CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

The Chair

[redacted]
THE MANAGER
[redacted]
[redacted]

Paris, on 15 June 2023

Our Ref. : [redacted]
To be quoted in all correspondence
Registered letter with proof of posting no. [redacted]

Dear Sir,

[redacted] is a creator of professional social networks specialising in the recruitment of finance professions (website "[redacted]") and new technologies (website [redacted]). Among other services, these networks enable members to publish their professional profiles online for recruiters.

On 2 June 2022, in accordance with Decision No. [redacted], the Commission Nationale de l'Informatique et des Libertés (CNIL, "French Data Protection Authority") carried out an online inspection of the websites accessible at the URLs [redacted] and [redacted] published by [redacted]. This inspection continued with an inspection at the company's premises on 22 June 2022.

The purpose of this inspection was to verify the compliance of the processing carried out by your company with the provisions of Regulation (EU) 2016/679 on data protection (GDPR) and Law No. 78-17 of 6 January 1978 as amended ("Data Protection Act"). This was specifically in response to to several complaints referred to the CNIL data protection authority concerning the exercise of the rights of members of the [redacted] and [redacted] sites.

The findings from these inspections, and the additional findings on 21 July 2022, **prompt me to issue the following observations:**

I. Analysis of the facts in question

1. <u>On the breach of the obligation to provide transparent information</u>

In law, Article 12 of the GDPR provides that *"The data controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 [...] to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language*".

Article 13 of the GDPR requires the data controller to provide the data subject with various information, in particular concerning its identity and 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 regulation requires, where necessary to ensure *"fair and transparent processing"* of personal data, that individuals are informed 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.

In this case,with regard to the [redacted] website, the delegation found that the registration form contains a link to the General Terms and Conditions. I observe that these General Terms and Conditions contain a "Personal Data" paragraph, the content of which does not specify all the mandatory information provided for in Article 13 of the GDPR (no mention of the identity of the data controller, the legal basis for processing or the recipients of the data). In addition, information on the duration of data retention, the rights to portability and the right to lodge a complaint with a supervisory authority is also not supplied to data subjects.

The delegation also noted the presence of a "legal information" section containing information on personal data which is incomplete and obsolete (reference to Article 34 of the French Data Protection Act).

Informal post-audit checks revealed that [redacted] has now made a "Privacy Policy" accessible online in the site footer and from the registration form. Overall, this includes all the information required in Article 13, but remains imprecise as to the identity of the data controller and the retention periods. The "legal notices" section and the "personal data" section of the T&Cs were unchanged.

Finally, with regard to **the [redacted] website**, the delegation found that the registration form contains a link to the Privacy Policy which remains incomplete on the identity of the data controller and the retention periods.

In conclusion, with regard to the [redacted] website, the presence in the T&Cs and the "Legal Notices" of incomplete and obsolete information relating to data protection does not meet the transparency requirements set out in the GDPR.

Furthermore, with regard to the Privacy Policy put on line on the [redacted] and [redacted] websites, Article 13 of the GDPR requires the data controller to provide, at the time the data is collected, information relating to its identity. In addition, information on the retention period of the data is not sufficiently explicit. These periods are, however, necessary to enable the data subject to exercise his/her rights before the data is deleted.

It is therefore my view that [redacted] disregarded the provisions of Articles 12 and 13 of the GDPR by not providing all the information provided for in Article 13 of the GDPR to data subjects in an easily accessible, concise and comprehensible manner.

2. Regarding the breach of the obligation to specify and comply with a personal data retention period in proportion to the purpose of the processing

Article 5.1.e of the GDPR provides that "*Personal data shall 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 [...]*".

With regard to the specific case of the retention of data related to a user account created on a website, they may in principle be kept until the account is deleted. However, it is common for users to no longer use these accounts without deleting them, which means that they persist indefinitely. In this case, the principle of limited retention of personal data requires the controller to determine a reasonable period of time at the end of which, if the account has not been the subject of any activity on the part of the user, it must be considered as inactive and must be deleted, along with the personal data related to it.

In this respect, the CNIL considers, in its reference framework relating to personal data implemented for the purposes of managing commercial activities, that a period of two years is proportionate. Recommended practice is to notify the users concerned before deleting the accounts of those who have not reacted within the time limit set by the organisation.

