Decision no. MED 2020-037 of November 12th, 2020 giving order to comply to the company [redacted]

(N° MDM201069)

The Chair of the Commission Nationale de l'Informatique et des Libertés (French Data Protection Authority),

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 the free movement of such data, in particular articles 56 and 60;

Having regard to Act no. 78-17 of 6 January 1978 amended, on information technology, data files and liberties (French Data Protection Act), particularly its article 20;

Having regard to Decree no. 2019-536 of 29 May 2019, implementing Act no. 78-17 of 6 January 1978 on information technology, data files and civil liberties;

Having regard to deliberation no. 2013-175 of 4 July 2013 adopting the internal regulations of the Commission Nationale de l'Informatique et des Libertés;

Having regard to decision no. 2019-041C of 15 February 2019 of the Chair of the Commission Nationale de l'Informatique et des Libertés tasking the Secretary General with performing or assigning a third party to perform an investigation on the company [redacted];

Having regard to records of investigation nos. 2019/041-1, 2019/041-2 and 2019/041-3 of 19 February, 20 February and 13 June 2019;

Having regard to the other items in the case file;

I. Context

[redacted] (hereinafter referred to as "the company") is a simplified joint-stock company located at [redacted].

The company belongs to the [redacted] Group, which is composed of three distinct companies: [redacted], a French holding company which wholly owns [redacted], an American company responsible for the Group's activities on USA territory and which itself wholly owns [redacted], the company forming the subject of this procedure. [redacted] was established in 2013 and the Group was established in 2015.

The company has about fifteen employees. [redacted] has four employees. [redacted] has about ten employees.

[redacted]. is responsible for most of the Group's turnover. In 2018, its turnover was to the tune of [redacted]. It is currently in deficit. It carries out fundraising campaigns on a regular basis. It aims to be profitable in 2022.

In the context of its activity, [redacted] develops a mobile application (named [redacted], hereinafter referred to as "the application") designed to put individuals into contact with one another in a professional context. A degraded version of the service is also accessible via a dedicated website. After completing a profile providing various items of personal information (including identity, position held, professional interests and goals), users are presented with the profiles of fifteen other members every day, mostly selected for their geographical proximity. Where there is mutual interest, individuals can contact each other on the application's messaging service. Members can also subscribe to a service providing them with privileged access to a number of extra functionalities.

On 19 February 2019, pursuant to the Chair of the Commission's decision no. 2019-041C of 15 February 2019, a CNIL delegation conducted an online investigation of the application published by the company. Onsite investigations on the company's premises were carried out on 20 February and 13 June 2019.

In several exchanges of emails following the investigations, the company communicated various documents requested by the delegation, including accounting and contractual items.

On September 18th 2020, a draft decision was submitted to the concerned supervisory authorities as part of the cooperation procedure, on the basis of Article 60 of the GDPR.

This draft decision did not give rise to relevant and reasoned objections.

II. Characterisation of the facts

A breach of the obligation to minimise data

Article 5 of the GDPR provides that "*Personal data shall be [...] limited to what is necessary in relation to the purposes for which they are processed*".

Firstly, the investigation delegation found that the application published by the company collects data on the geolocation of the device on which it is installed. The delegation was informed that these data were used to enable the company to present users with profiles of people living in the same city.

Yet the delegation also found that geolocation data was retained in the company's servers with five decimal-place precision, which corresponds to a coordinate with one-metre accuracy. Collecting such accurate geolocation data would appear excessive as the profiles of people presented to users are located across a much wider area. The company could therefore provide an identical service by retaining degraded geolocation data.

Secondly, the investigation delegation was informed that a user using an Android device was obliged to provide a photograph when creating their account. Such obligation was not imposed on terminals operating on iOs or on the "browser" version of the service.

It would therefore appear that this piece of data is not necessary to the intended purposes of the published application and that nothing justifies it being required of users of terminals operating on Android.

Taken together, these facts constitute a breach of Article 5 of the GDPR as the company processes data not necessary to the intended purposes, including precise geolocation and the obligatory photograph for users of the Android device.

A breach of the obligation to set a data retention period proportionate to the purpose of the processing

Article 5 of the GDPR also 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*".

The delegation was informed that no retention period had been set for data stored in the company's database, and those data are therefore retained with no limitation of duration.

As regards accounts whose creation procedure was not completed, the data already provided are retained with no limit set on duration. The delegation found that the company's databases contained 428,905 accounts whose registration procedure had not been completed (out of a total of 1,916,379 registered accounts). One such uncompleted, inactive profile had been retained since its creation on 12 May 2016. Although data retention may be justified for a strictly determined limited period, in order to enable a user to complete an unfinished registration procedure, such retention is excessive beyond any retention period defined.

As regards accounts whose deletion has been requested by their users, the delegation found that they are assigned a special status and become unusable by the users concerned. However, the data are not erased from the database and are retained without justification on the part of the company.

