Deliberation of the Restricted Committee No. SAN-2023-023 of 29 December 2023 concerning [redacted]

The Commission nationale de l'Informatique et des Libertés (CNIL - French Data Protection Authority), met in its Restricted Committee consisting of [redacted] (members);

Having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data and on the free movement of such data;

Having regard to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on the processing of personal data and the protection of privacy in the electronic communications sector;

Having regard to amended French Data Protection Act No. 7817 of 6 January 1978, in particular Articles 20 et seq.;

Having regard to amended Decree No. 2019536 of 29 May 2019 implementing French Data Protection Act No. 7817 of 6 January 1978;

Having regard to deliberation No. 2013175 of 4 July 2013 concerning adoption of the CNIL's internal regulations;

Having regard to Decision No. 2021-193C of 29 June 2021 of CNIL's Chair to instruct the general secretary to carry out or have a third party carry out an assignment to verify the personal data processing implemented by or on behalf of the company;

Having regard to the CNIL Chair's decision appointing a rapporteur before the Restricted Committee of 29 March 2022;

Having regard to the report of François Pellegrini, commissioner and rapporteur, notified to [redacted] on 3 July 2023;

Having regard to the written observations made by [redacted] on 18 August 2023;

Having regard to the other documents in the file;

The following were present at the Restricted Committee session on 16 November 2023:

- Mr François Pellegrini, commissioner, his report having been read;

In the capacity of representatives of [redacted]:

- [redacted]

[redacted] having spoken last;

The Restricted Committee has adopted the following decision:

I. Facts and proceedings

1. [redacted] (hereinafter "the company"), whose registered office is [redacted], was registered in the Trade and Companies Register on [redacted]. In 2019, its revenue amounted to [redacted] for a net result of [redacted] and in 2020, its revenue was [redacted], with a net result of [redacted]. In 2023, it had six employees.

2. [redacted] is an electronic money distributor that enables online payments. The company offers two forms of payment solutions: (a) it distributes [redacted] coupons at approved points of sale, through which individuals can make online payments on partner websites; (b) the use of [redacted] coupons can also be accompanied by the creation of an electronic wallet, which requires creating a user account on the [redacted] website or the "[redacted]" mobile application and crediting it by means of coupons or a bank card. Creating a user account makes it possible to make online payments or receive funds. It is this second activity that is at issue in these proceedings.

3. Two audit assignments took place pursuant to Decision No. 2021-193C of 29 June 2021 of the President of the CNIL in order to verify the company's compliance with all the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter "the GDPR") and Law No. 78-17 of 6 January 1978 on data processing, files and freedoms, as amended (hereinafter "the Data Protection Act"). On 24 September 2021, the CNIL first carried out an online audit from the "[redacted]" website. On 13 October 2021, the CNIL departments carried out an on-site audit at the premises of [redacted], located in [redacted]).

4. The main purpose of the online audit of the website [redacted] (now [redacted]) was to verify the procedures for informing individuals and the procedure for creating a user account. It made it possible to observe the storage of cookies and other trackers via the said website. The on-site audit focused more specifically on the verification of the documentation required by the GDPR, the account creation process on the [redacted] mobile application, the retention periods applied to user account data, and the technical and organisational measures for ensuring the security of the data collected through the website and the mobile application.

5. These two audit assignments resulted in the preparation of minutes no. 2021-193/1 and 2021-193/2. In letters dated 8 October, 22 October and 15 November 2021, the company sent the Commission additional information.

6. In accordance with Article 56 GDPR, on 10 May 2023, the CNIL informed all European supervisory authorities of its competence to act as lead supervisory authority for cross-border processing carried out by the Company, as a result of the fact that the Company's sole place of business was in France. After discussion between the CNIL and the European data protection authorities within the framework of the "one-stop-shop" mechanism, it appears that the German, Austrian, Belgian, Cypriot, Danish, Spanish, Finnish, Greek, Irish, Italian, Luxembourg, Dutch, Norwegian, Polish, Portuguese, Romanian and Swedish and authorities are affected by the processing of user accounts that have been created by residents of these States.

7. In order to examine these items, the CNIL Chair appointed Mr François Pellegrini as rapporteur on 29 March 2022, pursuant to Article 22 of the French Data Protection Act.

8. On 3 July 2023, the rapporteur notified the company of a report detailing breaches of Articles 5(1)(e), 12, 13 and 32 of the GDPR and Article 82 of the French Data Protection Act, which he deemed to have occurred in this case.

9. On 18 August 2023, the company submitted observations in response to the sanction report.

10. In a letter dated 29 September 2023, the rapporteur informed the company's counsel that the investigation was closed, pursuant to Article 40, III of amended decree no. 2019-536 of 29 May 2019.