2.1 on the breach of the obligation to specify a data retention period for members of the [redacted] website

In this case, the delegation was informed that members' data have been kept for an unlimited period since the implementation of the site in 2009. They are kept for as long as the member is registered. In addition, data from deleted accounts are neither anonymised nor deleted from the database. The delegation noted the presence of 111,875 accounts with the status "deleted" and 337,720 accounts that had not logged in for more than 3 years.

With regard to the retention of data from deleted accounts, such a retention does not seem justified with regard to the purpose of the processing; namely, the management of members' accounts registered free of charge on the website.

In addition, the data controller has not specified any period of inactivity of the account that would trigger a data deletion procedure; a period of three years would, as an initial analysis, appear to be the maximum permissible.

It is therefore my view that, for these two reasons, [redacted] disregarded the provisions of Article 5.1(e) of the GDPR.

2.2 On the breach of the obligation to comply with a proportionate data retention period on the [redacted] website

In this case, the delegation was informed that the data from site users' accounts have been collected since November 2021. It was specified that in the event that a member requests deletion of his/her account, his/her data is kept for a period of 3 years and, at the end of this period, the data is subject to an anonymisation process. The data are then replaced by empty text chains.

It emerges from the case information that the company has been unable to state the purpose justifying the retention of all the data related to the accounts after their deletion. It therefore appears that the retention for a period of 3 years of all the data of users who requested that their accounts be deleted does not seem appropriate, and exceeds the duration necessary for the purposes for which they are processed. Unless their retention can be justified in order to meet a legal obligation or evidential purposes, such retention, as for the data of the deleted accounts of [redacted] members, does not seem to be justified with regard to the purpose of [redacted] processing.

It is therefore the view of the sub-commission that the company breached the provisions of Article 5.1 of the Regulation.

3. <u>Concerning the obligation to respect the right to erasure</u>

In law, Article 17-1-c) of the GDPR states, *"The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where [...] the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing*".

Article 12.3 of the GDPR further states that "*The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request*". *If necessary, this period may be extended by two months, taking into account the complexity and number of requests. The controller shall inform the data subject of this extension and the reasons for the postponement within one month of receipt of the request. Where the data subject submits his or her request in electronic form, the information shall be provided electronically where possible, unless the data subject requests otherwise.*"

In this case, with regard to complaints nos. [redacted] received by the CNIL, the delegation found, during the online inspection in June 2022, that the professional profiles of the complainants were still online on the website [redacted] despite their request to delete data concerning them with your company made on [redacted].

Post-audit checks revealed that complainants' requests for erasure had been satisfied and that their professional profile was no longer available on the [redacted] site.

Furthermore, with regard to referral No. [redacted], the complainant referred the matter to the CNIL due to difficulties in obtaining the deletion of their data following their registration on the [redacted] website. The delegation found that the company had received the complainant's request for erasure and that it was unable to provide the delegation with the response to it. The delegation also found that the complainant's data had been erased.

It is my view that [redacted] disregarded the provisions of Article 17 of the GDPR by failing to comply with requests to erase data from data subjects within the required deadlines. It is also my view that [redacted] disregarded the provisions of Article 12.3 of the GDPR by not informing the data subject of the measures taken following their request for erasure.

However, I note the erasure of the complainants' data, which puts an end to the breach arising from Article 17 of the GDPR.

4. Regarding the breach of processing obligations

In law, Article 28 of the GDPR provides that "*Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.*" Article 28.3 details the clauses to be included in the contract.

In this case, the delegation found that no data protection clause governs the subcontracting relationship between [redacted] and [redacted] responsible for the development and maintenance of the [redacted] website.

It is therefore my view that [redacted] breached the provisions of Article 28 of the GDPR.

5. On the failure to implement a register of processing activities

In law, Articles 30.1 of the GDPR require the data controller to keep a record of the processing activities carried out under their responsibility.

An exception is provided in Article 30-5 for organisations *"employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes [data referred to in Articles 9 and 10 of that legislation]."*

In this case, during the online inspection, the delegation noted that it was necessary to create an account on the [redacted] and [redacted] websites in order to benefit from [redacted]'s services. The creation and management of such accounts leads to the implementation of non-occasional processing of personal data. A record was therefore mandatory.

