Decision No. MED -2022-112 of 24 November 2022 serving an order on the company [redacted]

(No. MD221128)

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 the Council of 27 April 2016 on the protection of natural persons regarding 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 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 referrals No. [redacted], [redacted], [redacted], [redacted], [redacted], [redacted], [redacted] and [redacted];

Having regard to Decision No. 2021-002C of 4 January 2021 of CNIL's Chair to instruct the general secretary to carry out or have a third party carry out an assignment to verify the processing of personal data implemented by the company [redacted] or on its behalf;

Having regard to the online investigation record no. 2021-002/1 of 7 January 2021;

Having regard to the summons for hearing report no. 2021-002/2 of 16 February 2021;

Having regard to the other exhibits;

I. <u>The procedure</u>

The simplified joint stock company [redacted], (hereinafter "the company"), located at [redacted], publishes a website at the following URL: [redacted]. Dedicated to the online sale of organic cosmetic products, the company was founded in 2015 and, in this context, implements processing for the purpose of managing customers and prospects.

The company has [redacted] employees and generated revenue of around [redacted] million in 2020.

An account must be created on the site to place an order. The payment method offered by the company is payment by bank card only, which can take the form of a monthly direct debit if

the user chooses to subscribe to the "[redacted]" offer. The user then receives a monthly box containing cosmetics products. The company's payment provider is [redacted].

The company has [redacted] customers with an "active" status, i.e. having an ongoing subscription, and [redacted] customers with an "inactive" status, i.e. having terminated their subscription. In addition, it has [redacted] customers with an "archive" status, which corresponds to customers "inactive" for more than three years. Of the "active" clients, [redacted] are located in Belgium and [redacted] in Luxembourg.

Pursuant to Decision No. 2021-002C of 4 January 2021 of the co-chair of the French Data Protection Authority (CNIL), a CNIL delegation carried out an online investigation on 7 January 2021 regarding this company on the website [redacted] for the purpose of verifying the compliance of the processing implemented by the latter with all of the provisions of Act No. 78-17 of 6 January 1978 on information technology, files and freedoms as amended and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter the "Regulation" or the "GDPR").

This audit was followed by a hearing on 16 February 2021, the terms of which had been notified to the company in a letter dated 14 January 2021.

The company provided additional information by email dated 24 February and 6 April 2021.

On 14 October 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.

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

II. The processing operations in question and responsibility for the processing

According to Article 4(7) of the GDPR, the data controller is *"the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing"*.

Article 4(8) of the GDPR defines the processor as *"a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"*.

By way of illustration, in guidelines 07/2020 on the concepts of data controller and processor in the GDPR, the European Data Protection Board specified that *"the nature of the service will determine whether the processing activity amounts to processing of personal data on behalf of the controller within the meaning of the GDPR. In practice, where the provided service is not specifically targeted at processing personal data or where such processing does not constitute a key element of the service, the service provider may be in a position to independently determine the purposes and means of that processing which is required in order to provide the service. In that situation, the service provider is to be seen as a separate controller and not as a processor"* (§82).

In this case, [redacted] must be regarded as the data controller for the management of accounts, orders and the customer file.

The company uses a shipping service provider, [redacted], to deliver its packages. To this end, [redacted] signed on 9 October 2020 with [redacted] the general terms and conditions of sale concerning the organisation of the transport of packages.

To this end, [redacted] sends it delivery instructions and personal data concerning the package recipients. It emerges from the file that the service requested by [redacted] does not specifically constitute data processing but above all a delivery service; that [redacted] constitutes its own database from the personal data transmitted, in particular, by [redacted]; that it itself independently monitors the delivery and delivery of the package by contacting the recipient directly.

With regard to these elements, [redacted] must be considered the data controller for its delivery activity and not as a subcontractor of [redacted]. Therefore, the contract between the two companies is not subject to the requirements of Article 28(3) GDPR.

III. Breaches of the GDPR

Breach of the obligation to specify and comply with a personal data retention period in proportion to the purpose of the processing

According to Article 5(1)(e) GDPR, 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ("storage limitation")".*

At the hearing of 16 February 2021, the auditing delegation was informed that the information relating to the bank cards of subscribed users is hosted by a subcontractor, [redacted]. The company has a table, in its database, that contains an alias provided by [redacted] ("[redacted]") enabling it to submit direct debit requests to [redacted]. This "subscriber reference" is systematically comprised of the letter "B" followed by a series of numbers. For the direct debit request to be processed, [redacted] needs this "subscriber reference", as well as three other pieces of information it generates: the fields "code_cb" (bank card code), "date_val" (validation date) and "type_cb" (bank card type).

The company indicated that if a user has terminated their subscription, this "subscriber reference" is retained for a period of three months after the last direct debit. At the end of these three months, the fields "code_cb", "date_val" and "type_cb" are deleted. With regard to the "subscriber reference", only the letter "B" is deleted and the series of numbers is retained.

The company justifies the retention of the altered "subscriber reference" for cases where a customer wishes to re-subscribe after terminating their last subscription. They could then be asked to update their bank card data, the "subscriber reference" being necessary for updating this data. However, the company states that this is a rare case implemented in certain resubscription campaigns. Apart from these specific campaigns, the resubscription corresponds to a new order on the site, which requires entering data relating to a new bank card.

