Decision No. MED 2022-079 of 8 September 2022 issuing an order to the company, [redacted]

(No. MDM221085)

The Chair of the Commission Nationale de l'Informatique et des Libertés (CNIL),

Having regard to 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 the free movement of such data, in particular Articles 56 and 60;

Having regard to the French Data Protection Act No. 78-17 of 6 January 1978, as amended, particularly Article 20;

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 Agency);

Having regard to the decision of the Chair of the French Data Protection Authority (CNIL) no.2021-183C dated 29 June 2021 of the Chair of the CNIL to instruct the Secretary-General to carry out or have carried out a verification of the compliance of the personal data processing carried out by or on behalf of [redacted];

Having regard to the online investigation record no. 2021-183/1 of 05 August 2021;

Having regard to the onsite investigation record no. 2021-183/2 of 28 September 2021;

Having regard to the other documents in the case file;

I. The procedure

Created in 2009, under the name [redacted] the company called [redacted] since 2012 (hereinafter "the company"), whose registered office is located at [redacted] operates an online sales platform that connects buyers and sellers of second-hand luxury clothing and fashion accessories.

The company employs [redacted] employees worldwide and achieved turnover of [redacted] in 2020, including [redacted] in France.

It has subsidiaries in Germany and Italy, which are mainly in charge of logistical aspects.

Approximately 13 million users are registered on the platform, of which approximately 9 million are located throughout all Member States of the European Union, and in particular 3,872,538 in France, 1,250,899 in Italy, 876,141 in Germany, 590,073 in Spain and 244,074 in Belgium.

The website and application are available in several languages (English, Italian, Spanish).

The processing operations are carried out in the same way, regardless of the user's country of residence.

Pursuant to Decision No. 2021-183C of 29 June 2021 of the Chair of the Commission nationale de l'informatique et des libertés (hereinafter "CNIL "), a CNIL delegation carried out an online investigation on 5 August 2021, then on 28 September 2021, an on-site investigation vis-à-vis the company located (as of the date of the inspections) at 255, boulevard Pereire in PARIS (75017), for the purpose of verifying the compliance of the personal data processing carried out by company or on its behalf, within the provisions of the aforementioned (EU) 2016/679 regulation (hereinafter "GDPR" or "Regulation") and amended Law No. 78-17 of 6 January 1978 and, where applicable, the provisions of Articles L. 251-1 et seq. of the Internal Security Code.

The delegation also focused on monitoring compliance with the provisions of Article L.34-5 of the French Postal and Electronic Communications Code (CPCE).

The platform offered by the company is accessible from the website [redacted] or from the [redacted] app, available on all Android and iOS app stores, for mobiles.

The company has two business models:

- either direct contact, with the direct sending of the product by the seller to the buyer. In this case, the company deducts a purchase commission;

- or contact with authentication of the product by [redacted]: the buyer sends the product to the company for verification, which then makes the delivery to the buyer. In this case, the company deducts a commission on purchase as well as an additional verification fee.

On 8 October, 24 November 2021 and 13 January 2022, the company sent the additional documents requested during the inspections and at the time of the verifications which followed concerning, in particular, the nature of the personal data collected and its retention period, the data processing agreements and the security and confidentiality of the personal data processed.

On 6th July 2022, as part of the cooperation procedure, a draft decision was submitted to the authorities concerned on the basis of Article 60 of the GDPR.

No relevant and reasoned objection has been expressed by one of the relevant authorities.

II. Breaches of the GDPR

1. Breach of the obligation to define 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 must 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 […] (storage limitation)".*

The CNIL recalls, by way of illustration, in its practical guide on retention periods (https://www.cnil.fr/sites/default/files/atoms/files/guide_durees_de_conservation.pdf), that in the absence of a text defining the retention period, *"it is the responsibility of the data controller, pursuant to the general principle of responsibility, to define said period. To do so, it must rely on the purpose for which the processing of personal data is implemented, i.e. the purpose it pursues. It is therefore necessary to identify and assess its operational needs. On the basis of these elements, a period to be applied, or, at least, the criteria for setting it (for example: the time of the business relationship) will thus be defined"* (practical guide, p. 7).

In this respect, by way of clarification, the reference guidelines relating to processing personal data implemented for the purposes of managing commercial activities recommend, in particular, that the data necessary for the performance of a contract or management of the commercial relationship be kept in an active database only for the duration of the contractual and commercial relationship. At the end of said period it must be deleted or anonymised. In some cases, after sorting the personal data processed, part of these data may be archived – in particular for compliance with legal obligations – or retained for other purposes, for example for marketing purposes.

With regard, specifically, to commercial activities that involve the creation of an online account by clients, the reference guidelines specify that the data are intended to be kept until the user deletes the account. However, it is common for users to no longer use these accounts without deleting them, which leads them to continue indefinitely and is contrary to the principle of limitation of data retention laid down by Article 5(1)e of the Regulation. In this case, the CNIL recommends that the accounts be considered inactive after two years and be deleted at the end of this period, unless the user expresses their wish to keep the account active.

In this case, no data retention policy has been defined by the company, with said company indicating that it retains user data for a period of 3 years from a user's last interaction with the platform.

However, the delegation was able to observe in the database:

- 5,646,633 accounts whose last connection was more than 3 years ago,
- 2,556,507 accounts whose last connection was more than 5 year ago,
- 716,481 accounts whose last connection was more than 8 years ago.

The retention of personal data of inactive users for more than 3 years therefore appears excessive.

Moreover, the company clarified that no automated data deletion process was implemented. However, in view of the volume of data processed, only automatic purge or archiving rules would be able to guarantee compliance with the retention periods.

