within the framework of the services provided to merchants, the services of subcontractors. As the company indicates, SLIMPAY's subcontractors are therefore second-level subcontractors vis-à-vis the merchants.32. The Restricted Committee also considers that the company SLIMPAY acted as the controller concerned by the data breach, this being an internal research processing operation concerning a mechanism for combating fraud, for which it alone determined the purposes and the means. The company also indicates itself to act as data controller, in the additional data breach notification that it sent to the CNIL on February 26, 2020.33. It is therefore up to the Restricted Committee to examine, with regard to these qualities, the grievances formulated by the rapporteur against the company.B. On the characterization of breaches with regard to the GDPR34. As a preliminary point, the Restricted Committee notes that, in defence, the company disputes the fact that breaches unrelated to the breach of personal data can be upheld, whereas this is at the origin of the procedure.35 . The Restricted Committee considers that the fact that the CNIL's investigations were initially motivated by the occurrence of the data breach, following its notification, has no impact on the possibility of finding the existence of other breaches of the GDPR with regard to the facts observed during the

investigations carried out by the CNIL's supervisory delegation.36. Indeed, it follows from article 8 of the Data Protection Act that the CNIL, on the one hand, can carry out verifications relating to all processing and, if necessary, obtain copies of all documents or data carriers. information useful to its missions, on the other hand, must ensure that the processing of personal data is implemented in accordance with the provisions of the said law and the other provisions relating to the protection of personal data provided for by the texts laws and regulations, European Union law and France's international commitments.37. In this context, and in application of article 20 of the Data Protection Act, the restricted committee takes measures and pronounces sanctions against data controllers or subcontractors who do not respect the obligations arising from the GDPR and said law.1. On the breach of the obligation to regulate by a formalized legal act the processing carried out by a subsequent subcontractor38. According to Article 28 paragraph 3 of the GDPR, "The processing by a processor is governed by a contract or other legal act under Union law or the law of a Member State, which binds the processor vis-à-vis the controller, defines the object and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects, and the obligations and rights This contract or other legal act provides, in particular, that the processor: a) only processes personal data on documented instructions from the controller, including with regard to data transfers personal data to a third country or to an international organisation, unless he is required to do so under Union law or the law of the Member State to which the processor is subject; in this case, the subcontractor informs the controller e of the processing of this legal obligation before the processing, unless the law concerned prohibits such information for important reasons of public interest; b) ensures that the persons authorized to process the personal data undertake to respect confidentiality or are subject to an appropriate legal obligation of confidentiality; c) take all the measures required under Article 32; d) comply with the conditions referred to in paragraphs 2 and 4 to recruit another processor; […] “.39. Pursuant to paragraph 4 of the same article, when a processor recruits another processor to carry out specific processing activities on behalf of the controller, the same obligations in terms of data protection than those laid down in the contract between the controller and the processor are imposed on this other processor by a contract or by means of another legal act, in particular as regards the provision of guarantees sufficient in terms of the implementation of appropriate technical and organizational measures so that the processing meets the requirements of the Regulation. When this other subcontractor does not fulfill its obligations in terms of data protection, the initial subcontractor remains fully responsible to the data controller for the performance by the other subcontractor of its obligations.40 As part of the investigations carried out by the CNIL, the company SLIMP AY has indicated