11. In a letter dated 02 October 2023, the company was informed that the case file was on the agenda of the Restricted Committee of 16 November 2023.

12. The rapporteur and the company presented verbal observations at the Restricted Committee meeting.

II. Reasons for the decision

A. On the European cooperation procedure

13. Pursuant to Article 60(3) of the GDPR, the draft decision adopted by the Restricted Committee was transmitted to the other competent European supervisory authorities on 29 November 2023.

14. As of 28 December 2023, none of the supervisory authorities concerned had raised a relevant, reasoned objection to this draft decision, so that, pursuant to Article 60(6) of the GDPR, they are deemed to have approved it.

B. On the breach of the requirement for limitation of the data retention period

15. According to the terms of Article 5(1)(e) of the GDPR, personal data must be "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.*"

16. **The rapporteur** noted that when creating a user account on the [redacted] website, the surname, first name, date of birth, postal address, email address, telephone number and, where applicable, bank details were collected, as well as personal documents, such as proof of identity and address. However, the rapporteur noted that it was apparent from the on-site audit that if the company had specified a retention period of ten years for this data from the last transaction carried out on the account, in fact, the accounts were merely deactivated at the end of this period, while the data itself was retained in the production database for an indefinite period. It also noted that no purge had been carried out in the company's databases since the start of its activity in 2005. In particular, the rapporteur considered that the company's letter of 15 November 2021 showed the retention of 70,049 accounts that had been inactive for more than ten years. In addition, he was of the view that the company had not provided evidence of the application of the new five-year retention period that it defined following CNIL audits for user

account data. Finally, he noted that 51,735 accounts were being kept for no purpose, insofar as they were "unconfirmed", i.e. the email address had not been confirmed when the account was created.

17. **In its defence**, during the investigation, the company first stated that it had set a ten-year retention period for user accounts for the purposes of combating money laundering and the financing of terrorism ("AML-CFT") before stating, in its letter of 15 November 2021, that this period was now only applied to customer contracts entered into for an amount greater than €120 excluding tax, pursuant to Article D. 213-1 of the French Consumer Code, and that the other user account data would now be retained for five years from the last transaction carried out on the account. In its observations in response, the company also corrected the declarations made during the investigation as to the period applicable to the retention of certain data for AML-CFT purposes, which is five years pursuant to Article 561-2 of the French Monetary and Financial Code. The company submits that the request provided for the 70,049 inactive accounts would show that these accounts have been on the database for ten years, and not for more than ten years. It explains that the sole purpose of this request was to show the effective application of the new five-year retention period that it had defined. In its comments, the company provides a new screenshot intended to unambiguously show the removal of accounts that have been inactive for five years.

18. Regarding the 51,735 unconfirmed accounts, the company claims that the data associated with these accounts is retained for one year and then deleted if the account is not confirmed. It states that the purpose of this retention is to give users sufficient time to confirm their account, and accuses the rapporteur of having prejudged excessive retention of data associated with unconfirmed accounts, without even questioning the purpose of the processing and the retention period applied to this data.

19. **The Restricted Committee** points out, firstly, that the personal data retention period must be specified according to the purpose of the processing. In cases where the data are no longer necessary for the purpose for which they were collected, they must either be deleted, or be subject to intermediate archiving when storage of the data is necessary for compliance with legal obligations or for pre-litigation or litigation purposes. The data thus placed in intermediate archiving are then archived for a period not exceeding that necessary for the purposes for which they are stored, in accordance with the provisions in force. Thus, after having carried out a sorting of relevant data to be stored, the data controller must provide for this purpose a dedicated archive database or logical separation in the active database. This logical separation is ensured by the implementation of technical and organisational measures ensuring that only persons with an interest in processing the data due to their duties can access them. Beyond these interim archival retention periods, personal data must, subject to exceptions, be deleted or anonymised (CNIL, FR, 8 September 2022, Sanction, Group X, no. SAN-2022-018, published)

20. Secondly, pursuant to Article L. 213-1 of the French Consumer Code: "*In cases where the contract is signed electronically and relates to an amount equal to or greater than an amount fixed by decree, the professional contractor shall ensure the retention of the document which records it for a period specified by the same decree, and shall guarantee its co-contractor access to it at all times if the latter so requests*." Article D. 213-1 of the same code provides that "*[t]he amount specified in ArticleL. 213-1 is set at 120 euros*" and Article D. 213-2 provides that "*[t]he period specified in Article L. 213-1 is set at ten years from the conclusion of the contract in cases where the delivery of the goods or the performance of the service is immediate. Otherwise, the period shall run from the conclusion of the contract until*

the date of delivery of the goods or performance of the service and for a period of ten years from this date."