Consequently, keeping user data for a longer period than that defined in its retention policy constitutes a breach of Article 5(1)e of the GDPR.

It is therefore the company's responsibility to effectively implement its personal data retention policy vis-à-vis the data that it processes.

2. Failure to provide a formal legal framework for the processing operations carried out on behalf of the data controller

Article 28(3) of the GDPR provides that any processing carried out by a data processor must be governed by an agreement concluded between the data controller and the data processor which "defines the purpose and duration of the processing, the nature and purpose of the processing, the type of personal data and the categories of data subjects, and the obligations and rights of the data controller". This agreement must therefore provide for a set of mandatory information, detailed in points a) to f) of the same article.

In this case, the delegation found that certain agreements entered into with data processors did not contain all the information required by Article 28 of the Regulation. Namely:

- the agreement entered into with [redacted], which does not contain any information relating to the details of the processing operations carried out (notably, the agreement does not define the reason, nature and purpose of the processing);

- the agreement with [redacted] which does not contain a clause providing for the assistance of the data processor in carrying out an impact assessment, or an obligation for the data processor to inform the data controller in the event of instructions that would be contrary to the GDPR.

The company indicated to the delegation that it had sent draft amendments to the data processors concerned by the incomplete agreements. However, the company has not provided either the amendments sent or the list of data processors concerned. Nor did the company inform the CNIL of the progress of the negotiations for their signature.

These elements therefore constitute a breach of Article 28 of the Regulation.

3. A breach of the obligation to ensure the security and confidentiality of personal data

As data controller within the meaning of the GDPR, the company is subject to the obligations relating to the security of the personal data processing that it performs.

In this respect, Article 32.1 of the GDPR provides that*: "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"*, and notably *"the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services"*.

Firstly, the CNIL highlights that the National Information Systems Security Agency ("ANSSI") had the opportunity to recall the best practices to be applied in this area*: "Any person accessing a sensitive IS resource must be identified and authenticated by means of an individual account"* (Recommendations for the architecture of sensitive or confidential restricted

distribution information systems of 28 December 2020) Moreover, *"Identifiers and secrets associated with administrative accounts, whether technical or business, are part of the first computer attack targets because they have high privileges. It is therefore necessary to be very vigilant about the management of these identifiers and secrets, by adopting at least the following measures and choosing equipment that authorises their implementation: […] use of individual administration accounts instead of generic accounts where possible"* (Recommendations on the security of physical access control and video protection systems of 4 March 2020).

The CNIL then highlights that only individual accounts allow for good traceability of accesses and actions carried out on the information system. The CNIL also notes that shared accounts do not allow proper application of the authorisation policy. However, the latter is a fundamental element of the security of information systems, aimed at limiting access to the data that a user needs (CNIL guide https://www.cnil.fr/fr/securite-gerer-les-habilitations). Indeed, the shared accounts make the accountability of an action much more difficult and complicate the investigation work in the event of a security incident.

Lastly, with regard to passwords, the CNIL highlights that, in accordance with the basic rules on information system security, in order to be effective a password must remain secret and individual. However, when an account is shared between several individuals, this rule is no longer respected.

In this case, the delegation noted that all members of the on-call team in charge of managing the database used a shared account, which does not allow for the proper logging of actions or tracing potential security incidents. Said configuration also jeopardizes the confidentiality of the password for the account concerned.

These facts constitute breaches of Article 32 of the GDPR, which imposes on the data controller the implementation of means to ensure the security of the personal data processed. The company must therefore set up named accounts for members of the on-call team in charge of managing the database.

III. A breach of Article L.34-5 of the French Postal and Electronic Communications Code (Not submitted to the cooperation procedure)

In application of Article L.34-5 paragraph 1 of the Postal and Electronic Communications Code (CPCE), "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".

Paragraph 4 of the same article specifies that direct e-mail marketing is authorised if the recipient's contact details "have been collected from him/her, in compliance with the provisions of French Data Protection Act 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 at the time they are collected and every time a marketing e-mail is sent to him/her if he/she has not initially refused such use".

In this case, the delegation was informed that when a user sells or buys products on the [redacted] platform, said user is then likely to receive marketing emails on the basis of the exception of similar products and services provided for in Article L.34-5 of the CPCE.

Nevertheless, when registering, the user does not have the option of objecting to the receipt of these subsequent emails.

Therefore, if the company fails to offer said option, these facts constitute a breach of the obligations arising from Article L. 34-5 of the French Postal and Electronic Communications Code.

Consequently, [redacted], located at [redacted] is hereby ordered, within three (3) months of notification of this decision, and subject to any measures it may have already adopted, to:

- **effectively implement its personal data retention period policy, which must not exceed the period necessary for the purposes for which the data are collected and proceed with purging or, where applicable, archiving the data stored at the end of the planned retention period, and in any event – concerning the data of users of the platform considered as inactive – by deleting the data of users who have been inactive for more than 3 years;**

- **ensure that the data processing agreements contain all the information provided for in Article 28 of the Regulation;**

- **take all security measures, for all personal data processing that it implements, to preserve the security of said data and to prevent unauthorised third parties from having access to the data, by setting up personal accounts for members of the on-call team concerning the management of the database;**

- **refrain from sending marketing emails based on the exception of similar products or services without having previously offered the recipients, expressly and unambiguously, the possibility of objecting, free of charge and simply, to the use of their contact details at the time said details are collected;**

- **provide supporting documentation to CNIL that all of the aforementioned claims have been complied with within the time limit set.**

At the end of the period, if [redacted] has complied with this order, it will be considered that these proceedings are closed and a letter will be sent to the company to that effect.

Conversely, if [redacted] has not complied with this order by the end of the period, 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 amended Act of 6 January 1978.

The Chair

Marie-Laure Denis