Deliberation of the Restricted Committee no. SAN-2022-018 of 8 September 2022 concerning the Economic Interest Group [redacted]

The Commission Nationale de l'Informatique et des Libertés (CNIL - French Data Protection Agency) met in its Restricted Committee consisting of Mr Alexandre Linden, Chair, Mr Philippe-Pierre Cabourdin, Vice-Chair, Ms Christine Maugüé, Mr Alain Dru and Mr Bertrand du Marais, 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 amended French Data Protection Act No. 78-17 of 6 January 1978, in particular articles 20 *et seq.*;

Having regard to amended Decree No. 2019-536 of 29 May 2019 implementing French Data Protection Act No. 78-17 of 6 January 1978;

Having regard to Deliberation No. 2013-175 of 4 July 2013 adopting the internal rules of procedure of the CNIL (French Data Protection Authority);

Having regard to Decision No. 2021-032C of 6 January 2021 of the CNIL's Chair instructing the General Secretary to carry out, or have carried out, an audit of the data processing activities accessible from the website [redacted] or concerning personal data collected from this domain;

Having regard to the decision of CNIL's Chair appointing a rapporteur before the Restricted Committee meeting of 21 October 2021;

Having regard to the report of Mr François Pellegrini, the commissioner rapporteur, notified to the Economic Interest Group [redacted] on 16 February 2022;

Having regard to the written observations made by the Economic Interest Group [redacted] on 15 April 2022;

Having regard to the other documents in the case file;

The following were present at the Restricted Committee session on 12 May 2022:

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

As representatives of the Economic Interest Group [redacted]:

[redacted];

The Economic Interest Group [redacted] having last spoken;

The restricted committee has adopted the following decision:

I. Facts and proceedings

1. [redacted] (hereinafter "the organisation" or "the group"), whose registered office is located at [redacted] is an Economic Interest Group [redacted] that has been publishing the service for the dissemination of legal and official information on companies through several channels since 1986, in particular the website [redacted] since 1996.

2. The website [redacted] allows users to view legal information on companies and to order documents [redacted] Users wishing to view or order a paid document on the website must have an account and are designated by [redacted] as "members". Users can also take out an annual subscription, enabling "subscribers" to access certain services in the business consultation section. When creating a member or subscriber account, the user must complete the following mandatory fields: last name, first name, postal and email addresses, landline or mobile telephone and choice of a secret question and its answer. Subscribers' bank details (IBAN and BIC) are also processed by [redacted].

3. In 2019, the organisation generated revenue of [redacted] and a net loss of [redacted] In 2020, it generated revenue of [redacted] and a net loss of [redacted].

4. On 12 December 2020, the Commission nationale de l'informatique et des libertés (hereinafter "the CNIL" or "the Commission") received a complaint about the organisation from an individual stating that the website [redacted] stores users' passwords in clear text and that she was able to obtain her password over the telephone by simply giving her name to the helpline operator.

5. Pursuant to decision no. 2021-032C of 6 January 2021 by the CNIL Chair, an investigation was carried out to verify the compliance of any processing accessible from the domain [redacted], or concerning personal data collected from the latter, with the provisions of the amended law no. 78-17 of 6 January 1978 concerning information technology, files and freedoms (hereinafter "the amended law of 6 January 1978" or the "French Data Protection Act") and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the "Regulation" or the "GDPR").

6. As such, an online audit was carried out on 4 March 2021 on the website [redacted] implemented by the grouping. Record no. 2021-032/1 drawn up at the end of this audit was notified to the organisation by registered letter, received on 10 March 2021.

7. The CNIL delegation focused in particular on verifying the procedure for transmitting users' passwords when an account is created or in the event that a password is forgotten or lost.

8. By letters dated 19 March, 25 May and 24 June 2021, the organisation sent to the CNIL the information requested in record no. 2021-032/1 and replied to its requests for additional information sent by email on 17 May and 18 June 2021. In particular, the organisation confirms that it determines the purposes and methods of implementing the processing of personal data on the website [redacted]. It also specifies how long it keeps the data it collects and the measures taken to ensure their security. [redacted] also told the delegation that during 2020, the website was visited by over 24 million people worldwide and that, of the 3.7 million people with an account, more than 8,000 European accounts were not French.