that it uses […] subcontractors acting under its authority as second level subcontractors vis-à-vis merchants, for the services it provides to the latter (recurring payment services, SEPA mandates , etc.). The company also specified that it sends these subcontractors a "questionnaire relating to subcontracting" in order to comply with the GDPR. On the said questionnaire, it is indicated: "as a payment service provider, SlimPay is determined to comply with the provisions of the regulation on the protection of personal data (regulation (EU) 2016/679). To this end, we must ensure that the data processing carried out by our partners complies with legal requirements.".41. The rapporteur considered that the steps taken by the company with its subcontractors through these questionnaires were not sufficient to meet its obligations and ensure that subsequent subcontractors provide the required guarantees. It also noted that the contracts and amendments concluded with three companies did not contain all the clauses provided for in Article 28(3) of the GDPR and that those concluded with three other companies did not include any of the mandatory information provided for by that same article.42. In defence, the company explains that it is implementing concrete measures to ensure its compliance with data protection regulations as part of an ongoing process, not only by relying on the compliance documentation provided by its subcontractors. contractors, who offer standard contractual commitments, but also through occasional questionnaires. It specifies that the questionnaires communicated during the CNIL inspection were only intended to justify the verifications carried out by SLIMPAY with its subcontractors, adding that, for lack of the said subcontractors to provide contractual documentation framing the guarantees in with regard to data protection, it is planned to submit such an agreement to them. SLIMPAY also reports on ongoing negotiations with certain companies on the signing of riders relating to the protection of personal data.43. Firstly, the Restricted Committee notes that the company has not provided proof that the questionnaire referred to is completed by subsequent subcontractors. In any case, even if it were, the Restricted Committee emphasizes that the said questionnaire has only declarative value and that it does not constitute a binding legal act by which the subsequent subcontractor undertakes to respect the defined elements. Sending this questionnaire does not therefore allow the obligations set out in Article 28 paragraphs 3 and 4.44 to be met. Secondly, the Restricted Committee notes that some of the contracts concluded by the company with its subcontractors do not contain all the clauses provided for in Article 28 paragraph 3 of the GDPR. In this sense, it notes that the contracts and amendments concluded with […] do not specify all the mandatory information under Article 28 of the GDPR, including in particular the type of data concerned as well as the obligations and rights of the person responsible. treatment. Similarly, in the contract and the amendments concluded with […] - the type of data and the obligations

and rights of the controller are not mentioned.45. The Restricted Committee also notes that the contracts and amendments concluded with the companies […] do not contain any of the mandatory information provided for in Article 28 of the GDPR.46. Thirdly, the Restricted Committee notes that the company SLIMPAY provided, in the context of the sanction procedure, an example of a "protection of personal data" endorsement concluded with the company […] in July 2021 and that it clarified that negotiations are underway with the companies […]. The Restricted Committee takes note of the partial compliance within the framework of this procedure. The fact remains that the fact that the company has taken steps with the subcontractors in the context of this procedure clearly demonstrates that it was not in compliance at the time of the investigations carried out by the CNIL.47 . It is still not, moreover, with regard to certain contracts, thus continuing to disregard the obligation to regulate by a formalized legal act the processing carried out by a subsequent subcontractor.48. Therefore, in view of all of these elements, the Restricted Committee considers that the breach of Article 28 paragraphs 3 and 4 of the GDPR is clear.2. On the breach of the obligation to ensure data security49. According to Article 32 of the GDPR, "1. Taking into account the state of knowledge, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risks, including the degree of probability and seriousness varies, for the rights and freedoms of natural persons, the controller and the processor implement the appropriate technical and organizational measures to guarantee a level of security appropriate to the risk, including between others, as required: a) pseudonymization and encryption of personal data; b) means to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; means to restore the availability of personal data and access to them within an appropriate period of time in the event of a physical or technical incident; d) a procedure for testing, analyzing and evaluating Regularly monitor the effectiveness of the technical and organizational measures to ensure the security of the processing.2. When assessing the appropriate level of security, account is taken in particular of the risks presented by the processing, resulting in particular from the destruction, loss, alteration, unauthorized disclosure of personal data transmitted , stored or otherwise processed, or the unauthorized access to such data, accidentally or unlawfully […] ".a) On the security defect that led to the breach of personal data- On the characterization of the breach.50 The rapporteur notes that it appears from the elements communicated to the CNIL that, within the framework of a research project carried out in 2015, SLIMPAY reused personal data of debtors for the purposes of testing a anti-fraud system. The project ended the following year, in July 2016, but the data remained hosted on a server not subject to any particular security measures. On February 14, 2020, the society has been notified by one of its customers of the possibility of freely accessing

