Decision no. MED-2025-083 of 1st July 2025 issuing an order to the company [redacted]
(MDM251042)

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

Having regard to Law No 78-17 of 6 January 1978 on data processing, data files and individual liberties, as amended, in particular Article 20;

Having regard to the French Postal and Electronic Communications Code,

Having regard to Decree No 2019-536 of 29 May 2019 implementing Law No 78-17 of 6 January 1978 on data processing, data files and individual liberties;

Having regard to deliberation No 2013-175 of 4 July 2013 adopting the internal rules of procedure of the CNIL;

Having regard to Decision No 2023-100C of 20 March 2023 by the Chair of the French Data Protection Authority to instruct the Secretary General to carry out or have carried out an assignment to verify the processing of personal data relating, in whole or in part, to data relating to the marketing or use of products or services associated with the [redacted] brand;

Having regard to online inspection report No 2023-100/1 of 9 May 2023;

Having regard to on-site investigations report No 2023-100/2 of 11 May 2023 ;

Having regard to the other exhibits in the case file.

I. The procedure

[redacted] (hereinafter the "company"), located at [redacted], is a simplified joint stock company created in [redacted] specialising in the sale of women's clothing and accessories. It operates around 400 stores and employs around 2,500 employees in France. Its revenue in 2022 was [redacted]

The company, whose main establishment is located in France, sells its items in stores through its subsidiaries located in France, Belgium, Luxembourg, Switzerland and in its affiliated stores. It also sells on-line on its e-commerce website and publishes several websites for individuals located in Italy, Germany, Spain, Poland and France.

It is responsible for the processing it implements in the context of its subsidiaries, affiliated stores and e-commerce sites. The purpose of this processing is marketing by e-mail and SMS for customers who have made at least one purchase or who have subscribed to the "[redacted]" loyalty programme.

It also carries out marketing by email to its prospects, i.e. any individual who has created an account on the website without making a purchase.

The company has approximately eight million customers and prospects in its database.

Pursuant to my Decision N° 2023-100C of 20 March 2023, a delegation of the Commission nationale de l'informatique et des libertés (hereinafter, the "CNIL") carried out on 9 May 2023 an on-line investigation of the [redacted] website, then on 11 May 2023 an on-site inspection at the company's premises located at [redacted].

The purpose of these inspections was to verify the compliance of the processing of personal data concerning, in whole or in part, data relating to the marketing or use of the products or services associated with the "[redacted]" brand with the provisions of Regulation No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data (hereinafter the "GDPR") and Law No 78-17 of 6 January 1978 as amended on information technology, files and freedoms (hereinafter the "Data Protection Act"). The delegation also focused on monitoring compliance with the provisions of Article L. 34-5 of the French Postal and Electronic Communications Code (CPCE).

In letters dated 22 and 23 May, 1 September, 3 October and 13 October 2023, the company sent the additional documents requested during the audit of 11 May 2023 and during the subsequent verifications concerning in particular the retention period of the personal data collected, the procedures for objecting to marketing and the security of the personal data processed.

II. Application of the cooperation and consistency mechanism

On 17 April 2025, in accordance with Article 56 of the GDPR, the CNIL informed all European supervisory authorities of its competence to act as lead supervisory authority with regard to cross-border processing operations implemented by the company, based on the fact that the company's sole establishment is located in France.

After exchanges between the CNIL and the European data protection authorities within the framework of the one-stop-shop mechanism, the following authorities are concerned: Belgium, Spain, Poland, Luxembourg, Italy, Germany, Sweden, Austria and Czech Republic.

Pursuant to Article 60(3) GDPR, the draft decision was forwarded to the European concerned supervisory authorities on 28 May 2025.

On 25th June 2025, none of the concerned supervisory authorities had raised any relevant, reasoned objection to this draft decision so that, pursuant to Article 60(6) of the GDPR, they are deemed to have approved it.

Breaches under the French Postal and Electronic Communications Code do not fall within the scope of the cooperation mechanisms.

III. Breaches of GDPR

A. Breach of the obligation to define and comply with a retention period proportionate to the purpose of the processing (Article 5(1)(e) GDPR)

In law, Article 5(1)(e) GDPR states 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*".

