Deliberation SAN-2022-018 of September 8, 2022 National Commission for Computing and Liberties Nature of the deliberation: Sanction Legal status: In force Date of publication on Légifrance: Tuesday September 13, 2022 Deliberation of the restricted committee n° SAN-2022-018 of 8 September 2022 concerning the GIE INFOGREFFE The 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 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 relating to the protection of personal data and the free movement of such data; Having regard to Law No. 78-17 of 6 January 1978 relating to data processing, files and freedoms, in particular its articles 20 and following; Considering the decree n ° 2019-536 of May 29, 2019 modified 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; decision n° 2021-032C of January 6, 2021 of the President of the National Commission for Computing and Liberties to instruct the Secretary General to carry out or to have carried out a verification mission of any processing accessible from the site " infogreffe.fr" or relating to personal data collected from the latter; Having regard to the decision of the President of the National Commission for Computing and Liberties appointing a rapporteur before the restricted formation, dated October 21, 2021; Having regard to the report of Mr. François PELLEGRINI, commissioner rapporteur, notified to GIE INFOGREFFE on February 16, 2022; Having regard to the written observations submitted by GIE INFOGREFFE on April 15, 2022; 3 documents in the file; Were present, during the session of the restricted committee of May 12, 2022:- Mr François PELLEGRINI, commissioner, heard in his report; As representatives of the GIE INFOGREFFE:- […];- […] ;- […]. The GIE INFOGREFFE having had the floor last;The Restricted Committee adopted the following decision:I. Facts and procedure1. Infogreffe (hereinafter "the body" or "the group"), whose registered office is located at 5, avenue de Paris in Vincennes (94300), is an economic interest group (GIE) of commercial court registries de France, which since 1986 has been publishing the service for the dissemination of legal and official information on companies through several channels, in particular the website "infogreffe.fr" since 1996.2. The "infogreffe.fr" website allows you to consult legal information on companies and to order documents certified by the registries of the commercial courts. Users wishing to view or order a paid act on the website must have an account and are designated by Infogreffe as "members". It is also possible for users to take out an annual subscription, in particular allowing "subscribers" to access certain services in the business consultation section.

When creating an account, member or subscriber, the user must fill in the following mandatory fields: surname, first name, postal and electronic addresses, landline or mobile phone and choice of a secret question and its answer. Subscribers' bank details (IBAN and BIC) are also processed by Infogreffe.3. For the year 2019, the organization achieved a turnover of […] euros, for a net result of […] euros. In 2020, it achieved a turnover of […] euros, for a net profit of […] euros.4. On December 12, 2020, the National Commission for Computing and Liberties (hereinafter "the CNIL" or "the Commission") received a complaint against the organization, a person indicating that the "infogreffe.fr" website keeps users' passwords in plain text and that she was able to obtain her password by telephone by simply giving her name to the telephone helpline contact. 5. In application of decision n° 2021-032C of January 6, 2021 of the President of the CNIL, a control mission was carried out in order to verify the conformity of any processing accessible from the "infogreffe.fr" domain, or relating to personal data collected from the latter, to the provisions of law n ° 78-17 of January 6, 1978 modified relating to data processing, files and freedoms (hereinafter "the law of January 6, 1978 modified " or the " 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. Thus, an online check was carried out on March 4, 2021 on the "infogreffe.fr" site implemented by the group. The report n° 2021-032/1 drawn up at the end of the inspection was notified to the organization by registered mail, received on March 10, 2021.7. The CNIL delegation has in particular endeavored to check the procedure for transmitting user passwords when creating an account or in the event of forgetting or losing the password.8. By letters dated March 19, May 25 and June 24, 2021, the organization sent the CNIL the elements requested by the report n° 2021-032/1 and responded to its requests for additional information sent by email. on May 17 and June 18, 2021. The organization confirms in particular that it determines the purposes and methods of implementing the processing of personal data on the "infogreffe.fr" site. It also specifies the retention periods for the data it collects and the measures taken to ensure their security. Infogreffe also told the delegation that during the year 2020, the site was consulted by more than 24 million people worldwide and that, of the 3.7 million people with an account, more of 8,000 European accounts were not French.9. In accordance with Article 56 of the GDPR, the CNIL has informed all the European supervisory authorities of its competence to act as lead supervisory authority concerning the cross-border processing implemented by Infogreffe, resulting from the fact that the sole establishment of the grouping is in France. After discussion between the CNIL and the European data protection authorities within the framework of the one-stop-shop mechanism, these are all concerned by the processing since user accounts have been created by residents of all the Member States of the