this data from the Internet by means of a URL simply composed of an IP address and a communication port, without any other access restriction or measure of security. That same evening, the company isolated the server containing the personal data concerned.51. According to the rapporteur, the company's breach of its security obligation thus began in 2015, when merchant customer data was imported onto a server not subject to any security measures, and it continued since it only ended in February 2020, after the company was alerted by one of its customers. It considers, since it is a continuous breach, that it is appropriate to sanction from the point of view of the GDPR and that such an analysis was recently confirmed by the Council of State in its decision of 1 March 2021 concerning Futura Internationale.52. With regard to the facts constituting the breach, the rapporteur emphasizes that access to the server in question was not subject to any satisfactory access restriction measure and that the company had not implemented any access logging measure. to the server.53. In defence, SLIMPAY contests the rapporteur's analysis according to which the principle of non-retroactivity of the more severe criminal sanction cannot apply to breaches which continue to produce effects over time, to the point that even started under under the Data Protection Act, they persist under the aegis of the GDPR and must therefore be qualified as continuous and apprehended, for the period after the entry into force of the GDPR, by the application of the provisions of the said Regulation. . To do this, it also relies on the judgment of the Council of State of March 1, 2021 relating to the company Futura Internationale, considering that this case law applies to a specific case distinct from this case: in the Futura Internationale judgment, the Council of State took care to specify that deliberate breaches had not been corrected despite formal notice from the CNIL. This case law is therefore not transposable to the case in point according to the company insofar as it was automatically offered a sanction without formal notice or prior injunction from the CNIL and that it also collaborated with diligently and in good faith with the CNIL upon notification of the incident.54. In addition, the SLIMPAY company explains that the vulnerability of the server is the consequence of isolated human negligence and not of a deficiency in its technical and organizational device. It recalls that the general security obligation of companies must be analyzed as an obligation of means and not of result. She adds that she terminated the data breach immediately upon being notified. It also indicates that the use of data stored on the server required computer knowledge and the use of specific tools, that the data present on the server dated from 2012 to 2013 and that, consequently, they were difficult to use by a attacker. Finally, it notes that the server's IP address was not referenced on a search engine.55. During the Restricted Committee session, the company clarified that the human negligence referred to in its pleadings was in fact attributable […]. It largely insisted on the fact that it had not committed, as data controller, any breach of

its security obligations insofar as the error was made by […].56. Firstly, with regard to the principle of non-retroactivity, the Restricted Committee considers that, insofar as the breach of personal data, as well as the lack of security in which it originated, continued after 25 May 2018, the date of entry into force of the GDPR, it is with regard to this text that the shortcomings of which SLIMPAY is accused must be assessed. This analysis was confirmed by the Council of State in its decision of March 1, 2021 concerning Futura Internationale. In this case following a complaint relating to cold calling by the company Futura Internationale, the Conseil d'État considered that, if the company's shortcomings were noted during a control mission to which proceeded by the CNIL before the entry into application of the GDPR, they continued after this date. The Council of State concluded that "it is thus right that the CNIL, noting the continuous nature of the breaches noted […], considered the GDPR applicable to the facts of the case and assessed the breaches with regard to this one" (Council of State, 10th-9th chambers combined, March 1, 2021, Futura Internationale, n° 437808).57. The Restricted Committee also recalls that, in accordance with Article 20 of the Data Protection Act, the President of the CNIL is not required to send a formal notice to the organization before opening a sanction procedure. against him.58. Secondly, the Restricted Committee notes that access to the server in question was not governed by any satisfactory access restriction measure insofar as it was possible to access it from a URL consisting of an easily identifiable IP address using port scanners, which are available on the web and often used by attackers to detect unsecured or unsecured servers.59. The Restricted Committee also notes that the company had not implemented any server access logging measures, which would nevertheless have made it possible to detect the actions carried out on the server. Indeed, the implementation of a logging of activities, that is to say a recording of activities in "log files" or "logs", in particular for access to the various servers of an information system , is crucial in that it makes it possible to trace activities and detect any anomalies or events related to security, such as fraudulent access and misuse of personal data. Thus, in its security recommendations for the implementation of a logging system, the National Agency for the Security of Information Systems (ANSSI) noted that "event logs constitute a technical brick essential to the management the security of information systems "in so far as they can be used "a priori to detect security incidents" and a posteriori to "understand the path of an attack and […] assess its impact". 60. The Restricted Committee also notes that the data contained in the server could easily be read since they were stored in formats readable by means of a simple text editor or tools available and well documented on the Internet.61. Thus, the lack of implementation of security measures protecting the server in question, in particular the restriction of access to only persons who should have been authorized, caused the accessibility of the data

