The President

[redacted]

Paris, Click here to enter a date.

[redacted]

Madam Chair,

[redacted] main business is software publishing. In particular, it develops and publishes the mobile dating app '[redacted] designed to connect people who are geographically close to one another, available on the Android and iOS app stores.

In accordance with my decision No· 2024-098C of 27 March 2024, a delegation from the French Data Protection Authority (hereinafter "the CNIL" or "the Authority") carried out an inspection on 7 May 2024 at the premises of [redacted] located at [redacted]

The purpose of this inspection was to verify compliance by the company [redacted], located [redacted], the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter the 'GDPR') and Law No° 78-17 of 6 January 1978 on data processing, files and freedoms.

This inspection formed part of a *coordinated enforcement framework* by the European Data Protection Board (EDPB), which decided in 2024 to verify the conditions under which public and private bodies manage the exercise of data subjects' right of access.

The findings made during the inspections, together with the additional information provided by the company on 23 May 2024, lead me to note the following facts.

I. Analysis of the facts in question

1. Regarding the breach of the obligation to collect data that is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed

In law, Article 5(1)(c) of the GDPR provides that personal data must be *'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation)*'.

Article 12(6) of the GDPR provides that *'where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of further information necessary to confirm the identity of the data subject*.'

Guidelines 01/2022 on the rights of data subjects – Right of access, paragraphs 70 to 78, specify that the controller must carry out a proportionality assessment when requesting additional information to confirm the identity of the data subject. In particular, paragraph 74 states *that '*it *should be emphasised that the use of a copy of an identity document as part of the authentication process creates a risk to the security of personal data and may lead to unauthorised or unlawful processing and, as such, should be considered inappropriate, unless it is necessary, appropriate and in accordance with national law[.] It is also important to note that authentication by means of an identity card is not necessarily useful in an online context (for example, where pseudonyms are used) if the data subject cannot provide any other evidence, such as other characteristics corresponding to the user account."* Furthermore, paragraph 77 states that *'to comply with the principle of data minimisation, the controller should inform the data subject of the information that is not necessary and of the possibility of obscuring or masking those parts of the identity document'.*

In this case, during the on-site inspection, the delegation was informed that when a user exercises their right of access via the contact form on the mobile app, their request is automatically linked to their account on the '[redacted] app, and no verification is carried out. In other cases, your company asks the data subject for their identity document to authenticate them. The identity document is used to verify the person's photograph and date of birth. If a person provides their [redacted] ID, which is visible on the app's interface, your company considers them to be sufficiently identified.

However, the systematic provision of an identity card does not appear necessary insofar as other elements, such as a unique identifier linked to the data subject's account, are sufficient to identify them. Furthermore, your company requests a photograph of the identity document, without specifying whether certain details may be obscured. A photograph of the identity document contains information that is not necessary to confirm the identity of the data subject. For example, [redacted] does not mandatorily collect the surname, so it is not necessarily useful for the data subject to provide a photograph of their identity card containing their surname if this data is not in [redacted] possession.

Consequently, the systematic request for a photograph of the identity card, without specifying the possibility of obscuring certain details, in order to identify the data subject is not proportionate to the purpose.

I therefore consider that [redacted] has failed to comply with the provisions of Article 5(1)(c) and Article 12(6).

These facts justify issuing a formal notice to [redacted] requiring it to propose alternatives to identification by means of an identity document for requests to exercise rights made by individuals who are not logged into their accounts, and to comply with the principle of data minimisation when identification is carried out by means of an identity document.

2. **<u>Regarding the failure to define and comply with a retention period proportionate to the purpose of the processing</u>**

In law, 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*'.

Guidelines 01/2022 on the rights of data subjects - Right of access, paragraphs 79, specify that the EDPS recommends *"as a matter of good practice, that the controller, after verifying the identity card, make a note, stating for example 'the identity card has been verified' in order to avoid the unnecessary copying or storage of copies of identity cards".*

In this case, [redacted] has set a retention period of two years for correspondence relating to requests to exercise rights.

[redacted] retains correspondence relating to requests in the [redacted] tool and maintains a register of requests for the right of access. The delegation noted the presence, within the [redacted] customer management tool, of requests to exercise rights dating from 2020, some of which included copies of identity documents still visible alongside the requests for the purpose of identifying the individual.

On the one hand, the company is not complying with the two-year retention period it has set for requests to exercise rights under the GDPR, in particular requests for the right of access, which leads it to retain data related to these requests for a period exceeding that which is necessary in view of the purpose pursued.

Furthermore, as the CNIL's restricted panel has already noted[1] , where identity documents are collected for the purpose of identifying the person making the request to exercise a right, they need not be retained once identification has been established.

I therefore consider that [redacted] has failed to comply with the provisions of Article 5(1)(e) by retaining data for periods exceeding the purposes for which it was collected.

These facts justify issuing a formal notice to [redacted] firstly, to delete requests for access rights and the supporting documents provided that have been retained beyond the period necessary for the defined purposes, and, secondly, to ensure in future that such requests and their supporting documents are retained only for the period necessary for the defined purposes.

3. **<u>Regarding the breach of the obligation of transparency and information to data subjects</u>**

[1] CNIL, France, 18 November 2020, penalty, Decision SAN-2020-008 of 18 November 2020, published.

In law, Articles 12 to 14 of the GDPR set out the requirements incumbent on data controllers regarding the provision of information to data subjects concerning the processing of their data and the procedures for data subjects to exercise their rights.