Union. European.10. For the purpose of examining these elements, the President of the Commission, on October 21, 2021, appointed Mr François PELLEGRINI as rapporteur on the basis of Article 22 of the law of January 6, 1978 as amended, and informed organization by letter dated October 26, 2021.11. On December 2, 2021, the rapporteur asked the organization to provide its last three balance sheets, which the organization did by letter dated December 15, 2021.12. At the end of his investigation, the rapporteur, on February 16, 2022, had the organization notified of a report detailing the breaches of the GDPR that he considered constituted in this case, accompanied by a notice to attend the meeting of the restricted training of April 21, 2022. The letter notifying the report indicated to the organization that it had one month to submit its written observations in response, in accordance with Article 40 of Decree No. 2019- 536 of May 29, 2019 amended.13. This report proposed to the restricted formation of the Commission to impose an administrative fine with regard to the breaches of Articles 5, paragraph 1, e) and 32 of the GDPR. He also proposed that this decision be made public, but that it would no longer be possible to identify the organization by name after the expiry of a period of two years from its publication.14. On February 22, 2022, the organization requested an extension of the one-month deadline to produce observations in response to the sanction report. On February 25, 2022, the Chairman of the Restricted Committee granted this request and postponed the Restricted Committee meeting.15. On April 15, 2022, the organization produced its observations in response to the sanction report and requested the closed session of the restricted committee session. This request was rejected by the president of the restricted committee, the organization being notified by letter dated April 21, 2022.16. The organization and the rapporteur presented oral observations during the restricted committee session.II. Reasons for decision17. Pursuant to Article 60(3) of the GDPR, the draft decision adopted by the Restricted Committee was sent to all European data protection authorities on July 19, 2022.18. As of August 16, 2022, no supervisory authority had raised any relevant and reasoned objections to this draft decision, so that, pursuant to Article 60(6) of the GDPR, these are deemed to be having approved it.A. On the breach of the obligation to retain the data for a period proportionate to the purpose of the processing pursuant to Article 5, paragraph 1, e) of the GDPR19. According to Article 5, paragraph 1, e) of the GDPR, personal data must be kept in a form allowing the identification of the persons concerned for a period not exceeding that necessary in relation to the purposes for which they are kept. are processed.20. As part of the check, the delegation noted that the "Confidentiality Charter" of the "infogreffe.fr" website provides that the personal data of members and subscribers are kept for 36 months from the last service order and /or documents.21. However, the organization provided the CNIL delegation with a spreadsheet file from which it appears that on

May 1, 2021, it retained the personal data of 946,023 members and 17,558 subscribers, including the last order, the last formality or even the last invoice for subscribers, dated more than 36 months ago, without the organization being able to justify recent contact with said members or subscribers.22. The rapporteur notes that no procedure for the automatic deletion of personal data has been put in place by the organization and that the data were kept for excessive periods of time in relation to their purpose and the own policy set by the organization. .23. In defence, the organization admits that personal data have been kept longer than the duration indicated in its Charter but contests the fact that the duration indicated in this Charter is taken as the only reference whereas with regard to other purposes, such as those relating to recovery operations, it would be justified for certain data to be kept for a period of more than 36 months. With regard to the anonymization of personal data, the organization admits that 25% of accounts were kept for more than 36 months after the last order, formality or invoice, without being anonymized. He also admits the delay in automating the anonymization but contests the fact that there was no anonymization of the accounts.24. Firstly, the Restricted Committee notes that the purpose relating to recovery operations, cited by the organization, and the related retention period could a priori only concern the data of subscribers and not of members, the latter paying immediately in exchange receipt of a document. In addition, the Restricted Committee notes that, for this purpose as for