concerned from the Internet and these data were easily readable in because of the format in which they were stored.62. Thirdly, the Restricted Committee considers that the company's argument, consisting in saying that it would not be liable for the breach of its security obligations insofar as the error was made by […], cannot carry conviction.63. First of all, the Restricted Committee notes that the security flaws do not result from an isolated human error, but from repeated shortcomings, since the company should have taken care to ensure the security of the data in question at several stages. In this respect, when it decided to reuse the data for its internal project, it was up to it to verify that the server used for these purposes was only accessible by authorized persons. The same monitoring requirement was imposed at least on the company when it completed its research project. Also, the company cannot blame these repeated shortcomings on an isolated human error […], who, in any event, was acting in his capacity as an employee on the instructions of the company and on its behalf.64. Then, the security of an information system is based on a set of technical and procedural measures, and not only on the competence of individuals […]. The effective implementation of these technical and procedural measures should precisely compensate for human shortcomings. The company should therefore have provided additional safeguards. The Restricted Committee considers that this situation reflects an organizational problem within the company.65. Therefore, the Restricted Committee considers that SLIMPAY has breached its obligation resulting from the provisions of Article 32 of the Rules.- On the scope of the breach66. The company maintains that the breach did not cause prejudice to the persons affected by the personal data breach, as none of these persons informed it of a fraudulent use of their personal data. It explains that it had an audit carried out by a third-party company, the company […], after the discovery of the vulnerability, which revealed that the data present on the server had not been exploited by an attacker.67. With regard to the scope of this breach, the Restricted Committee notes that it appears from the supplement to the notification sent on February 26, 2020 to the CNIL services that the personal data breach compromised the personal data of 12 478,819 European nationals.68. The Restricted Committee considers that the absence of proof of fraudulent use of the data has no impact on the characterization of the breach of the security obligation. Indeed, the risk of fraudulent use of personal data was real, independently of the cases of fraud, insofar as the data of many people were made accessible to unauthorized third parties. The absence of proven harm to the persons concerned does not affect the existence of the security defect, which constitutes the breach of Article 32 of the GDPR.69. The Restricted Committee also recalls that civil status data (title, surname, first name), postal, electronic and telephone contact details, and banking information (BIC/IBAN) were compromised.70. It emphasizes in this regard that, given the nature of this personal data,

the persons concerned by the breach are exposed to the risk of their personal data being reused by attackers. Indeed, they run the risk that their directly identifying data may be subject to illicit access, resold to third parties and reused in other attack schemes, in particular phishing (or "phishing"), a technique consisting of pretending to be an official body (social security body, bank, etc.) which, for example, asks its "prey" to confirm its bank details. In addition, these people are particularly exposed to the risk of identity theft.b) On the complaint of insufficient robustness of passwords for access to the user interface71. The rapporteur notes that the passwords allowing merchants to access their "customer" space are kept with the SHA-1 hash function, which is obsolete. It also notes that these passwords may consist of only one character, which does not ensure the security of the data to which they give access.72. In defence, the company explains that an error crept into the first information communicated by SLIMPAY during the documentary check. It indicates that the use of the SHA-1 hash function only concerns the old user interface made available by SLIMPAY and currently being decommissioned, and not the current interface. It specifies that access to this old interface has been revoked and that only two merchants still use this solution, although SLIMPAY has duly notified them of the need to migrate to the new solution as soon as possible.73. The company adds that the new solution uses the Bcrypt hash function recommended by the CNIL to store passwords on a dedicated database. The latest version of the current interface embeds a so-called "anti brute-force" function, which integrates multi-factor authentication and requires the use of a password with a length of 10 to 128 characters, including four types of characters (uppercase, lowercase, number and special character).74. The Restricted Committee notes first of all that, in its observations in response to the sanction report, the company transmitted information different from that communicated during the documentary check with regard to the hash function used for storing passwords allowing merchants to access their "customer" area. The company has thus indicated that the use of the deprecated hash function (SHA-1) concerns only the old user interface, which is being decommissioned, and which is used by two merchants. The Restricted Committee then notes that the two merchants in question have been given formal notice to migrate as soon as possible to the latest version of the interface, which uses a satisfactory hash function. Finally, the Restricted Committee observes that the evidence in the file does not allow the company's current statements to be called into question.75. The Restricted Committee therefore takes note of these statements and considers that there is no reason to hold any breach relating to the security obligation due to insufficient robustness of the passwords for access to the interface. user, allowing merchants to access personal data relating to their account.3. On the breach of the obligation to communicate to the persons concerned a breach of personal data76. Under