As regards geolocation data, the delegation was informed that they are retained for sixty days and that each new position recorded is listed in the user's geolocation history if it is more than five kilometres from any positions already recorded. If the new position is less than five kilometres from a position already recorded, the latter is incremented and the aforementioned sixty-day period is renewed. Each position records the date on which it was recorded for the first time as well as the incrementation number. The company's database contains 761,834 positions recorded in user accounts. The delegation noted that a user's account created in 2013 had been located over 17,000 times and that 73 positions connected with their profile had been retained. The investigation delegation also found that the position most frequented by the user concerned had been recorded on 18 November 2016 and incremented 1,709 times. Hence, the adopted system provides the company with extremely long visibility of presence in a given place when the user concerned regularly comes within the five-kilometre radius acting as reference. Retention of information on dates of creation of geolocation points is not necessary when retention of the date of its latest update is enough to achieve the desired objective.

As regards messages exchanged by members, the delegation was informed that all such messages were retained by the company. Hence, the delegation found that 30,453,795 messages were stored in the database. Although retention of messages exchanged by active users may be justified by the possibility provided to users of going back over the history of their exchanges, retention of messages exchanged by accounts that have become inactive or been deleted can only be regarded as excessive.

Taken together, these facts constitute a breach of Article 5 of the GDPR as data are retained for excessive periods given the purposes for which they were collected.

A breach of the obligation to inform data subjects

Article 13 of the GDPR obliges the data controller to communicate information to data subjects, including "*reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available*" when data is likely to be transferred outside the European Union (Article 13.1.f) and "*the existence of the right to withdraw consent* *at any time*” (Article 13.2.c). It also specifies that such information must be communicated to the data subject “*at the time when personal data are obtained*”.

Article 12 of the GDPR obliges the data controller to ensure that such information is “*easily accessible*”.

As regards content of the information, the delegation found that, when the application is opened, the homepage asks users to register or log on to their accounts. The homepage also includes two links, one to the general conditions of use and the other to the application’s confidentiality policy.

The investigation delegation found that the confidentiality policy contained most of the information required by Article 13 of the GDPR, but no details of guarantees governing data transfer outside European Union territory; nor was the possibility of withdrawing consent included in the information notices, even though users’ consent sometimes constitutes the legal basis of processing operations.

As regards accessibility of information, the delegation found that, although there was a link to the confidentiality policy on the homepage, there was no link enabling users to access the confidentiality policy and obtain communication of this information during the registration procedure, and therefore at the time when data are actually collected.

Taken together, these facts constitute a breach of Articles 12 and 13 of the GDPR as the information communicated by the company is incomplete and not accessible during collection of data.

<u>A breach of the obligation to ensure data security and confidentiality</u>

Article 32 of the GDPR provides that “*the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk*”.

The delegation found that, when an account was created on the [redacted] application, a password composed of eight figures (in this case, “12345678”) was accepted.

The delegation also found that the password protecting access to certain employees’ workstations was only composed of eight characters comprising three of the four categories of characters. This is not complex enough, given that these workstations enable access to the company’s database and that logins and passwords enabling connection are recorded in the database management software.

Authentication based on use of an insufficiently complex password may lead to associated accounts being compromised and to attacks by unauthorised third parties, brute-force attacks for example.

As an illustration, in its deliberation no. 2017-012 of 19 January 2017, the CNIL considered that, in order to meet password robustness requirements and ensure adequate levels of security and confidentiality, a password must contain at least twelve characters and include at least one uppercase letter, one lowercase letter, one figure and one special character. When a password is composed of eight characters, containing three of the four categories of characters, it must be accompanied by a complementary security measure (such as blocking the account after several unsuccessful attempts at connection) in order to ensure adequate levels of security and confidentiality.

Finally, the delegation was informed that passwords are stored in the database in the form of a hash obtained by the SHA-1 algorithm with addition of a salt.

In this respect, it should be borne in mind that the National Cybersecurity Agency of France's General Security Reference Framework advises against use of SHA-1, and has done so since it was first published in 2010 (Appendix B1 of General Security Regulation 1.20 of 26 January 2010, p. 24). Earlier versions of the reference framework for cryptographic mechanisms had already noted this hashing function's obsolescence since the update in 2008.

There must be no further use of cryptographic mechanisms based on the SHA-1 as it is no longer in keeping with the state of the art.

Taken together, these facts constitute a breach of Article 32 of the GDPR as access to application users' accounts and to developers' workstations is not protected by passwords of a complexity appropriate to the data protected and as the algorithm used for hashing users' passwords uses a hashing function with known vulnerabilities.

Failure to access, by means of electronic communication, information already stored on the user's terminal without the user's consent and without specific information.