accounting and tax purposes, the organization had not identified these purposes and the corresponding durations in its Confidentiality Charter on the date of the inspection. In any case, the Restricted Committee notes that while the retention of certain data for these purposes may appear justified, it requires that various actions be carried out. Thus, 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 archiving, to a duration not exceeding that necessary for the purposes for which they are kept, in accordance with the provisions in force. Only the relevant data must be placed in intermediate archiving, either in a dedicated archive database, or by performing a logical separation within the active database, allowing only authorized persons to access it. The Restricted Committee notes that on the day of the inspection, none of these actions had been implemented by the organisation.25. Secondly, the Restricted Committee notes that the manual anonymization implemented by the organization at the request of users only concerned a very small number of accounts since on the day of the online check, 25% of the accounts were not anonymized when they should have been. The Restricted Committee notes that no automatic anonymization procedure was implemented on the day of the online check, the organization thus retaining identifying data without time limit in the absence of

an anonymization request from the users.26. Therefore, the Restricted Committee considers that the aforementioned facts constitute a structural breach of Article 5, paragraph 1, e) of the GDPR.27. The Restricted Committee notes that the organization indicated, during the procedure, that a purge of accounts inactive for more than 36 months had been implemented since the audit, but retains that the breach remains characterized for the past.B. On breaches of the obligation to ensure the security of personal data (Article 32 GDPR).28. Article 32 of the GDPR provides that "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, the degree of likelihood and severity of which 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 among others, as required: a) pseudonymization and encryption personal data; b) the means to guarantee the constant confidentiality, integrity, availability and resilience of the processing systems and services; c) the means to restore the availability of the personal data and the access to them in a timely manner in the event of a physical or technical incident; d) a procedure aimed at regularly testing, analyzing and evaluating the effectiveness of the measures s technical and organizational measures to ensure the security of the processing. "29. The rapporteur notes, firstly, that the delegation found that the passwords for connecting users to their accounts, accessible from the organization's website, are insufficiently robust in that they are limited to eight characters, without any complexity criteria, and are not associated with any additional security measures. In addition, the rapporteur notes that on the day of the findings, it was impossible for all users or subscribers of the site web "infogreffe.fr", i.e. for more than 3.7 million accounts, to enter a secure password due to the limitation of their size to a maximum of 8 characters.30 The rapporteur notes, secondly, that the organization sends non-temporary passwords allowing access to accounts in plain text by e-mail. secret questions and answers used during the procedure for resetting passwords by users.32. Finally, the rapporteur notes that the organization does not confirm to the user the modification of his password either. The rapporteur considers that the user who is not alerted in the event of an unauthorized modification is therefore not protected against attempts to usurp his account.33. In view of these elements, the rapporteur considers that the various security measures put in place by the organization are insufficient with regard to Article 32 of the GDPR.34. In defence, the organization argues that the security obligation is an obligation of means which must be assessed in concrete terms and that its non-performance must be established by a finding of the ineffectiveness of the measures implemented, having led to access unauthorized, which is not the case here. He stresses that the recommendation relating to passwords mentioned by

the rapporteur constitutes flexible law, that it is not a question of mandatory rules, applicable in abstracto, independently of any context and non-compliance with which would, in itself, even, such as to justify an administrative sanction. In addition, the organization specifies that the impact analysis relating to data protection revealed a low risk for personal data in the event of unauthorized access since for member accounts, representing the majority of accounts, bank details are not recorded, unlike subscriber accounts and an unauthorized third party will not be able to take any action other than the purchase of documents and the sending of formalities in place of the account holder. Finally, the organization emphasizes that the information accessible by logging into a user's account is essentially personal data present in the K or KBIS extracts and the other acts that can be ordered, except for the 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, to