CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

The Chairman

[redacted]

Paris, on August 8, 2024

Our ref.: [redacted]
To be stated in all correspondence

Registered letter with acknowledgement of receipt no. [redacted]

Dear Sir,

[redacted]'s main activity is the mail order sale of men's clothing, via its website, paper catalogues and telephone.

It offers its services in several European Union countries, with France and Germany accounting for around [redacted]% of its business. It has [redacted] customers and prospects in France, [redacted] in Germany, [redacted] in Belgium, [redacted] in the Czech Republic, [redacted] in Austria, [redacted] in Poland, [redacted] in the Netherlands, [redacted] n Slovakia and [redacted] in Hungary.

In accordance with **decision no. 2022-010C of 22 December 2021**, the Commission nationale de l'informatique et des libertés (CNIL) carried out an online inspection on 11 January 2022 of the website accessible at the URL "https://[redacted]" published by [redacted]. This inspection was followed by a hearing at the premises of the CNIL on 1 February 2022.

The purpose of this inspection was to verify the compliance of the processing operations carried out by your company with the provisions of Regulation (EU) 2016/679 on data protection (GDPR) and Law no. 78-17 of 6 January 1978 as amended. In particular, this involved following up on several complaints received by the CNIL, most of which were forwarded by our German counterparts, relating to the difficulties encountered by data subjects in exercising their right to access, delete and object to the processing of their personal data by [redacted]

The findings of these inspections, as well as the additions made on 31 January, 9 February, 8 April and 29 April 2022, **lead me to raise the following points**, for which I apologise for the delay.

As a preliminary remark, the inspection delegation was informed that the data of [redacted]'s customers and prospective customers may be used for marketing purposes by your company's partners.

Informal checks carried out after the online inspection revealed that the online account creation form now includes a link allowing Internet users to access a list of categories of commercial partners involved in marketing operations, but not a list with the identity of such partners.

In this respect, a distinction should be made depending on whether or not the data collected is transmitted to your commercial partners. If your company carries out electronic marketing operations on behalf of its partners without transmitting the data to the latter, and in order to guarantee the informed nature of consent within the meaning of Article L.34-5 of the French Postal and Electronic Communications Code, as clarified by the provisions of Article 4-11 of the GDPR, the data subjects must be informed of the identity of each of the partners on whose behalf consent is collected (for example, via a list accessible on the collection medium).

If the data collected is transmitted to your partners in order to enable them to carry out their own processing for electronic marketing purposes, the CNIL considers that the legal basis for this processing is the consent of individuals within the meaning of Article 6 of the GDPR. Consent to the resale of data does not mean that the consent of individuals must not also be obtained, pursuant to Article L. 34-5 of the French Postal and Electronic Communications Code, for the use of their data for electronic marketing purposes. This consent to receive marketing communications may either be obtained by the partners who have purchased or received the data and who will actually use it to send marketing messages, or by your company, which wishes to transmit it to its partners (this consent being obtained on their behalf). In the latter case, consent may be obtained jointly for the transmission of data and marketing, but this implies that your company is able to provide an exhaustive list of partners authorised, as data controllers, to use the data for electronic marketing.

I therefore invite you that you disclose the identity of each of the partners on whose behalf consent is collected. For all intents and purposes, the guidelines published by the CNIL on the management of commercial activities sets out the principles to be adhered to in the event of the transmission of data by a data controller to commercial partners. You will also find a practical information sheet on the transmission of data to partners on the CNIL website[1].

Furthermore, the delegation noted that the data relating to individuals who order online is kept for three years from their last order and for five years for catalogue and telephone orders. At the end of this period, the directly identifying data is replaced by "ANONYMOUS" in the main table of the database. However, the field relating to the customer identifier is retained.

The company also indicated that it retains order data indefinitely for statistical purposes. The delegation noted that the database table containing order data includes the customer identifier.

I would like to draw your attention to the fact that information relating to orders placed by an individual, i.e. in particular the product purchased and the date of purchase, together with the customer identifier, is personal data which may enable individuals to be identified. This configuration therefore does not meet the criterion of the impossibility of isolating an individual as detailed in the opinion of the Article 29 Working Party (G29, now the European Data Protection Board, EDPB) on anonymisation techniques[2].