Article 82 of Act no. 78-17 of 6 January 1978 amended, on information technology, data files and liberties (French Data Protection Act) provides that : *"Any subscriber or user of an electronic communication service shall be informed in a clear and comprehensive manner by the data controller or its representative, except if already previously informed, regarding:*

1° the purpose of any action intended to provide access, by means of electronic transmission, to information previously stored in their electronic connection terminal device, or to record data in this device;

2° the means available to them to object to such action.

Such access or recording may only be carried out provided that the subscriber or user has explicitly expressed, after receiving said information, their agreement that may result from appropriate parameter settings in their connection device or any other system under their control."

The same article specifies that obtaining the consent is not mandatory when the access to data is *"either exclusively intended to enable or facilitate communication by electronic means"* or *"strictly necessary for the provision of an online communication service at the user's express request"*.

When installing the application and creating an account, the inspection delegation found that the user was asked to allow the application to access the position of the device used via GPS through a pop-up window generated by the phone system. If the user refuses to give access to his or her geolocation data, he or she is redirected to an application page that requests again access to the data with a single button entitled "*Give access to my position*". The pop-up window reappears when the user clicks on this button. Then, if the user refuses to share his geolocation data again, he or she is redirected to the application page previously mentioned, must click on "*Give access to my position*", and is again asked to allow the application to access the position through the pop-up window. The user can only continue the registration process by clicking on the "*Allow*" button in the window.

These elements show that the user is forced to share his geolocation data in order to register and use the application from his mobile phone.

The delegation was informed that providing geolocation data was mandatory in the mobile versions of the application, whereas users of the service's web interface had to manually enter their location to be offered nearby profiles. It can be deduced that the geolocation data of the user's device is not strictly necessary for the provision of the service, since other solutions are offered on other platforms of the application, such as manual activation. Moreover, providing the geolocation data is not exclusively intended to enable communication.

Therefore, the consent of the user had to be obtained prior to the collection of the data.

However, article 2 of the French Data Protection Act provides that *"except where otherwise provided, within the framework of this Act, the definitions of Article 4 of Regulation (EU) 2016/679 of 27 April 2016 shall apply"*.

Article 4.11 of GDPR defines the consent as *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her"*.

In this case, as long as the offered service does not require access to geolocation data, the user should be able to refuse to give his or her consent without being denied access to the service from a mobile phone, as it is allowed on the web interface. Such consent is not free and cannot be considered as valid within the meaning of the GDPR and the French Data Protection Act.

Therefore, these facts constitute a breach of Article 82 of the French Data Protection Act since the user does not validly consent to access his or her geolocation data on his or her terminal.

In light of the above, the company [redacted] located at [redacted], is hereby given order to comply, <u>within 5 (five) months from the notification of this decision</u> and subject to measures it may already have adopted, to:

- **collect adequate, relevant data limited to what is necessary in view of the purposes for which they are processed**, in particular, unless its necessity can be justified, stop collecting the user's geolocation with one-metre accuracy and stop obligatory collection of users' photographs during creation of profiles;

- **define and implement a policy on user data retention periods that do not exceed the periods necessary to the purposes for which they are collected**, in particular regarding data on users who have not completed the account creation procedure and geolocation data;

- **inform data subjects in compliance with the provisions of Articles 12 and3 of the Regulation, with regard to personal data processing carried out**, and, in particular, provide information on the legal basis for such processing and a full description of data subjects' rights, and ensure provision of all the information referred to in Article 13 of the du GDPR, either on the registration form or via a link on the form;

- **for all personal data processing operations implemented, take all necessary measures to enable maintenance of such data's security and prevent unauthorised third parties accessing them,** in particular:

- by storing passwords transformed by means of a reliable non-reversible cryptographic function (i.e. using a public algorithm deemed to be strong whose software implementation has no known vulnerabilities) such as SHA-256;
- by implementing a binding policy on passwords used by users of the sites and mobile applications operated by the company, in line, for example, with one of the following modalities:
  - passwords composed of at least 12 characters, containing at least one uppercase letter, one lowercase letter, one figure and one special character;
  - passwords composed of at least 8 characters, containing 3 of the 4 categories of characters (uppercase letters, lowercase letters, figures and special characters) and accompanied by a complementary measure such as delaying access to an account after several failures, inclusion of a mechanism protecting against intensive automated attempts (e.g. "captcha") and/or blocking the account after several unsuccessful attempts at authentication (10 at most);

- **justify, to the CNIL, compliance with all of the above requests within the time-limit set.**

After this time-limit, if the company [redacted] has complied with this order to comply, this procedure shall be considered closed and a letter shall be sent to it to this end.

However, if the company [redacted] has not complied with this order to comply, a rapporteur shall be appointed and may request that the restricted committee issue one of the penalties set out under Article 20 of the Act of 6 January 1978, amended.

The Chair

Marie-Laure DENIS