Article 34 of the GDPR, “1. Where a breach of personal data is likely to result in a high risk to the rights and freedoms of a natural person, the controller shall communicate the data breach personal data to the data subject as soon as possible.2 The communication to the data subject referred to in paragraph 1 of this article describes, in clear and simple terms, the nature of the personal data breach and contains at least the information and measures referred to in points (b), (c) and (d) of Article 33(3) 3. Communication to the data subject referred to in paragraph 1 is not necessary if either of the following conditions is fulfilled: a) the data controller has implemented appropriate technical and organizational protection measures and these measures have been applied to the personal data affected by the said breach, in particular the measures which make the personal data incomprehensible to anyone who is not authorized to have access to it, such as encryption; b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms data subjects referred to in paragraph 1 is no longer likely to materialise; (c) it would require disproportionate effort. In this case, instead, a public communication or a similar measure is taken, whereby the persons concerned are informed in an equally effective manner. […] “.77. Recital 86 of the GDPR provides that, where the breach of personal data is likely to create a high risk for the rights and freedoms of the natural person, the controller should communicate it to the data subject as soon as possible so that he or she can take the necessary precautions.78 In this case, the rapporteur notes that following the data breach, the company SLIMPAY, which has a " procedure for dealing with personal data breaches", considered that the risk associated with it was not high for the persons concerned and that it should therefore not inform them.79. The rapporteur considers, however, that at the With regard to the nature of the personal data, the volume of data subjects, the ease of identifying the persons affected by the breach and the possible consequences for the data subjects, the risk associated with the breach may be con stunned as high and that a communication to the persons concerned should have been made.80. In defence, SLIMPAY indicates that it promptly informed the merchants on whose behalf it had collected the data subject to the data breach, and that they were thus put in a position, in their capacity as responsible for processing, to inform the data subjects if they consider it necessary.81. The company further specifies that, even if the processing carried out for the purpose of improving the fight against fraud was implemented by SLIMPAY as data controller, the data on the basis of which the processing was carried out was initially collected and processed by SLIMPAY as a processor on behalf of these merchants. It was therefore not possible, in its view, to inform the debtors concerned directly without the agreement of those merchants.82. The company considers in any event that the format of the data and the circumstances surrounding the data breach have led it to conclude that there is no high risk for data

subjects within the meaning of Article 34 of the GDPR, with regard to of the following elements: - the format of the data did not make it possible to directly understand the nature or the content of the data; - no disclosure of the data attributable to SLIMPAY has been established; - no usurpation or attempted identity theft was reported by a debtor to SLIMPAY; - the nature of the data did not allow to conclude that there was a high risk of financial fraud; - the risk for a data subject seemed ineffective insofar as any debtor has the ability to oppose an undue debit without justification for eight weeks and up to thirteen months after the transaction with justification.83. The company also points out that it did not have all the email addresses of the persons concerned. It therefore concludes that the individual information of the debtors would have proved impossible for a large part of them. It also considers that a public communication would not have been relevant insofar as its services being offered to professional clients, the majority of the debtors concerned would not have been able to determine whether or not their data had been processed. by it, acting invisibly as a payment service provider.84. Firstly, the Restricted Committee considers that the argument put forward by SLIMPAY to free itself from its liability, according to which the data on the basis of which the processing was carried out was initially collected and processed by SLIMPAY as a subcontractor on behalf of merchants, cannot carry conviction. The fact that the data in question was initially processed for another purpose for which the company acts as a processor does not affect its obligation under Article 34 of the GDPR insofar as it reused this data. for its own account, as data controller.85. Secondly, the Restricted Committee considers that, with regard to the nature of the personal data (including banking information in particular), the volume of people concerned (more than 12 million), the ease of identifying the people affected by the breach based on the accessible data and the possible consequences for the data subjects (risks of phishing or identity theft), the risk associated with the breach had to be considered high.86. Thirdly, the Restricted Committee notes that Article 34-3 of the GDPR provides that communication to the data subjects is not necessary in certain cases, in particular if the controller has implemented technical and organizational protection measures. appropriate, whether he has taken subsequent measures which ensure that the high risk to persons is no longer likely to materialize or whether it would require disproportionate effort. The Restricted Committee considers that the company cannot rely on these provisions insofar as it has not implemented appropriate protection measures to ensure the security of the data affected by the breach (in order to limit their access only to persons allowed). Furthermore, although the company closed the server concerned, the data remained accessible between November 2015 and February 2020, i.e. for a very long period.87. Next, with regard to the company's argument that informing all of the debtors individually would have required disproportionate