ensure the protection of personal data, it is the responsibility of the data controller to take "appropriate technical and organizational measures in order to guarantee 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 unauthorized third parties, such as "brute force" attacks " or " by dictionary ", which consist in successively and systematically testing many passwords and thus lead to a compromise of the associated accounts and the personal data they contain. It notes, in this respect, that the need for a strong password is recommended both by the National Agency for the Security of Information Systems (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 criterion, and are not associated with any additional security measure. The Restricted Committee considers that the risk run by the persons concerned is real: a third party having had access to the password could not only access all the personal data present in the account of the person concerned, but also consult the history of its orders, download its invoices and/or change the password of the account and the contact information without the knowledge of the user.36. In addition, the Restricted Committee considers that the procedures for the transmission and storage of passwords implemented by the organization are not appropriate with regard to the risk that the capture of their identifier and password would pose to the person concerned. goes through a third party. Indeed, the transmission, in plain text, of a password which is neither temporary nor for single use and whose renewal is not imposed, makes it easily and immediately usable by a third party who would have improper access. to the message that contains it. The Restricted Committee recalls that a simple handling error can lead to the disclosure of

personal data to unauthorized recipients and thus infringe the right to privacy of individuals. Finally, the Restricted Committee considers that the user who is not alerted in the event of an unauthorized modification is therefore not protected against attempts to usurp his account.37. Therefore, taking into account these risks for the protection of personal data and the privacy of individuals leads the Restricted Committee to consider that the measures deployed to guarantee data security in this case are insufficient.38. Next, the Restricted Committee specifies that if deliberation no. 2017-012 of January 19, 2017, the CNIL guide relating to the security of personal data and the ANSSI technical note relating to the passwords cited in the The rapporteur's writings are certainly not mandatory, but they do outline the basic safety precautions corresponding to the state of the art. Therefore, the Restricted Committee recalls that it retains a breach of the obligations arising from Article 32 of the GDPR and not the non-compliance with the recommendations, which moreover constitute relevant insight for assessing the risks and the state of the art in personal data security.39. In addition to these recommendations, the Restricted Committee points out that it has, on several occasions, adopted pecuniary sanctions where the characterization of a breach of Article 32 of the GDPR is the result of insufficient measures to guarantee the security of the data processed, and not just the result of the existence of a personal data breach. Deliberations No. SAN-2019-006 of June 13, 2019 and No. SAN-2019-007 of July 18, 2019 relate in particular to the insufficient robustness of passwords as well as their transmission to the organization's customers by email, in plain text. , after the creation of the account.40. Under these conditions, in view of the risks incurred by individuals, mentioned above, as well as the volume and nature of the personal data which may be contained in more than 3.7 million accounts (banking data of accounts subscribers, surname, first name, postal and electronic address, landline or mobile telephone numbers, secret question and its answer for all the accounts), the Restricted Committee considers that the organization has breached its obligations under the Article 32 of the GDPR.41. The Restricted Committee notes that in the context of this procedure, the organization 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 organization did not allow it to ensure a level of sufficient security of the personal data processed and that, therefore, a breach of the obligations of Article 32 of the Regulation has been constituted.III. On corrective measures and their publicity42. Under the terms of III of article 20 of the modified 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 from 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. "43. 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.44 Firstly, on the principle of imposing a fine, the organization insists in defense on the contractual responsibility of its subcontractor with regard to the instructions which had been given to him concerning the security and anonymization of personal data, on the prioritization of other legal and regulatory projects in relation to his compliance with the GDPR, on his important coo operation with the CNIL and the major efforts made since the beginning of the control.45. 