Pursuant to the aforementioned provisions, it is the responsibility of the data controller to define a retention period for personal data according to the purpose of the processing. Once this purpose has been fulfilled, the data must be deleted, anonymised or archived as an interim measure, where retention is necessary, in particular, to comply with legal obligations or for pre-litigation or litigation purposes. The effectiveness of the implementation of a data retention period policy makes it possible to ensure in practice that the data is kept in a form that enables the identification of the data subjects for a period not exceeding that necessary for the purposes for which it is processed. This also makes it possible, in particular, to reduce the risks of unauthorised use of the data in question, by an employee or by any third party (see CNIL, FR, 29 October 2021, Sanction, SAN-2021-019, published; CNIL, FR, 7 July 2022, Sanction, SAN-2022-015, published).

The CNIL indicates in its reference framework relating to the processing of personal data implemented for the purposes of managing commercial activities[1] that data relating to customers used for marketing purposes may be retained during the commercial relationship, then for a period of three years from the end of this relationship. It also indicates that data relating to prospects and which is also used for prospecting purposes may be retained for a period of three years from its collection or the last contact from the prospect.

1. On the retention of personal data of customers and prospects

In this case, the control delegation was informed of the definition and implementation by the company of a retention period policy for the data of its customers and prospects in a database.

The company indicated that it kept their data for three years from the "*last contact*" between them and the company. The company specified that by "*last contact*", it meant:

- the opening of an email;
- the purchase of an item;
- a click within an email;
- the connection to its website.

The delegation noted in the company's database the presence of 19,297 lines corresponding to customers who opened an email within three years of their purchase.

However, if making a new purchase, clicking on a link in an email or connecting to the company's website constitute actions that can justify an additional three-year retention period

[1] https://www.cnil.fr/sites/cnil/files/atoms/files/referentiel_traitements-donnees-caractere-personnel_gestion-activites-commerciales.pdf

of customer and prospect data in that they involve a positive action by the person, this is not the case for opening a simple email.

Indeed, in addition to the fact that it may result from an error or a semi-automated process within certain email clients, the action of opening an email does not attest, as such, to either a particular interest of the person in the content of the email received, or his or her particular desire to continue the business relationship with the company.

These facts constitute a breach of Article 5(1)(e) of GDPR.

Consequently, the company is ordered to amend its data retention policy by eliminating the possibility of retaining the personal data of its customers and prospects for an additional period of three years on the basis of the opening of an email. It will also have to delete customer personal data stored in this database for this reason. Where applicable, it must delete the personal data of prospects stored in the database for the same reason.

2. On the retention of personal data in the "[redacted]" table

In this case, the delegation was informed by the company during the onsite investigations "*that at the end of the three-year period, the data [of customers and prospects] goes to the 'pending deletion'' status. After 30 days, the data is then anonymised automatically in a batch*[2]".

During the same audit, the company also informed the delegation of the ongoing overhaul of its information system. On this point, the company indicated that the initial database was based on the [redacted] management system, which was to be replaced by the [redacted] management system.

Within the company's former database, the delegation noted the existence of a "[redacted]" table, containing an "*event*" tab tracing all the actions carried out on a customer account (account creation, association with a store, *etc*.).

Although the company specified that this table was "*depreciated*", had only "*technical utility*" and was supposed to be deleted in March 2024, the delegation noted that it contained personal data such as the surname, first name and email address of 3,901 customers whose accounts nevertheless appeared as archived. This data should therefore have been anonymised.

However, I note that during the onsite investigations, the company indicated that it was in a transition phase and was implementing several databases. I also note that the deletion of the "[redacted]" table was announced for March 2024.

These facts constitute a breach of Article 5(1)(e) of GDPR.

The company must – subject to the possible deletion of this table – delete the non-anonymised data of archived customers from the [redacted] table.

[2] That is, in batches.

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

In law, Article 32 GDPR requires 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 data processing it implements is sufficiently secure. The sufficiency of the security measures is assessed (a) with regard to the characteristics of the processing and the risks it entails, and (b) with consideration of the state of knowledge and the cost of the measures. The implementation of a robust authentication policy is a basic security measure that contributes to compliance with the obligations of Article 32 GDPR.