[redacted], from whom a record of processing activities was requested and which is responsible for such processing, informed the delegation that it did not keep such a record.

It is therefore my view that [redacted] breached the provisions of Article 30 of the GDPR.

6. Regarding the breach of the obligation to ensure the security and confidentiality of personal data

In law, Article 32 of the GDPR imposes the following requirement on the data controller, *"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, [to] implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk."* It follows from these provisions that the data controller is required to ensure that the automated processing of data that 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. The implementation of a robust authentication policy constitutes a basic security measure which generally contributes to compliance with the obligations of Article 32 of the GDPR.

In its deliberation no. 2022-100 of 21 July 2022 adopting a recommendation on passwords and other shared secrets – which is certainly not imperative but which provides relevant insight on the security measures to be taken – the Commission recommends that, in order to ensure a sufficient level of security and confidentiality, in the event that authentication is based solely on a username and password, the latter should be composed of at least 12 characters including uppercase letters, lower case numbers, numbers and special characters to be chosen from a list of at least 37 special characters possible, or composed of at least 14 characters including uppercase letters, lower case numbers and numbers, without any mandatory special character, or, when it corresponds to a phrase based on words in the French language, or composed of at least 7 words.

Failing this, the Commission considers that authentication based on a minimum length of 8 characters, consisting of 3 different categories of characters but accompanied by an additional measure such as, for example, a temporary ban on access to the account after several failures, the duration of which increases with each attempt, the implementation of a mechanism to protect against automated and intensive submission of attempts, also makes it possible to ensure a sufficient level of security and confidentiality (e.g.: "captcha") or locking the account after several unsuccessful authentication attempts (maximum 10);

In the present case, the Delegation noted that the password policy implemented for access to controlled sites does not require a minimum size or a certain level of complexity for the password in terms of account creation or reset. It follows from the above that more restrictive security measures should be adopted with regard to access to the accounts of your websites in order to prevent any access to data by unauthorised third parties; for example, by imposing sufficient complexity of passwords, as recommended by the Commission. It is therefore my view that [redacted] disregarded the provisions of Article 32 of the GDPR on this point.

Furthermore, in law, it also follows from Article 32 of the GDPR that the data controller must store users' passwords in a sufficiently secure manner, in order to avoid their compromise and to protect personal data that can be viewed and collected by accessing the accounts.

In the current state of the art, the Commission has established specific recommendations in its guide for developers[1], recommending storing passwords "in the form of a hash using a proven library, such as Argon2, yescrypt, scrypt, balloon, bcrypt and, to a lesser extent, PBKDF2." The SHA-1 algorithm, by contrast, is a hash function containing a vulnerability that is known to and immediately usable by attackers (risk of collision). It therefore does not guarantee the security of the data concerned.

In this case, the delegation was also informed that user account passwords are stored with the SHA1 hash function.

It follows from the above that the storage of passwords in the database of your website is therefore not in accordance with the state of the art as of the date of this decision. It is therefore your responsibility to store passwords using a proven hash algorithm, such as those listed in the Commission developer's guide.

It is therefore my view that [redacted] disregarded the provisions of Article 32 of the GDPR on this point.

7. <u>On the breach of the obligation to comply with the provisions of Article L.34-5 of the French Postal and Electronic Communications Code (CPCE)</u>

In law, Article L. 34-5 of the CPCE provides that "*direct prospecting by means of an automatic calling, fax or email system using, in any form whatsoever, the contact information of a natural person who has not expressed his or her prior consent to receiving direct prospecting by that means, is prohibited.*

For the application of the present article, consent shall mean any expression of free, specific and informed intent whereby a person agrees that personal data related to them is used for direct marketing purposes.

Direct marketing is the sending of any message intended to promote, directly or indirectly, goods, services or the image of a person selling goods or providing services.

However, direct e-mail marketing is authorised if the recipient's contact details have been collected directly from them, in compliance with the provisions of Data Protection Law No. 78-17 of 6 January 1978, in connection with a sale or provision of services, if the direct marketing concerns products or services similar to those previously provided by the same natural person or legal entity, and if the recipient is offered, expressly and unambiguously, the opportunity to object, without charges, other than those related to the transmission of the refusal, in a simple manner, to the use of his/her contact details

---

[1] CNIL. *Guide RGPD de l'équipe de développement*, v2, 13 December 2021, sheet 6, https://linenil.github.io/Guide-RGPD-du-developpeur/

at the time they are collected and every time a marketing e-mail is sent to them if they have not initially refused such use."