Article 12(1) states that *'the controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and to make any communication pursuant to Articles 15 to 22 and Article 34 regarding the processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information specifically intended for a child ".*

Article 12(2) states that *'the controller shall facilitate the exercise of the rights conferred on the data subject under Articles 15 to 22'.*

Article 12(6) of the GDPR provides that *'where the controller has reasonable doubts concerning the identity of the natural person making the request referred to in Articles 15 to 21, the controller may request the provision of further information necessary to confirm the identity of the data subject.'*

Guideline 01/2022 on the rights of data subjects – Right of access reiterates the general structure of the right of access, specifying**:**
'The right of access comprises three elements:

- *confirmation as to whether or not data relating to the individual is being processed;*
- *access to such personal data; and*
- *access to information about the processing, such as the purpose, categories of data and recipients, the duration of processing, the rights of data subjects and in the event of a transfer to third countries."*

Guideline 01/2022 on the rights of data subjects – Right of access, paragraph 142, specifies that**:** *"The concept of 'easily accessible' means that the information referred to in Article 15 should be presented in a manner that is easily accessible to the data subject. This includes, for example, the layout, the use of appropriate headings and the division into paragraphs. The information should always be expressed in a simple and clear manner. A controller offering a service in a country should also provide responses in a language understood by data subjects in that country."*

a) On information regarding the procedures for exercising the right of access

In this case, when a person logged into their account in the app clicks on their profile, then on 'Settings', then on 'My data', then on 'Access my data', they are taken to a page stating*: "To access your data, simply send an access request by email to* [redacted]*, accompanied by proof of identity [...]*".

This wording is misleading in that it suggests that proof of identity must always accompany the request and, in any event, encourages the data subject to provide proof of identity. This wording contradicts the process actually implemented by the company, whereby, when the user makes their request via the app whilst logged in, they are not asked for additional proof of identity.

The privacy policy, however, specifies that when exercising rights, proof of identity may be requested if there is any doubt as to the identity of the applicant.

Thus, the information on the procedures for exercising the right of access regarding the identification of the person making the request is unclear and varies depending on the source of information.

I therefore consider that [redacted] has failed to comply with the provisions of Article 12(1), (2) and (6) by providing contradictory information regarding the need to provide proof of identity in order to exercise the right of access.

These facts justify issuing a formal notice to [redacted] to clarify the information regarding the provision of proof of identity when exercising this right.

b) Regarding the information provided in response to the right of access

In this case, the delegation noted the presence of a document entitled *'Summary Information on personal data'* attached to some of the responses to requests to exercise the right of access. This document is written in English and contains information on the data collected, the sources of the data, the purposes of processing, the recipients of the data and the retention periods. This document therefore appears to correspond to the information to be provided under Article 15(1) of the GDPR.

When your company responds to a request for data disclosure under the right of access, it provides the data in the form of an encrypted archive. A summary of the information is provided in the form of an HTML file, and the raw data is also available in the form of JSON files.

The encrypted archive is sent by email to the data subject who made the request. That person receives a second email containing a link to a page with the password to decrypt the archive. The password is visible for only thirty days. Both of these emails are in English, regardless of the language used by the data subject in their request. However, correspondence prior to the sending of the data takes place in the language in which the request for access was made.

I therefore consider that [redacted] has failed to comply with the provisions of Article 12(2) of the GDPR by providing some of the responses to requests for access in English, regardless of the language of the person making the request, which creates a risk that non-English speakers may not be able to understand the information.

These facts justify issuing a formal notice to [redacted] requiring it to respond to requests for access in the language of the person making the request.

II. <u>Corrective measure issued by the CNIL (Article 20 of the Law of 6 January 1978)</u>

In view of all these factors and in accordance with Article 20 of Law No.º 78-17 of 6 January 1978, it is therefore necessary to issue **a FORMAL NOTICE** to [redacted] , established at the address

indicated above, **within a PERIOD OF THREE (3) MONTHS** from the notification of this decision and subject to any measures it may already have adopted, to:

- **propose alternatives to identification by means of an identity document for requests to exercise rights made by persons not logged into their account, and to comply with the principle of data minimisation when identification is carried out by means of an identity document;**
- **delete requests for access rights and supporting documents retained beyond the period necessary for the defined purposes;**
- **retain requests for access rights and their supporting documents only for the period necessary in view of the defined purposes;**
- **clarify the information regarding the provision of proof of identity when a request to exercise a right is made;**
- **respond to requests for access in the language of the person making the request.**

The requirements set out above must be strictly complied with in future. The CNIL will carry out further checks as necessary and reserves the right to exercise all the powers conferred upon it by the GDPR and by the Act of 6 January 1978.

This decision, which does not require a response from you, brings proceedings No. 2024-098C to a close. However, this closure is without prejudice to the Commission's right to carry out a further inspection to verify that your company has complied with this formal notice by the expiry of the specified deadline.

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

For further information regarding the formal notice procedure, please visit the CNIL website at the following page: https://www.cnil.fr/fr/la-procedure-de-mise-en-demeure-0.

The Commission's staff ([redacted] are available to provide any further information you may require. You will also find all the relevant information on the CNIL website (www.cnil.fr) or by telephone on 01.53.73.22.22 (from 10am to 12pm, except on Wednesdays).

Yours faithfully,

Marie-Laure Denis

A copy has been sent by email[redacted]