In its Deliberation No 2022-100 of 21 July 2022 adopting a recommendation on passwords and other shared secrets, which is not mandatory but which provides relevant information on the security measures that should be taken, the CNIL recommends that, to ensure a sufficient level of security and confidentiality, if authentication is based solely on an identifier and a password, the password be composed of at least 12 characters including upper case, lower case, numbers and special characters to be chosen from a list of at least 37 possible special characters, or be composed of at least 14 characters including upper case, lower case and numbers, without any mandatory special character, or, when it corresponds to a sentence comprising words in the French language, be composed of at least seven words.

Failing this, the CNIL considers that a sufficient level of security and confidentiality can also be ensured by authentication based on a password at least eight characters long, made up of three different categories of characters but accompanied by an additional measure such as, for example, a temporary ban on access to the account after several unsuccessful attempts, the duration of which increases with each attempt, the implementation of a mechanism to protect against automated and intensive submissions of attempts (e.g. “captcha”) or the blocking of the account after several unsuccessful authentication attempts (maximum 10).

The CNIL has examined the institution’s practices with regard to these principles.

In this case, it emerges from the online findings that when creating an online customer account, the password allowing access to this account is composed of at least 8 characters of 3 different categories (1 upper case letter, 1 lower case letter, 1 number) without any additional security measures being required.

However, this password policy does not guarantee a sufficient level of security. Although the number of characters of the password allowing the customer to access his/her account is sufficient with regard to the aforementioned recommendations, it is on the condition that it is accompanied by an additional security measure, which is not the case here.

These elements characterise a breach of Article 32 of the GDPR.

Therefore, the company is ordered to put in place a password policy allowing access to customer accounts that is more restrictive, in particular by implementing the following measures: either by extending the length of the passwords of customer accounts, or by

accompanying this password with an additional measure such as the implementation of a mechanism to protect against automated and intensive submission of attempts, for example.

IV. Breach of Article L34-5 of the French Post and Electronic Communications Code

(Breach not subject to the cooperation mechanism)

In law, Article L. 34-5 of the French Postal and Electronic Communications Code (CPCE) provides that *"direct prospecting by means of an automated electronic communications system within the meaning of 6° of Article L. 32, a fax or e-mail using the contact details of a natural person, subscriber or user, who has not previously expressed his/her consent to receive direct marketing by this means is prohibited.*

Direct prospecting is the sending of any message that is directly or indirectly intended to promote goods, services or the image of an individual selling goods or providing services. For the purposes of this article, calls and messages whose purpose is to encourage users or subscribers to call a premium rate number or to send premium rate text messages also fall within the scope of direct marketing.

However, direct prospecting by e-mail is permitted if the contact details of the recipient have been collected from them, in compliance with the provisions of Act no. 78-17 of 6 January 1978 relating to data processing, files and freedoms, at the time of a sale or provision of services, if the direct prospecting action concerns similar products or services provided by the same natural or legal person, and if the recipient is expressly and unambiguously offered the option to object, free of charge, other than charges related to the sending of the objection, and in a simple manner, to the use of his/her contact details at the time they are collected and each time a prospecting email is sent to him/her in the event that he/she has not refused such exploitation from the outset.

1. Marketing messages sent to customers as part of the "[redacted]" loyalty programme

In this case, **firstly,** with regard to consent, the delegation noted that when a customer joined the online "[redacted]" loyalty programme, he/she was automatically subscribed to marketing communications by e-mail related to this loyalty programme. The company stated that, similarly, for customers subscribing to the loyalty programme in-store, no consent was obtained to send messages concerning the loyalty programme.

The company indicated that these emails were "*inherent in the programme and that a refusal would mean that the person concerned would not be able to enjoy its benefits, including the welcome cheque*".

It appears that the sending of emails in connection with the loyalty programme can be described as a service that is equivalent to joining this programme. Also, the company may avail itself of the exemption from obtaining consent provided for in Article L. 34-5 of the CPCE in order to send customers emails related to the loyalty programme.

Secondly, with regard to the objection, the delegation noted that customers who have joined the loyalty programme are not able to object to the use of their personal data to send marketing messages when they join this programme but only *a posteriori* in their customer space or by an unsubscribe mechanism at the bottom of emails.