The CNIL recalls 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 for the personal data concerned by the processing, *"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."*

In this context, personal data cannot be stored for an indefinite period. Where the data is no longer necessary for the purpose for which it was collected, the data must be deleted or be subject to intermediate archiving only in the case of relevant data, when the data is necessary for compliance with legal obligations or for pre-litigation or litigation purposes. Beyond the data retention periods in intermediate archives, personal data must, unless otherwise provided, be deleted or anonymised.

The "subscriber reference" altered beyond three months cannot be used by the company to trigger a payment, as the procedure requires further information that has been deleted. However, "the subscriber reference", even altered, can allow a single instance of correspondence between a customer's bank data recorded in the [redacted] database, which keeps the bank data for a period of 13 months from the last transaction, and the customer account at the company.

The "subscriber reference" data is therefore stored without a retention period being defined and without meeting a specific purpose. These elements combined constitute a breach of Article 5-1-e of the GDPR.

Breaches of the obligation to ensure the security and confidentiality of data

Article 32 of the Regulation provides that the data controller must guarantee the security and confidentiality of the personal data it processes, in these terms: *"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, including inter alia as appropriate: (...) b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services."*

Firstly, the delegation noted that a user's password, generated if forgotten, is communicated clearly by email and that it is not necessary for the user to change it after the first login.

This practice generates a risk to the confidentiality of the user's data and is contrary to the recommendations of the CNIL on this subject, which, under basic security measures, recommends that the password should never be communicated to the user in clear text by email, unless it is a temporary password or one that must be changed during the first use (https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires).

These facts disregard, in this case, the provisions of Article 32 of the GDPR.

Secondly, the delegation was informed that the passwords of the persons having access to the back office of the after-sales department, namely the persons of the after-sales department, the statutory auditors and the chairman of the company, are created manually by the chairman of the company himself. He then hands over passwords in person in order for the data subject to register it in their password manager. If the password is forgotten, it is also the chairman of the company who must generate a new one. Lastly, on certain occasions, the password created by the chairman was communicated, by email, to the director of the after-sales department team, who was responsible for giving it to the persons concerned.

However, this measure does not make it possible to ensure that only the account holder holds the associated password, which is not liable to guarantee the traceability of access to the data (removing their attributable nature), particularly in the event of unauthorised third-party access.

According to the basic rules concerning the security of information systems, in order to be effective, a password must remain secret and individual. However, when it is known to several individuals, as in the present case, this rule is no longer respected.

To reduce the risk of disclosure of the password and respect its secrecy, it should only be known to the account holder. As such, passwords should be created or, at a minimum, renewed from the first login by the users themselves and not by a third party. It should also be possible for users to renew passwords as many times as desired. Indeed, the Commission recommends that the data controller allow the data subject to change his/her password him/herself (deliberation no. 2017-012 of 19 January 2017 adopting a recommendation on passwords).

These facts disregard, in this case, the provisions of Article 32 of the GDPR.

Lastly, the delegation was informed that during certain resubscription campaigns, the emails sent contain unique and personalised links containing the identifier of former subscribers associated with an order identifier. As such, when the person clicks on the link to resubscribe, they are automatically identified on the [redacted] website when the identifier and order numbers correspond to an existing customer. These links have a lifetime of one month. In addition, the emails sent to former subscribers do not contain any information on the identifier of the links.

However, links to authenticate a user pose a risk to the data contained in users' accounts. Firstly, since these links are valid for a period of one month, any person having access to the user's inbox or being able to intercept his/her emails may, within this period of one month, have access to the user account data. Secondly, the recipient of the email may decide to legitimately send this email to other persons – for example to inform them of temporary offers – without realising that the link makes it possible to log in directly to their account. Former subscribers should at least be informed of the risks of access to their personal data through resubscription campaign emails.

As such, the authentifying nature of these links, without any additional measure making it possible to ensure that it is the user account holder and without informing the recipient of the risk incurred, provides an insufficient level of security of the personal data accessible from said account.

These elements combined constitute a breach of Article 32 of the GDPR.

With regard to these three breaches, it is therefore the company's responsibility to stop sending the site login passwords, in clear text by email, without additional protection measures; to implement any measure enabling the person concerned to change his/her password to access the back office; and to stop sending by email to former subscribers links allowing automatic login to their account during commercial operations, unless additional measures are taken, in particular to ensure the authentication and information function in a robust manner.

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

- **define and implement a data retention period policy that does not exceed the period necessary for the purposes for which data are collected in accordance with the provisions of Article 5(1)(e) of the GDPR,** by ensuring, when anonymising the data necessary for bank direct debits, to delete any element likely to allow re-identification by individualisation or cross-checking of any external data sets;

- **take measures to preserve the security of such data and to prevent unauthorised third parties from having access to it**:
    - by ceasing to send login passwords to the site, in clear text by email;
    - by implementing measures providing that only the holder of an account allowing access to the back office knows the password and that the passwords are created or, at least, renewed from the first login by the users themselves and not by a third party, but also by offering them the ability to renew their password at will;
    - by ceasing to send to former subscribers links allowing automatic authentication to their user account during commercial operations, except to take additional measures, in particular to ensure the authentication function and information in a robust manner.

This decision does not call for a response from you to the CNIL. However, if the breach referred to in this order is found to persist or to be repeated during subsequent investigations, I may appoint a rapporteur, within the CNIL, and refer the matter to the CNIL's restricted committee, without a new order being sent to you beforehand, so that one or more of the corrective measures provided for in Articles 20 et seq. of the Act of 6 January 1978 may be imposed, if necessary.

The Chair

Marie-Laure Denis