21. In this case, **the Restricted Committee** notes first of all, with regard to the retention of 51,735 unconfirmed accounts in the database, that although the company's letter of 15 November 2021 stated that the data of "inactive prospects" was deleted after one year, the retention period policy attached to this letter paradoxically provided for a retention period of three years for data related to the "management of non-customer prospect files". At the hearing, the company explained this contradiction by the fact that the three-year retention period was solely aimed at retention for commercial prospecting purposes, and that it was no longer engaged in this type of activity. In any event, the Restricted Committee is of the view that in its observations in defence, the company is providing evidence for a period and purpose for the retention of data from unconfirmed accounts, namely a retention period of one year in order to allow the data subjects to have adequate time to confirm their account. For this reason, it is of the view that the information for this case is not sufficient evidence of a breach of Article 5(1)(e) of the GDPR on this point.

22. Next, **the Restricted Committee** notes that on the date of the on-site audit, the company specified a period of ten years, which begins to run on the date of activation of the user account. Nevertheless, it notes that at the end of this period, the user accounts were inactivated but that the company continued to keep the account data in the database for an indefinite period. The Restricted Committee further notes that according to the statements of the company itself, no data purging had been carried out since 2005.

23. With regard to the retention of 70,049 inactive accounts, **the Restricted Committee** notes that the screenshot provided by the company in its letter of 15 November 2021 was intended to illustrate, at the request of the CNIL, "*the number of inactive accounts with a creation date more than 10 years prior to 13 October 2021*." The Restricted Committee is of the view that, given the explanations provided by the company, the screenshot that was taken showed the retention of accounts inactive for ten years, and not for more than ten years.

24. Nevertheless, **the Restricted Committee** notes that it follows from what has been stated above that when the retention period is reached, personal data must be deleted or anonymised and that the act of rendering an account inactive equates neither to the deletion of the personal data it contains, nor to anonymisation. Therefore, it emerges from the documents in the file that as of the date of the on-site audit, the company was retaining user account data, even if inactivated, for an indefinite period.

25. In any event, **the Restricted Committee** observes that the aforementioned screenshot and the other elements of the file show that until the audits carried out by the CNIL agents, the data of 70,049 customer accounts had been present in the database for ten years without any form of sorting between the data to be retained, in accordance with the provisions of Article D. 213-1 of the French Consumer Code, and the data to be deleted. The Restricted Committee notes that the five-year retention period for data other than those covered by this provision was only specified at the end of the on-site audit, as confirmed by the company in its letter of 15 November 2021, and that proof of its effective application was provided only during its observations in its defence, on 18 August 2023. For this reason, the Restricted Committee is of the view that the company has retained the data of accounts not covered by Article D. 213-1 of the French Consumer Code for excessive periods.

26. **Consequently**, the Restricted Committee is of the view that the above facts amount to a breach of Article 5(1)(e) of the GDPR.The Restricted Committee notes that during the procedure, the company complied with the implementation and application of adequate retention periods for user account data, with regard to the various purposes pursued. It nevertheless reiterates that these compliance efforts cannot absolve the company from its responsibility for past events.

C. On the breach of the obligation to inform people

27. Pursuant to Article 12 of the Regulation, the data controller must provide the data subjects with the information provided for in Article 13 of the same Regulation "*in a concise, transparent, comprehensible and easily accessible manner, in clear and simple terms* […]".

28. Article 13 of the GDPR lists the information to be provided to the data subject in cases where the personal data are collected directly from him/her. This information include the identity of the data controller and their contact details, the purposes of the processing operation, its legal basis, the recipients or categories of recipients of the data, and where applicable, the fact that the data controller intends to transfer data to a third country. In addition, the article requires the data controller, where deemed necessary to ensure "fair and transparent processing" of personal data in this case, to inform individuals of the period for which the personal data will be stored, the existence of various rights that individuals have, the existence of the right to withdraw consent at any time and the right to lodge a complaint with a supervisory authority.

29. The Regulations do not specify the means by which such information is to be provided. In practice, this information is generally grouped within a privacy policy.

30. In his report, **the rapporteur** notes in substance that the information provided by the company on the [redacted] website and on its mobile application via the privacy policy was incomplete, out of date and in English only. The rapporteur notes, however, that the company has, since the audits, engaged in a compliance process, although this has no bearing on past shortcomings.

31. **In its defence**, the company does not dispute this conclusion, but maintains that it has achieved compliance on this point since the audits. It accuses the rapporteur of basing certain claims in his report on informal verifications, at the end of which he supposedly found that shortcomings persisted on the day the report was sent, separately from any finding recorded in the presence of both parties in a report.