efforts, the Restricted Committee notes that the company had 6,250,310 e-mail addresses, i.e. approximately half of those affected. It could therefore at the very least have informed those persons of the data breach, without this representing a disproportionate effort.88. As regards the company's argument that a public communication on its website would not have been relevant since the majority of the debtors concerned would not have been able to determine whether or not they had used the services of SLIMPAY, which operates in an opaque manner as a payment service provider, the Restricted Committee notes first of all that the company's website includes the names of some of its customers and that the debtors of these merchants could thus have be able to know that their data was potentially processed by SLIMPAY and possibly affected by the breach. In this regard, it recalls that any natural person may exercise their rights provided for by the GDPR with any company and thus obtain information on the question of whether or not their data is processed by said company. In the event of a public communication, people who so wish could therefore have contacted the company to find out if they were affected by the data breach. Next, the Restricted Committee observes that information relating to a data breach of this magnitude can be found on the web (social networks, newspapers and specialized sites, etc.). Public communication on the body's website can thus be a starting point and the information can then take on a much more important dimension.89. In view of these elements, the Restricted Committee considers that the company has breached its obligations under Article 34 of the GDPR, relating to the communication to the persons concerned of a personal data breach.III. On corrective measures and their publicity90. Under the terms of III of article 20 of the amended law of January 6, 1978, "When the data controller or its subcontractor does not comply with the obligations resulting from regulation (EU) 2016/679 of April 27, 2016 or the 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 a formal notice provided for in II, seize the restricted formation of the commission with a view to the pronouncement, after adversarial procedure, of one or more of the following measures: […] 7° With the exception of cases where the processing is implemented by the State, an administrative fine not to exceed 10 million euros or, in the case of a company, 2% of the total worldwide annual turnover of the previous financial year, whichever is higher. 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 ".91. Article 83 of the GDPR provides that "each supervisory authority shall ensure that the administrative fines imposed in under this Article for breaches of this Regulation referred to in paragraphs 4, 5 and 6 are, in

each case, effective, proportionate and dissuasive", before specifying the elements to be taken into account in deciding whether to impose an administrative fine and to decide on the amount of this fine.92 Firstly, on the principle of imposing a fine, the company argues in defense that such a measure is not justified. it has complied with its legal and regulatory obligations and that it has cooperated with the CNIL diligently and in good faith since becoming aware of the security incident. It emphasizes in particular that it notified the breach of e data to the CNIL as soon as it becomes known within the regulatory period of 72 hours, has investigations carried out leading to the conclusion that there is no risk for the rights and freedoms of the persons concerned, put in place corrective measures very quickly and informed the merchants concerned at short notice.93. The Restricted Committee recalls that it must take into account, for the pronouncement of an administrative fine, the criteria specified in Article 83 of the GDPR, such as the nature, gravity and duration of the violation, the measures taken by the controller to mitigate the damage suffered by data subjects, the degree of cooperation with the supervisory authority and the categories of personal data affected by the breach.94. The Restricted Committee notes first of all that the breaches concern a very large number of people, since the data breach affected more than 12 million debtors.95. The Restricted Committee then notes that the accessible data (title, surname, first name, e-mail address, postal address, telephone number, BIC/IBAN) make it possible to obtain very precise information on the persons concerned by revealing their identity and contact details. In addition, specific data are in question when some relate to financial information. The fact that the IBAN appears in particular is not insignificant. As the Banque de France indicated in its book "Payments and market infrastructures in the digital age", IBANs are "sensitive" payment data (in the ordinary sense of the term) because they can be used to commit fraud. . The European Data Protection Board describes this type of data as "highly personal". The Restricted Committee considers that the company should have shown particular vigilance with regard to the security of such data, which can be reused by unauthorized third parties, thus harming the persons affected by the data breach. These are, for example, exposed to a risk of identity theft or phishing (or "phishing", i.e. the sending of fraudulent letters for the purpose of obtaining data) when their full identity, associated with their e-mail address for many, was freely accessible.96. Finally, the Restricted Committee notes that the data remained accessible for a very long period, between the end of the import of the data on the server in November 2015 and the discovery of the incident by the company on February 14, 2020, and this then that the processing concerned, the research project, had ended in July 2016. It appears from the elements appearing in the file that, prior to the occurrence of the data breach, the company had not taken the basic measures in terms of security . It was only through a report by a merchant that