However, the customer must be able to object to the receipt of emails in the context of the exemption for similar products or services at any time, in particular when collecting data, which the company does not allow.

This results in a breach of Article L. 34-5 of the French Postal and Electronic Communications Code.

The company is ordered to allow customers who are members of the loyalty programme to object to the receipt of emails in connection with this programme, at the time their personal data is collected.

2. Marketing messages sent to customers and prospects as part of survey emails

In this case, the delegation noted that when creating an account, customers and prospects were *"subscribed by default"* in the "Survey" section, with the corresponding box pre-ticked. It was also noted that this section included the following information: "*Open the dialogue box and give us your opinion*".

The company also informed the delegation that customers and prospects only received one survey email to which they were "*free to respond or not*".

It emerges from these elements that these survey emails can be classified as marketing emails insofar as they may contribute to the commercial activity of the company and that they are addressed directly and individually to persons via their email address (CJEU, judgment of 25 November 2021, case C-102/20).

Regarding the sending of survey emails to customers, if the company can avail itself of the exception provided for in Article L. 34-5 of the CPCE, it must offer its customers the opportunity to object to the sending of such survey emails, at the time the customer's data is collected.

The delegation noted that customers who made a purchase are not able to object to the use of their data to send marketing messages when creating their account, but only *a posteriori* in their customer space by unticking the corresponding box.

It follows from these elements that customers may not object to receiving electronic marketing messages for similar products or services at any time, in particular at the time when their data is collected.

With regard to the sending of survey emails to prospects who have created an account without purchase, the delegation noted that their consent to the receipt of electronic marketing messages was not collected at any time.

However, the mere creation of an account cannot prejudge an order for products from the company. Therefore, the company cannot in this case avail itself of the exception of Article L. 34-5 of the CPE relating to "*similar services",* and it must obtain the consent of these prospects before sending them a survey email.

A breach of Article L34-5 of the French Postal and Electronic Communications Code is established.

The company is ordered to allow customers who create an account to object to the receipt of survey emails at the time their data is collected.

It must also, with regard to its prospects who have created an account, obtain their consent to the receipt of survey emails.

Consequently, [redacted], located at [redacted], is <u>ORDERED WITHIN THREE (3) MONTHS OF NOTIFICATION OF THIS DECISION</u> and subject to any measures it may already have taken, to:

- **amend its personal data retention policy pursuant to Article 5(1)(e) of the GDPR and,**
  - **eliminate the opening of an email as a type of "last contact from" the individual, making it possible to delay the starting point of the retention period in the active database of the data of its customers and prospects;**
  - **delete the data of its customers and prospects stored in the database for this reason;**
  - **delete the personal data of the 3,901 customers whose accounts are archived from the "[redacted]" table**;

- **implement a binding policy on passwords for online customer accounts** based, for example, on the following terms:
  - passwords are composed of at least 12 characters, containing at least one capital letter, one lowercase letter, one number and one special character **<u>or</u>** passwords are composed of at least 8 characters, containing 3 of the 4 categories of characters (capital letters, lowercase letters, numbers and special characters) and are accompanied by an additional measure such as, for example, delaying access to the account after several failures (temporary suspension of access, the duration of which increases as attempts are made), setting up a mechanism to guard against automated and intensive submission of attempts (e.g. "*captcha*") and/or blocking the account after several unsuccessful authentication attempts (maximum 10);

- **with regard to prospecting carried out electronically in accordance with Article L. 34-5 of the CPCE:**
  - **not send electronic marketing messages for similar products or services without first offering customers the possibility of objecting to the receipt of emails in connection with the loyalty programme**, free of charge and in a simple manner, at any time, including when their data is collected;
  - **not send electronic marketing messages for similar products or services without first offering customers the opportunity to object to the receipt of survey emails,** free of charge and in a simple manner, at any time,

including when their data is collected;
    - **obtain the consent of prospects** with a customer account prior to sending survey emails.

- **prove to the CNIL that all the aforementioned requests have been complied with within the allotted time.**

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

Conversely, if it has not complied with this order, it is recalled that a Rapporteur may be appointed to request that the Restricted Committee impose one of the sanctions set forth by Article 20 of the Law of 6 January 1978, as amended.

The Chair

Marie-Laure Denis