32. **The Restricted Committee** notes, first of all, that the findings made during the audits show that with regard to the [redacted] website, a privacy policy available at the bottom of the website's home page was available only in English. In this respect, it notes, as does the rapporteur, that the information provided by means of a privacy policy available only in English, relating to data processing targeting a mainly French-speaking audience, is insufficient to enable the data subjects to assess in advance the scope and consequences of the processing, and therefore does not comply with the requirements of transparency of information laid down by Article 12 of the GDPR. The Restricted Committee is of the view that the same is true of the English language-only reference made to the privacy policy on the account creation form.

33. Next, the Restricted Committee notes that the homepage of the website and the user account creation page both referred to versions of the 2018 and 2021 privacy policy, which mentioned

neither the retention period of the data nor the right to lodge a complaint with the CNIL. The Restricted Committee notes that in view of the data processed by the company, including bank details, such information was necessary to ensure fair and transparent processing within the meaning of Article 13(2) of the GDPR. It also notes, like the rapporteur, that the coexistence of these two incomplete versions of the privacy policy was likely to create confusion among data subjects as to the extent of the rights they had with regard to their data and the consequences of their processing.

34. With regard to the [redacted] mobile application, **the Restricted Committee** notes that as of the date of the audits, the account creation page also offered an incomplete privacy policy dated 2018, available in English only, disregarding Articles 12 and 13 of the GDPR in the same way for the reasons already given with regard to the website.

35. Consequently, **the Restricted Committee** is of the view that the company committed a breach of articles 12 and 13 of the GDPR. It specifies that the breach which it considered is the one which became apparent at the time of the audits, and that the informal verifications by the rapporteur preceding the submission of his report were only intended to draw the company's attention to the fact that it had not yet achieved compliance. The Restricted Committee notes that the company is now in compliance.

D. On the breaches of the obligation to ensure the security of personal data

36. Article 32(1) GDPR provides that *"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:*

a) the pseudonymisation and encryption of personal data;
b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
d) *a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing*".

1. <u>On user account passwords</u>

37. In order to recommend that the Restricted Committee take the view that the company had breached its obligations under Article 32 of the GDPR, **the rapporteur** noted that during the online audit, the delegation had first noted that when creating a user account on the company's website, six-character passwords composed of three categories of characters (upper case, lower case and numbers) were accepted and that no access restriction in the event of failed authentication was implemented. In addition, he noted that 49,214 passwords were recorded in plain text in the company's database and associated with their email address and identifier. Finally, the rapporteur noted that the passwords that were not kept in plain text were stored in a hashed and salted form using the SHA-1 function, which was deemed obsolete.

38. **In its defence,** the company does not dispute the breaches, but states that it has taken corrective actions. First of all, it points out that it has modified its password policy in order to achieve the minimum entropy rate of 50 bits recommended by the CNIL in cases where this password is accompanied by an access restriction measure, and states that it completed implementing these new measures in August 2023. It also accuses the rapporteur of relying on informal checks which supposedly enabled him to find entropy that was still insufficient at the date on which the report was sent. Next, the company states that access to unencrypted passwords was due to technical constraints related to the implementation of password encryption measures for old accounts created when it first started trading, and that as of the date of its submissions in its defence, all passwords are encrypted in the database. Lastly, the company takes note of the rapporteur's conclusions concerning the use of the SHA-1 hashing algorithm, and announces that it has opted to switch to the SHA-512 standard, effective since July 2023.

39. **Firstly, the Restricted Committee** points out that it follows from the provisions of Article 32 of the GDPR that the data controller is required to ensure that the automated data processing it implements is sufficiently secure. The adequacy of the security measures is assessed, firstly, with regard to the characteristics of the processing and the risks it entails, and secondly, taking into account the state of knowledge and the cost of the measures.

40. The Restricted Committee is of the view that the use of overly lenient rules governing password complexity, which would allow users to choose passwords that are insufficiently strong, can lead to attacks by unauthorised third parties, such as "brute force" or dictionary" attacks, which involve successively and repeatedly testing numerous passwords, thus compromising the associated accounts and the personal data contained in those accounts.

41. In this respect, the Restricted Committee notes that the need for a strong password is recommended by both the French National Cyber Security Agency (ANSSI) and the CNIL in its deliberation no. 2017-012 of 19 January 2017 adopting a recommendation on passwords, this requirement being confirmed in its deliberation no. 2022-100 of 21 July 2022.

42. By way of illustration, the rapporteur points out that the Commission is of the view in its deliberation no. 2017-012 of 19 January 2017 – which admittedly is not binding, but does provide relevant clarification on the measures to be taken in terms of security – that, in order to ensure a sufficient level of security and confidentiality, in the event that authentication is based solely on an identifier and a password, the latter must be composed of at least twelve characters including upper case letters, lower case letters, numbers and special characters.