In this case, the delegation noted, on the registration form of the [redacted] website, the following statement: *"I would like to receive offers from [redacted] partners"* preceded by a pre-checked box. It was specified that these offers are sent by [redacted] on behalf of its partners, and not for itself. These offers include job offers, recruitment events and articles relating to the partner's news, such as an employee's career.

The delegation noted that offers from partners were not only job offers. For example, an email communication may contain a presentation of [redacted]'s employee savings solutions.

It follows from the provisions of Article L. 34-5 that such marketing emails are subject to recipients' consent. In this respect, it is specified that the company cannot avail itself of the exemption from consent provided for in paragraph 4 of Article L.34-5 insofar as the latter only concerns prospecting for similar goods and services provided by the same natural or legal person, and not by third-party companies.

It is therefore my view that [redacted] disregarded the provisions of Article L.34-5 of the CPCE by not first obtaining the consent of the persons concerned to send offers from its partners by email.

II. Corrective action specified by CNIL (Article 20.II of the French Data Protection Act of 6 January 1978)

In light of all of the above, and in agreement with the other data protection authorities concerned by this processing, the following corrective measures must therefore be imposed against [redacted]:

- **A LEGAL REPRIMAND,** in accordance with the provisions of Article 20.II of the French Data Protection Act of 6 January 1978, with regard to the obligation to respond to requests to exercise the rights of persons within the required time limits.
- **AN ORDER** in accordance with the provisions of Article 20.II of the French Data Protection Act of 6 January 1978, within a period **of three (3) months from the notification of this decision and subject to any measures it may have already adopted:**

  - **to inform data subjects**, in accordance with the provisions of Articles 12 and 13 of the GDPR, by providing them with complete, concise, transparent, understandable and easily accessible information, in particular by expanding the Privacy Policy of the [redacted] and [redacted] websites and the data protection notices in the T&C and the legal notices of the [redacted] website; for example, by making reference to the Privacy Policy;

  - **to define and implement a data retention period policy** which does not exceed the period necessary for the purposes for which they are collected, in particular for the account data of inactive users; to delete all the account data of users who have made such a request, as well as data from inactive accounts, unless it can justify the retention of said data in order to meet a legal obligation or probative purposes;

  - **to ensure that a contract that meets the requirements of Article 28** of the GDPR is binding on [redacted] and its subcontractor, [redacted];

  - **to keep a register of the processing activities** carried out under its responsibility, which includes all the information mentioned in Article 30.1 of the GDPR;

- **to take all security measures**, for all personal data processing operations, to preserve the security of such data and prevent unauthorised third parties from accessing it, in line with the provisions of Article 32 of the GDPR, and in particular by:
    - establishing a binding policy on passwords used by users of the site, in particular in terms of complexity for creating an account or renewing a password for existing accounts;
    - storing the passwords of users of the sites securely and in accordance with the state of the art, including by transforming them using a specialised, non-reversible and secure cryptographic function;
- **to obtain free, specific and informed consent** from members of the website [redacted] to the use of their contact details for direct electronic marketing purposes, by ensuring, for example, that the box preceding the words "*I would like to receive offers from* [redacted] *partners*" is unchecked.

This formal notice, which does not require a response from you, signals the closure of procedure [redacted]. However, this closure takes place without prejudice to the right of the Commission to carry out a fresh verification procedure in order to check that your company has complied with this formal notice at the end of the time limit.

In the event of a fresh verification procedure, if your company has not complied with this formal order, a rapporteur will be appointed who may request that the restricted committee to issue one of the sanctions provided for by Article 20.of the French Data Protection Act of 6 January 1978.

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

For more information on the formal notice procedure, you can consult the CNIL website at the following page: https://www.cnil.fr/fr/la-procedure-de-mise-en-demeure-0.

The Commission staff – [redacted] and [redacted] – are at your staff's disposal for any additional information.

Yours sincerely,

Marie-Laure DENIS