9. In accordance with article 56 of the GDPR, the CNIL informed all European supervisory authorities of its competence to act as lead supervisory authority regarding cross-border processing implemented by [redacted] due to the fact that the company's sole establishment is located in France. After dialogue between the CNIL and the European data protection authorities in the framework of the one-stop shop mechanism, they are all concerned by the processing, since user accounts have been created by residents of all European Union Member States.

10. In order to examine these items, the Commission Chair appointed Mr François Pellegrini as rapporteur on 21 October 2021, pursuant to article 22 of the amended law of 6 January 1978, and notified this to the organisation in a letter dated 26 October 2021.

11. On 2 December 2021, the rapporteur asked the organisation to provide its last three balance sheets, which the organisation did by letter dated 15 December 2021.

12. At the end of his investigation, on 16 February 2022, the rapporteur sent the organisation a report detailing the breaches of the GDPR that he considered to have occurred in this case, together with a summons to attend the meeting of the restricted committee on 21 April 2022. The letter notifying the report indicated to the organisation that it had one month to submit its written observations in response, in accordance with article 40 of decree no. 2019-536 of 29 May 2019 as amended.

13. This report proposed to the Restricted Committee of the Commission to impose an administrative fine, in view of the breaches of articles 5, paragraph 1, e) and 32 of the GDPR. It also proposed that this decision be made public and that the organisation no longer be identifiable by name upon expiry of a two-year period following its publication.

14. On 22 February 2022, the organisation requested an extension of the one-month deadline for submitting observations in response to the sanction report. On 25 February 2022, the Chair of the Restricted Committee granted this request and postponed the Restricted Committee's meeting.

15. On 15 April 2022, the organisation submitted its observations in response to the sanction report and asked for the Restricted Committee meeting to be held behind closed doors. This request was rejected by the Chair of the Restricted Committee, the organisation being notified by letter dated 21 April 2022.

16. The organisation and the rapporteur presented oral observations at the Restricted Committee meeting.

II. Reasons for the decision

17. In accordance with Article 60(3) of the GDPR, the draft decision adopted by the Restricted Committee was transmitted to all European data protection authorities on 19 July 2022.

18. On 16 August 2022, no supervisory authority had raised any relevant and reasoned objection to the draft decision and therefore, pursuant to Article 60(6) of the RGPD, they are deemed to have approved it.

A. <u>On the breach of the obligation to store data for a period proportionate to the purpose of the processing pursuant to article 5, paragraph 1, e) of the GDPR</u>

19. Article 5, paragraph 1, e) of the GDPR provides that personal data must be kept in a form which permits identification of individuals for no longer than is necessary for the purposes for which the personal data is processed.

20. In the course of the audit, the delegation noted that the "Confidentiality Charter" of the website "[redacted]fr" states that the personal data of members and subscribers are kept for 36 months from the last order for services and/or documents.

21. However, the organisation provided the CNIL delegation with a spreadsheet file showing that, as of 1 May 2021, it was storing the personal data of 946,023 members and 17,558 subscribers whose last order, last formality or last invoice for subscribers was more than 36 months ago, without the organisation being able to prove recent contact with said members or subscribers.

22. The rapporteur notes that no automatic deletion procedure for personal data was put in place by the organisation and that the data were kept for excessive periods of time relative to their purpose and the organisation's own policy.

23. In its defence, the organisation admits that personal data were kept for longer than the period indicated in its Charter, but contests the fact that the period indicated in this Charter should be taken as the only reference, whereas in view of other purposes, such as that relating to collection operations, it would be justified for certain data to be kept for a period longer than 36 months. As regards the anonymisation of personal data, the organisation admits that 25% of accounts were kept for more than 36 months after the last order, formality or invoice, without being anonymised. It also admits the delay in automating the anonymisation, but disputes that there was no anonymisation of accounts.