the security defect was brought to the attention of the company.97. If the Restricted Committee notes that SLIMPAY immediately reacted to the data breach as soon as it was discovered in February 2020 and that it cooperated throughout the procedure with the services of the CNIL, it considers that the data breach results negligence of basic information system security rules which led to the personal data processed by the company being made accessible to unauthorized third parties.98. The Restricted Committee recalls that the negligence committed in terms of security was particularly serious: access to the server in question was not subject to any satisfactory access restriction measure, the company had not implemented any logging accesses to the server and the data contained in the server could easily be read.99. The Restricted Committee notes that this negligence is all the more serious with regard to the sector of activity of the company which also prides itself on being the European leader in recurring payments and which is a company whose management of information systems complex is the core business.100. The Restricted Committee also notes that, in breach of Article 34 of the GDPR, the company did not inform the persons concerned of the occurrence of the data breach, even though it had more than 6 million addresses of e-mail to do so, ie approximately half of the persons concerned, and that it could have informed the remaining half by means of a public communication on its site.101. Finally, the Restricted Committee recalls that the company has used subcontractors acting under its authority as second-level subcontractors vis-à-vis the merchants, for the services it provides to the latter, without having taken sufficient steps to ensure that the latter provide the required guarantees and without having concluded contracts with some of them containing all the clauses provided for in Article 28 paragraph 3 of the GDPR. 102. Consequently, the Restricted Committee considers that an administrative fine should be imposed with regard to the breaches of Articles 28 paragraphs 3 and 4 of the GDPR, 32 and 34 of the GDPR.103. Secondly, with regard to the amount of the fine, the company considers that that proposed by the rapporteur is disproportionate in view of its economic situation. She insists on her financial deficit and specifies that a high fine would have a catastrophic impact on the jobs she is trying to maintain.104. The Restricted Committee recalls that paragraph 3 of Article 83 of the Rules provides that in the event of multiple violations, as is the case here, the total amount of the fine cannot exceed the amount fixed for the most serious violation. Insofar as the company is accused of a breach of Articles 28, 32 and 34 of the Regulations, the maximum amount of the fine that can be withheld is 10 million euros or 2% of annual turnover. worldwide, whichever is higher.105. The Restricted Committee also recalls that administrative fines must be dissuasive but proportionate. It considers in particular that the activity of the company and its financial situation must be taken into account for the determination of the sanction and in particular, in the event of an

administrative fine, of its amount. It notes in this respect that the company reports a turnover of […] euros in 2019 and […] euros in 2020, for a net result amounting to […] euros in 2019 and […] euros in 2020.106. In view of these elements, the Restricted Committee considers that the imposition of a fine of 180,000 euros appears justified.107. Thirdly, with regard to the publicity of the sanction, the SLIMPAY company argues that it is trying to find a place for itself in a very competitive international market of payment service providers, mainly dominated by Chinese and American companies, who are not very concerned about the protection of Europeans' data. It adds that it has made substantial efforts for more than ten years to become a trusted partner for European economic players, specifying that a public sanction would permanently destroy the results obtained thanks to its efforts.108.The Restricted Committee considers that the publicity of the penalty is justified in view of the seriousness of the breaches committed, their persistence and the number of people concerned.FOR THESE REASONSThe Restricted Committee of the CNIL, after deliberation, decides to: administrative fine in the amount of 180,000 (one hundred and eighty thousand) euros; - make public, on the CNIL website and on the Légifrance website, its deliberation, which will no longer identify the company by name upon expiry a period of two years from its publication. President Alexandre LINDEN This decision may be appealed to the Council of State within two months from the date of publication. er of its notification.