43. Failing this, the Commission is of the view that authentication based on a password with a minimum length of eight characters, consisting of three different categories of characters but accompanied by an additional measure such as, for example, timing out access to the account after several failures (temporary suspension of access, the duration of which increases as attempts are made), the implementation of a mechanism to protect against automated and intensive attempts, (e.g. "captcha") and/or locking the account after several unsuccessful authentication attempts (a maximum of ten).

44. The Restricted Committee points out that it has repeatedly imposed financial penalties where a breach of Article 32 of the GDPR is caused by insufficient measures to guarantee the security of the data processed. Deliberations no. SAN-2019-006 of 13 June 2019, no. SAN-2019-007 of 18 July 2019 and no. SAN-2022-018 of 8 September 2022 specifically refer to weak passwords.

45. Firstly, the Restricted Committee points out that securely storing passwords constitutes a basic precaution in the protection of personal data. In 2013, the ANSSI issued an alert and a reminder of best practice regarding the retention of passwords, stating that they must "be stored in a form transformed by a one-way cryptographic function (hash function) that is slow to calculate, such as PBKDF2" and that "the transformation of passwords must involve a random salt to prevent an attack using pre-computed tables" (ANSSI, "CERTA-2013-ACT-046 News Bulletin", 15 November 2013, https://www.cert.ssi.gouv.fr/actualite/CERTA-2013-ACT-046/).

46. Similarly, in its deliberation no. 2017-012 of 19 January 2017, the CNIL had already stated that it "recommends [that the password] be transformed by means of a non-reversible and secure cryptographic function (i.e. using a reputable public algorithm whose software implementation is free of known vulnerability), integrating the use of a salt or a key." This is because the non-robust hash functions have known vulnerabilities that do not protect the integrity and confidentiality of passwords in the event of a brute force attack once the servers that host them have been compromised.

47. The Restricted Committee notes that in this case, the passwords of users of the [redacted] website were required, at the time of the audits, to be composed of six characters of three different kinds and without any additional security measures.

48. It is of the view that a composition of this kind did not protect the security of the data and prevent unauthorised third parties from having access to it. The Restricted Committee points out that, as highlighted by the rapporteur, as of the day of the on-site audit, the company was processing the data of nearly 700,000 user accounts, such as surname, first name, date of birth and email address, postal address, telephone number, and also bank details (in cases where the user had opted to add an electronic wallet) or proof of identity and address (in cases where a payment exceeds a certain amount). However, authentication based on the use of this kind of short password, without additional security measures, may lead to attacks by unauthorised third parties, and thus to a compromise of user accounts and the numerous forms of personal data they contain.

49. Consequently, the Restricted Committee is of the view that the password policy in use was not sufficiently robust to guarantee the security of the data processed, which breaches Article 32 of the GDPR.

50. **Secondly**, the Restricted Committee notes that the storage of user passwords in plain-text form, associated with their identifiers and email addresses, fails to ensure their security. This retention method implies that any person with access to the company's customer database may view and collect them. These user passwords, together with their identifiers, provide access to all the personal data contained in their [redacted] accounts, and even to other service accounts, with – as the rapporteur pointed out – the same identifiers and passwords often being used to access several services.

51. For these reasons, the Restricted Committee is of the view that the methods for storing passwords, on the date of the findings, failed to ensure the security and confidentiality of the personal data of [redacted] account holders, which is in breach of Article 32 of the GDPR.

52. **Thirdly,** the Restricted Committee points out that the use of the SHA-1 function for the hashing of passwords is no longer deemed to comply with best practice, as emerges in particular from the guide for the selection of cryptographic algorithms published by ANSSI, dated 8 March

2021, which states that it is *"prohibited for general use"*. The Restricted Committee also points out that in view of current best practice, CNIL has drawn up specific recommendations in its guide for developers, recommending the storage of passwords "*in the form of a hash using a proven library, such as Argon2, yescrypt, scrypt, balloon, bcrypt and, to a lesser extent, PBKDF2."(* https://lincnil.github.io/Guide-RGPD-du-developpeur/)·

53. **Consequently**, the Restricted Committee is of the view that the above actions, which have not been contested by the company, constitute a breach of its obligations under article 32 of the GDPR. It notes that since the audits, the company has remedied the observed breaches by implementing a password policy with an adequate level of security, encrypting all passwords and providing evidence of the implementation of a satisfactory hash system for said passwords, in SHA-512.

2. On shared access to the customer database

54. **The rapporteur** noted that, during the on-site audit, the delegation was informed that the account used for access to the customer database was shared by the development team.

55. **In its defence**, the company disputes the existence of any breach of regulations. It argues that only an employee has restricted access to the database to carry out their duties as a developer, and that a second person is authorised to access this database as part of their duties as a database administrator. It states that the login procedure is carried out by means of a bastion, i.e. via an intermediary server that then provides access to the database. Once connected to the bastion, connection to the database is enabled by a complex sixteen-character username and password: the company states that the database administrator and the developer have separate usernames and passwords to connect to the database, and that the connection is filtered by IP address, making it possible to preserve the traceability of access to the database.