24. **Firstly**, the Restricted Committee notes that the purpose relating to collection operations, cited by the organisation, and the related retention period could in theory only concern the data of subscribers and not of members, the latter paying immediately in exchange for receiving a document. Moreover, the Restricted Committee noted that, for this purpose as for the accounting and tax purposes, the organisation had not identified these purposes and the corresponding periods of time in its Confidentiality Charter at the time of the audit. In any event, the Restricted Committee notes that while the retention of certain data for these purposes may appear justified, it requires different actions to be taken. As such, the Restricted Committee recalls that once the purpose of the processing has been achieved, the retention of certain data for compliance with legal obligations or for pre-litigation or litigation purposes is possible, but the data must then be placed in intermediate storage, for a period not exceeding that necessary for the purposes for which they are retained, in accordance with the provisions in force. Only relevant data should be placed in interim storage, either in a dedicated archive database or by making a logical separation within the active database, allowing only authorised persons to access it. The Restricted Committee notes that on the day of the audit, none of these actions had been implemented by the organisation.

25. **Secondly**, the Restricted Committee notes that the manual anonymisation implemented by the organisation at users' request only concerned a very small number of accounts, since on the day of the online audit, 25% of the accounts had not been anonymised even though they should have been. The Restricted Committee notes that no automatic anonymisation procedure was in

place at the time of the online audit, with the organisation retaining identifying data for an unlimited period of time in the absence of an anonymisation request from users.

26. Therefore, the Restricted Committee considers that the above facts constitute a structural breach of article 5, paragraph 1, e) of the GDPR.

27. The Restricted Committee notes that the organisation had indicated during the procedure that a purge of accounts that had been inactive for more than 36 months had been implemented since the audit, but notes that the breach was still evident with respect to the past.

B. <u>Breaches of the obligation to ensure the security of personal data (article 32 of the GDPR).</u>

28. Article 32 of the GDPR states that "*1. 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."

29. The rapporteur notes, firstly, that the delegation found that the passwords used by users to log in to their accounts, which can be accessed from the organisation's website, are not sufficiently robust in that they are limited to eight characters, without any complexity criteria, and are not associated with any additional security measures. Furthermore, the rapporteur notes that on the day of the findings, it was impossible for all users or subscribers of the website "[redacted]", i.e. for more than 3.7 million accounts, to enter a secure password because of the limitation of their size to a maximum of 8 characters.

30. Secondly, the rapporteur notes that the organisation sends non-temporary passwords for accessing accounts in clear text via email.

31. Thirdly, the rapporteur points out that the organisation also keeps passwords and secret questions and answers used during the password reset procedure by users in clear text in its database.

32. Lastly, the rapporteur notes that the organisation does not confirm to users that the password has been changed either. The rapporteur considers that users who are not alerted to unauthorised changes are therefore not protected against attempts to steal their account.

33. In light of these elements, the rapporteur considers that the various security measures put in place by the organisation are insufficient with respect to article 32 of the GDPR.

34. In its defence, the organisation argues that the security obligation is a best efforts obligation that must be assessed *concretely* and that its non-fulfilment must be established by a finding of

the ineffectiveness of the measures implemented, having led to unauthorised access, which is not the case in this instance. It stresses that the recommendation on passwords referred to by the rapporteur constitutes flexible law, that it is not a matter of mandatory rules, applicable from *an abstract* viewpoint, independently of any context, and whose non-compliance would, in itself, justify an administrative sanction. In addition, the organisation states that the data protection impact assessment revealed a low risk to personal data in the event of unauthorised access, since for member accounts, which represent the majority of accounts, bank data is not recorded, unlike for subscriber accounts, and an unauthorised third party will not be able to do anything other than purchase documents and send formalities instead of the account holder. Lastly, the organisation stresses that the information accessible by logging in to a user's account is essentially personal data present in the company registration certificate extracts and other documents that can be ordered, except in the case of accounts created by non-professionals whose identification and location data are not public.