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 number of people affected , the measures taken by the controller to mitigate the damage suffered by data subjects, whether the breach was negligent, the degree of cooperation with the supervisory authority and the categories of personal data concerned by violation.46. The Restricted Committee first considers that although the organization gave specific instructions on anonymization and security to its subcontractor, it appears that it did not follow the execution of these instructions and has not exercised satisfactory and regular control over the technical and organizational measures implemented by its subcontractor to ensure compliance with the GDPR and, in particular, to ensure the anonymization and security of the personal data processed.47. The Restricted Committee also considers that the nature of the actor concerned should be taken into account, bringing together the clerks of the commercial courts, who are public and ministerial officers responsible for carrying out public service missions. As such, the Restricted Committee considers that the organization should therefore have shown particular rigor in respecting all of its legal and regulatory obligations. However, it results from the debates that the organization has postponed the implementation of projects

relating to the anonymization and security of personal data in order to respond, without increasing its available resources, to other obligations of compliance which were not related to data protection.48. The Restricted Committee then notes that the alleged breaches are breaches of key principles of the GDPR which were not introduced by this text but pre-existed in the "Informatique et Libertés" law. The Restricted Committee also stresses that these shortcomings cannot be regarded as an isolated incident. With regard to the breach relating to the retention period, the Restricted Committee recalls that the organization had itself set a retention period for personal data which it did not respect and that this breach concerns more than one million user, member and subscriber accounts. With regard to the breach relating to data security, the Restricted Committee considers that the extreme weakness of the password complexity rules, as well as the security measures for the communication, storage and renewal of passwords, in force since 2002, made all the accounts vulnerable.49. Finally, the Restricted Committee notes that the compliance measures put in place following notification of the sanction report do not exonerate the organization from its liability for the breaches observed.50. Consequently, the Restricted Committee considers that an administrative fine should be imposed with regard to the breaches constituted in Articles 5, paragraph 1, e) and 32 of the GDPR.51. Secondly, with regard to the amount of the fine, the organization insists in defense on the isolated nature of the complaint at the origin of the control and the absence of financial gain derived from the breaches.52. The Restricted Committee recalls that administrative fines must be both dissuasive and proportionate. It considers that the origin of the control, which took place following a single complaint, cannot minimize the seriousness of the shortcomings which, moreover, turned out to be structural. In this case, the Restricted Committee finds, with regard to the breach relating to the retention period of personal data, that the organization has shown gross negligence relating to a fundamental principle of the GDPR and that this breach concerns more 25% of accounts. With regard to the breach relating to security, the Restricted Committee notes that given the accumulation of security flaws, the facts observed are particularly serious, especially since they have reported all the accounts vulnerable. The Restricted Committee then recalls that the organization has postponed its compliance with the GDPR in favor of other legal and regulatory priorities. Finally, the restricted training takes into account the activity of the organization and its financial situation. It also records the efforts made by the organization to comply throughout this procedure.53. In view of these elements, the Restricted Committee considers that the imposition of an administrative fine of two hundred and fifty thousand euros appears justified.54. Lastly, with regard to the publicity of the sanction, the organization maintains that such a measure would be disproportionate in view of the harm it would cause.55. The Restricted

Committee considers that the publicity of the sanction is justified with regard to the seriousness of the breaches identified, the nature of the actor concerned who, given its size and activity, has the human, financial and technical resources to enable it to ensure a satisfactory level of protection of personal data and the strong reputation enjoyed by the website in terms of commercial data. against GIE INFOGREFFE an administrative fine of 250,000 (two hundred and fifty thousand) euros for breaches of Articles 5, paragraph 1, e) and 32 of the GDPR; make public, on the website of the CNIL and on the Légifrance site, its deliberation, which will no longer identify the organization by name at the end of a period of two years from its publication. The president Alexandre LINDEN This decision is likely to fa appeal to the Council of State within two months of its notification.