56. **The Restricted Committee** notes that the explanations provided by the company reveal that the development team consists of a single employee and that, therefore, only two persons are authorised to access the customer database; namely (a) the administrator of the database and (b) the developer, who has restricted access to this database. The Restricted Committee also notes that both the developer and the administrator have an individual access account to this database.

57. **Consequently**, the Restricted Committee is of the view that there has been no breach.

E. On the breaches of the obligation under Article 82 of the French Data Protection Act

58. Article 82 of the French Data Protection Act stipulates: *"Any subscriber or user of an electronic communications service must be informed in a clear and complete manner, unless he or she has been previously informed by the data controller or their representative:*
1° of the purpose of any action aimed at electronically accessing information already stored in their electronic communications terminal equipment, or writing information to this equipment;
2° Of how he or she can object to it.
Such access or recording may only take place provided that, after receiving such information, the subscriber or user has expressed his or her consent which may result from the appropriate parameters of his/her connection device or any other device under his or her control.

These provisions shall not apply if access to the information stored in the user's terminal equipment or the recording of information on the user's terminal equipment:
1° Either is for the exclusive purpose of enabling or facilitating communication by electronic means;
2 Or is strictly necessary for the provision of an online communication service at the express request of the user."

59. These provisions incorporate Article 5(3) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (called the "ePrivacy Directive") into French law.

1. <u>On the storage of [redacted] cookies on the user's device without consent</u>

60. **The rapporteur** notes that during the online audit, the delegation noted the storage of thirteen cookies before any action by the user as soon as they arrived on the home page of the [redacted] website, including [redacted] Analytics audience measurement cookies, which should have been subject to the user's prior consent.

61. **In its defence,** the company first argued during the investigation that the [redacted] Analytics cookie was an audience measurement tool for internal use that was exempt from the collection of consent, before acknowledging the acts in its submissions in its defence and announcing that it no longer used this tool. It provided a document certifying that as of 16 August 2023, [redacted] Analytics cookies are no longer stored on the devices of users of the [redacted] website and application.

62. **The Restricted Committee** points out that Article 82 of the French Data Protection Act states that the operations of accessing or registering information on a user's device may only take place after the user has expressed their consent, with only cookies whose exclusive purpose is to allow or facilitate communication by electronic means, or cookies which are strictly necessary for the provision of an online communication service at the express request of the user, being exempt from this obligation.

63. The Restricted Committee is of the view that the documentation made available online by [redacted] shows that (a) depending on the settings used by the publisher of the website concerned, [redacted] Analytics cookies may include advertising functions, and that (b) regardless of the settings used for the aforementioned advertising functionalities, the data collected via [redacted] Analytics cookies may be reused to maintain and protect the Analytics service.

64. For this reason, the Restricted Committee is of the view that the storage of these cookies is subject to prior collection of the user's consent if they are not exclusively intended to allow or facilitate communication by electronic means and are not strictly necessary for the provision of a service expressly requested by the user.

65. **Consequently**, the Restricted Committee is of the view that in allowing the storage and reading of the [redacted] Analytics cookie on individuals' devices upon arrival at the [redacted] website, without first obtaining their consent, the company deprived them of the possibility granted to them by Article 82 of the French Data Protection Act to make a choice as to the storage of trackers on their device.

66. The Restricted Committee notes that the company demonstrated during the proceedings that since 16 August 2023, no more [redacted] Analytics cookies have been stored on users' devices. The rapporteur nevertheless reiterates that the compliance measures adopted cannot absolve the company from its responsibility for past breaches.

2. <u>On the use of the [redacted] Captcha mechanism without obtaining the user's consent</u>

67. **The rapporteur** notes that the company used the [redacted] Captcha module, with the aim of blocking robots on the registration and connection page to the [redacted] website and mobile application. It is of the view that the use of a module without obtaining the prior consent of the user is contrary to Article 82 of the French Data Protection Act, insofar as it does not fall under any of the exemptions provided for in this article.

68. **In its defence**, the company does not dispute the actions described by the rapporteur, but states that it has remedied the shortcomings noted in the report, by making the use of [redacted] Captcha subject to the prior consent of the user and by not storing any cookie or tracker on their device in the event of refusal. The company adds that [redacted] Captcha will be definitively replaced by another solution at the end of October 2023.However, it thinks that, , in light of the relatively opaque and inaccessible information provided by [redacted] with regard to the consequences related to the use of the [redacted] Captcha service, it would be unfair to hold its client companies responsible for breaches of Article 82 of the French Data Protection Act without taking into account the lack of transparency and accessibility of the contractual information provided by [redacted], which has already been the subject of CNIL judgements on these grounds (CNIL [redacted] Consequently, it requests a reduction of the proposed fine.