35. First of all, the Restricted Committee recalls that, pursuant to article 32 of the GDPR, in order to ensure the protection of personal data, it is incumbent on the data controller to take "*appropriate technical and organisational measures to ensure a level of security appropriate to the risk*". The Restricted Committee considers that the use of a short or simple password without imposing specific categories of characters and without additional security measures can lead to attacks by unauthorised third parties, such as "brute force" or "dictionary" attacks, which consist of successively and systematically testing numerous passwords and therefore result in a compromise of the associated accounts and the personal data they contain. In this respect, it notes that the need for a strong password is recommended both by the *Agence Nationale de la Sécurité des Systèmes d'Information* (National Cybersecurity Agency of France - ANSSI) and by the Commission in its deliberation no. 2017-012 of 19 January 2017. In this case, the Restricted Committee notes that the passwords in question are limited to eight characters without any complexity criteria, and are not associated with any additional security measures. The Restricted Committee considers that the risk incurred by data subjects is real: a third party having had access to the password could not only access all of the personal data present in the data subject's account, but also view the history of their orders, download their invoices and/or change the account password and contact information without the user's knowledge.

36. Furthermore, the Restricted Committee considers that the methods of transmitting and storing passwords implemented by the organisation are not appropriate in view of the risk that the data subject would be exposed to if a third party were to capture their username and password. Indeed, the transmission, in clear text, of a password that is neither temporary nor for a single use and whose renewal is not made mandatory makes it easily and immediately usable by a third party, who would have undue access to the message containing it. The Restricted Committee recalls that a simple handling error can lead to the disclosure of personal data to unauthorised recipients and thereby breach individuals' privacy rights. Lastly, the Restricted Committee considers that a user who is not alerted in case of unauthorised modification is therefore not protected against attempts to steal their account.

37. Consequently, taking into account these risks for the protection of personal data and the privacy of individuals, the Restricted Committee considers that the measures deployed to guarantee data security in this case are insufficient.

38. Next, the Restricted Committee specifies that although deliberation no. 2017-012 of 19 January 2017, the CNIL guide on the security of personal data and the ANSSI technical note on passwords cited in the rapporteur's writings are certainly not imperative, they nevertheless set

out the basic security precautions corresponding to the state of the art. Consequently, the Restricted Committee recalls that it is considering a breach of the obligations arising from article 32 of the GDPR and not a failure to comply with the recommendations, which in any case provide relevant information for assessing the risks and the state of the art in terms of personal data security.

39. In addition to these recommendations, the Restricted Committee stresses that it has, on several occasions, adopted financial penalties where the characterisation of a breach of article 32 of the GDPR is the result of insufficient measures to ensure the security of the data processed, and not merely the result of the existence of a personal data breach. Deliberations no. SAN-2019-006 of 13 June 2019 and no. SAN-2019-007 of 18 July 2019 are aimed in particular at the insufficient robustness of passwords and their transmission to the organisation's customers by email, in clear text, after the account has been created.

40. In these circumstances, in view of the risks incurred by individuals, as recalled above, and the volume and nature of the personal data that may be contained in more than 3.7 million accounts (bank details of the subscriber accounts, last name, first name, postal and email address, landline and mobile telephone numbers, secret question and its answer of all of the accounts), the Restricted Committee considers that the organisation has failed to fulfil its obligations under article 32 of the GDPR.

41. The Restricted Committee notes that in the context of the present procedure, the organisation has taken certain measures to ensure the security of the data processed. Nevertheless, it considers that, since the implementation of its password policy in 2002 and until June 2021, the security measures put in place by the organisation did not enable it to ensure a sufficient level of security of the personal data processed and that, therefore, a failure to comply with the obligations of article 32 of the Regulation is established.

III. Regarding corrective powers and their publication

42. Under the terms of article 20(III) of the Act of 6 January 1978 amended:

"*When the data controller or its data processor fails to comply with the obligations resulting from Regulation (EU) 2016/679 of 27 April 2016 or this law, the chair of the CNIL may also, if applicable, after sending the warning provided for in point I of this article or, where applicable, in addition to an order provided for in II, contact the restricted committee of the Authority with a view to the announcement, after adversarial proceeding, 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 shall be increased, respectively, to 20 million euros and 4% of the said turnover. In determining the amount of the fine, the Restricted Committee shall take into account the criteria specified in the same article 83.*"

43. Article 83 of the GDPR further states that "*Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 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.