69. In this case, the Restricted Committee notes that a [redacted] Captcha mechanism, provided by [redacted], is used when creating an account and when connecting to the [redacted] website and mobile application. The restricted committee is of the view that it was the website publisher - in this case [redacted] - who chose to use the [redacted] Captcha mechanism, and therefore permitted read and write operations for the data on users' devices.

70. In view of this information, the Restricted Committee is of the view that the company is not justified in arguing that it would be unfair to hold [redacted]'s corporate clients (including the company) responsible for breaches of Article 82 of the French Data Protection Act, and pointing to the lack of transparency and accessibility of [redacted]'s contractual conditions. Rather, the Restricted Committee is of the view that in its capacity as a company using [redacted] Captcha service, the company is also responsible for compliance with the provisions of the French Data Protection Act when using this mechanism.

71. **Secondly**, the Restricted Committee is of the view that while a data controller can claim an exemption from information and collection of consent in cases where the read/write operations performed on a user's device are for the sole purpose of securing an authentication mechanism for the benefit of users (see on this point CNIL, FR, 27 September 2021, Sanction, FIGARO Company, No. SAN-2021-013, published), this does not apply in cases where these operations also pursue other purposes that are not strictly necessary for the provision of a service. However, the purpose of the [redacted] Captcha mechanism is not solely to secure the

authentication mechanism for the benefit of users; it also enables analysis operations by [redacted] which [redacted] itself specifies in its General Terms and Conditions of Use.

72. The Restricted Committee notes that [redacted] informs companies using [redacted] Captcha technology, under the General Terms and Conditions of Use available online, that the operation of the [redacted] CAPTCHA API is based on the collection of hardware and software information (such as data on devices and applications) and that these data are sent to [redacted] for analysis. [redacted] also states that such companies are responsible for informing users and requesting their permission regarding the collection and sharing of data with [redacted]

73. It emerges from this information that [redacted] should have informed users and obtain their consent, which they did not do in this case.

74. In view of the above, the Restricted Committee is of the view that by using the [redacted] Captcha mechanism provided by [redacted] without obtaining their consent, the company breached the provisions of Article 82 of the French Data Protection Act. The Restricted Committee notes, as confirmed at the hearing, that [redacted] ceased to use this technology at the end of October 2023. However, as of the date of the audits, this mechanism was indeed in use, without the prior consent of the users.

III. Corrective measures and publication

75. Under the terms of Article 20 III of the amended Act of 6 January 1978:

"When the controller or its subcontractor fails to comply with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or this law, the President of the CNIL may also, if applicable, after sending the warning specified in point I of this article or, where applicable, in addition to an order provided for in II, contact the CNIL's Restricted Committee with a view to the imposition, after proceedings in which both sides are represented, 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 may not exceed EUR 10 million or, in the case of an undertaking, 2% of the total worldwide annual turnover of the preceding financial year, whichever is greater. In the cases mentioned in 5 and 6 of Article 83 of Regulation (EU) 2016/679 of 27 April 2016, these upper limits will be increased, respectively, to €20 million and 4% of said revenue. In determining the amount of the fine, the Restricted Committee shall take into account the criteria specified in the same Article 83."

76. Article 83 of the GDPR specifies that "*Each supervisory authority shall ensure that the imposition of administrative fines* […] *shall in each individual case be effective, proportionate and dissuasive*", before specifying the elements to be taken into account when deciding whether to impose an administrative fine and to decide on the amount of that fine.

A. On the issue of an administrative fine and its amount

1. On the issue of an administrative fine

77. **In its defence**, the company maintains that the proposed administrative fine is disproportionate to the alleged breaches and its conduct since it has implemented several corrective measures,

including the effective application of its user account data retention policy, the implementation of a password policy with an adequate level of security, the use of a password hash algorithm in accordance with the state of the art and the collection of consent to the deposit of cookies and trackers where required. With regard to this last breach, it maintains that it is unfair to hold publishers solely liable when, in reality, it is the restrictive policy of the CNIL that seeks to prevent the use of certain tools such as those offered by [redacted]. In addition, it stresses that it has fully cooperated with the CNIL's staff. Finally, it maintains that the fine of €200,000 proposed by the rapporteur is equivalent to 1.8% of its 2020 turnover, and is therefore excessive.

78. **The Restricted Committee** notes that, in imposing an administrative fine, it must take into account the criteria specified in article 83 of the GDPR, such as the nature, severity and duration of the infringement, the scope or purpose of the processing concerned, the number of people affected, the measures taken by the data controller to mitigate the damage suffered by the data subjects, the fact that the breach was committed due to negligence, the degree of cooperation with the supervisory authority and, in some cases, the level of damage suffered by the data subjects.