44. **Firstly**, with regard to the principle of imposing a fine, the organisation insists in its defence on the contractual responsibility of its data processor with regard to the instructions given to it concerning the security and anonymisation of personal data, on the prioritisation of other legal and regulatory projects in relation to its compliance with the GDPR, on its extensive cooperation with the CNIL and on the major efforts undertaken since the beginning of the audit.

45. 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 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 the categories of personal data concerned by the infringement.

46. The Restricted Committee considers firstly that although the organisation gave specific instructions on anonymisation and security to its data processor, it appears that it did not monitor the execution of these instructions and did not exercise satisfactory and regular control over the technical and organisational measures implemented by its data processor to ensure compliance with the GDPR and, in particular, to ensure the anonymisation and security of the personal data processed.

47. The Restricted Committee also considers that it is necessary to take into account the nature of the actor concerned, [redacted] In this respect, the Restricted Committee considers that the organisation should therefore have been particularly rigorous in complying with all of its legal and regulatory obligations. However, it appears from the debates that the organisation has postponed the implementation of the anonymisation and security of personal data projects in order to meet other compliance obligations not related to data protection, without increasing its available resources.

48. The Restricted Committee then notes that the breaches complained of were breaches of key principles of the GDPR that were not introduced by this text but pre-existed in the "French Data Protection Act". The Restricted Committee also emphasises that these breaches cannot be considered an isolated incident. With regard to the failure to comply with the retention period, the Restricted Committee recalls that the organisation had itself set a retention period for personal data that it had not complied with and that this breach concerns more than one million user accounts, both members and subscribers. With regard to the data security breach, the Restricted Committee considers that the extreme weakness of the password complexity rules, as well as the security measures concerning the communication, storage and renewal of passwords, in force since 2002, rendered all of the accounts vulnerable.

49. Lastly, the Restricted Committee notes that the compliance measures put in place following the notification of the sanction report do not concern all of the breaches and do not exonerate the company from its responsibility for the breaches observed.

50. Consequently, the Restricted Committee considers that an administrative fine should be imposed in view of the demonstrated breaches of articles 5, paragraph 1, e) and 32 of the GDPR.

51. **Secondly**, with regard to the amount of the fine, the organisation insists in its defence on the isolated nature of the complaint that gave rise to the audit and the absence of financial gain from the breaches.

52. The Restricted Committee notes that administrative fines must be both dissuasive and proportionate. It considers that the origin of the audit, which was carried out following a single complaint, does not minimise the severity of the breaches, which in any case proved to be structural. In the present case, the Restricted Committee notes, with regard to the breach concerning the personal data retention period, that the organisation has demonstrated serious negligence concerning a fundamental principle of the GDPR and that this breach concerns more than 25% of the accounts. With regard to the security breach, the Restricted Committee notes that given the accumulation of security deficiencies, the facts observed were particularly serious, especially as they rendered all of the accounts vulnerable. The Restricted Committee then recalls that the organisation had postponed compliance with the GDPR in favour of other legal and regulatory priorities. Lastly, the Restricted Committee takes into account the organisation's activity and its financial position. It also acknowledges the efforts made by the organisation to comply throughout this procedure.

53. In view of these elements, the Restricted Committee considers that the imposition of an administrative fine of €250,000 appears justified.

54. **Lastly**, with regard to the publicity of the penalty, the organisation maintains that such a measure would be disproportionate given the harm it would cause.

55. The Restricted Committee considers that the publicity of the sanction is justified in view of the severity of the breaches noted, the nature of the actor concerned which, given its size and activity, has the human, financial and technical resources to ensure a satisfactory level of protection of personal data and the strong reputation that the website enjoys with regard to commercial data.

FOR THESE REASONS

CNIL's Restricted Committee, after having deliberated, has decided to:

- **impose an administrative fine on the Economic Interest Group [redacted] in the amount of 250,000 (two hundred and fifty thousand) euros for the breaches of articles 5, paragraph 1, e) and 32 of the GDPR;**

- **make public, on the CNIL website and on the Légifrance website, its deliberation, which will no longer identify the organisation at the end of a period of two years following its publication.**

The Chair

Alexandre Linden

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