79. The Restricted Committee notes, firstly, that the company's alleged breaches infringe fundamental principles provided for under the GDPR, and affect many people.

80. With regard to the breach of the principle of limiting the retention period of personal data, the company was negligent, merely inactivating the user accounts it kept instead of anonymising or deleting the data contained therein. In any event, assuming it was applied, the ten-year retention period declared during the audits was not accompanied by any sorting of the data to be retained from the data to be deleted, as confirmed by the company at the. The restricted committee notes that this breach potentially concerns a significant number of people, with the company claiming about 700,000 users having an account at the date of the audits.

81. With regard to the breach of the obligation to inform data subjects and of transparency, the Restricted Committee notes that the company failed to comply with the requirement to provide complete and transparent information to data subjects, despite the fact that this constitutes an essential prerequisite for this type of processing of personal data.

82. With regard to the breach of the obligation to ensure the security of personal data, the Restricted Committee emphasises the number of observed breaches of basic security obligations; namely, the use of an insufficiently robust password for user accounts containing, in some cases, bank details and the hashing of passwords by means of an obsolete function. The Restricted Committee, like the rapporteur, is of the view that this series of security flaws by a company offering online payment solutions and collecting categories of highly personal data has helped to accentuate the fact that said data did not sufficiently benefit from the protection offered by the GDPR.

83. With regard to the breach relating to cookies stored on the user's device when visiting the company's website, the Restricted Committee is of the view that the failure to obtain consent affected each of the individuals who visited the website in question, which necessarily amounts to several hundreds of thousands of people, given the fact that the company reported around 328,186 million unique visitors to its website between September 2020 and September 2021. It also notes that the use of the [redacted]Captcha module without obtaining prior user consent affected – at least potentially – the 700,000 account holders as of the date of the audits.

84. Finally, while taking into account that the company has put in place measures following the issuance of the sanction report, the Restricted Committee notes that these actions do not exempt the company from its liability for past breaches.

85. **Consequently**, the Restricted Committee is of the view that there are grounds to impose an administrative fine for the breaches of Articles 5(1)(e), 12, 13 and 32 of the GDPR and Article 82 of the French Data Protection Act.

2. <u>On the amount of the administrative fine</u>

86. The Restricted Committee notes, firstly, that the breaches relating to Articles 5(1)(e), 12 and 13 of the GDPR constitute breaches of key principles of the GDPR which, under Article 83 of the GDPR, may be subject to an administrative fine of up to €20,000,000 and up to 4% of annual revenue, whichever is greater.

87. The Restricted Committee subsequently notes that administrative fines must be effective, proportionate and dissuasive. It notes that in 2020, [redacted] generated revenue of around €4.6 million and a net loss of around €3.7 million. The Restricted Committee notes that the rapporteur rejected the breach relating to the sharing of database access accounts, and that the company does not dispute the other breaches referred to in the report.

88. **Therefore**, with regard to the company's liability, its financial capacity and the relevant criteria of Article 83 of the Regulation, the Restricted Committee is of the view that an administrative fine of 90,000 (ninety thousand) euros, for the breaches constituted by Articles 5(1)(e), 12, 13 and 32 of the GDPR, and an administrative fine of 15,000 (fifteen thousand) euros with regard to the breaches of Article 82 of the French Data Protection Act appear justified.

B. <u>On publication of the decision</u>

89. **The company** disputes the rapporteur's proposal to make this deliberation public, invoking in particular the protection of business secrets that it claims fall under its contractual obligations under the contract entered into with the electronic money issuing institution.

90. **The Restricted Committee** is of the view that the publication of this Decision is justified in view of the severity of the breaches in question and the number of data subjects. It is also of the view that the publication of the sanction will in particular inform all the data subjects of the consequences of the breaches. Finally, with regard to the argument related to the disclosure of business secrets, it points out that information relating to business secrets is concealed from its published decisions.

91. Lastly, the measure is proportionate since the decision will no longer identify the company by name upon expiry of a period of two years following its publication.

FOR THESE REASONS

CNIL's Restricted Committee, after having deliberated, decides to:

- **issue [redacted] with an administrative fine of ninety thousand euros (€90,000) for breaches committed under Articles 5(1)(e), 12, 13 and 32 of (EU) Regulation No. 2016/679 of 27 April 2016 on data protection;**

- **issue [redacted] with an administrative fine of fifteen thousand euros (€15,000) for breaches of Article 82 of the French Data Protection Act as amended;**

- **publish its decision on the CNIL and Légifrance websites, which will no longer identify the company at the end of a two-year period following its publication.**

The Chair of the Restricted Committee

Alexandre LINDEN

This decision may be appealed before the CE within two months of its notification.