[1] https://www.cnil.fr/sites/cnil/files/atoms/files/transmission_des_donnees_a_des_partenaires.pdf
[2] Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques*, 10 April 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

I therefore invite that you do not retain any other information, such as invoices, which, when cross-referenced with the data contained in your IT system, would make it possible to re-identify individuals after the retention period and, in particular, to retrieve the orders they have placed. I also encourage that you put in place appropriate measures to counter the risks of re-identification, which could include, but are not limited to, the deletion of the lines concerned, the replacement of the customer identifier with a new identifier or the aggregation over time of the information that is useful to you in order to meet your statistical purposes.

I. Analysis of the facts in question

1. Regarding the breach of the obligation to define and comply with a retention period proportionate to the purpose of the processing operation

Article 5(1)(e) of the 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* [...]".

In 2018, the CNIL also published a recommendation on the processing of payment card data relating to the remote sale of goods or provision of services. This stipulates that bank card details should only be kept for the duration of the payment and the expiry of the deadlines set for the withdrawal or return of products. In this case, the retention period for the card number and expiry date may be the period stipulated in Article L. 133-24 of the French Monetary and Financial Code, i.e. 13 months following the debit date. This period may be extended to 15 months to take account of the possibility of using deferred debit payment cards. Lastly, the recommendation states that "*the retention of the security code after the first transaction is prohibited in all cases*".

In this case, when ordering via the paper catalogue, the company's customers have the option of paying by credit card by entering their card number, expiry date and security code on the order form. The delegation was informed that purchase orders are kept by one of your company's service providers for a period of four years before being securely destroyed.

The data relating to payment cards is therefore retained for an excessive period insofar as this exceeds the period necessary for the management of any complaints provided for by the French Monetary and Financial Code.

I therefore consider that [redacted] has breached the provisions of Article 5(1)(e) of the GDPR by storing credit card information for an excessive period of time.

2. On the breach of the obligation of transparency and to provide information to individuals

Article 12 of the GDPR states that "*The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14* [...] *to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language*".

Article 13 of the GDPR requires the data controller to provide the data subject with various items of information, in particular regarding the identity and contact details of the data controller, the purposes of the processing carried out, its legal basis, the recipients or categories of recipients of the data, and whether the data controller intends to transfer data to a third country.

The regulation also requires that, where it appears necessary to ensure "*fair and transparent processing*" of personal data, that individuals are informed about the period of data retention, the existence of the various rights that individuals have, the existence of the right to withdraw consent at any time, and the right to lodge a complaint with a supervisory authority.

In this case, with regard to the information provided on the website "[redacted]", the delegation noted that the "Personal Data Policy" contains all the information required by Article 13, with the exception of information on data retention periods, which is not sufficiently explicit. Information on data retention periods is necessary, in particular, to enable data subjects to exercise their rights before their data is deleted.

The delegation also noted the presence on the same website of an order form that can be downloaded in PDF format and accessed in the "Prices Catalogue" section, which does not include any information or reference to the personal data policy.

Lastly, the delegation was informed that orders can be placed by telephone. It was specified that telephone conversations may be recorded for quality monitoring purposes.

It was stated that no information on the processing for the purpose of managing the order is given to the data subjects. With regard to processing for the purpose of recording telephone conversations, it was stated that the customer service representatives working for French customers do not inform data subjects at the time of the call of the purpose of the recording of their telephone conversation, the recipients of the recording, and their right to object to and access the recordings. German customer service representatives only inform of the right to object.

It follows from the above that the data subjects are not given the opportunity to understand the reason for the collection of the various data concerning them, the processing that will be carried out on their data and the rights they hold in this respect.

I therefore consider that [redacted] has breached the provisions of Articles 12 and 13 of the GDPR.

3. On the breach of the obligation to comply with requests to exercise rights

Article 15 of the GDPR states that any person has the right to know whether a data controller holds personal data concerning him or her and lists the information that must be communicated to him or her, where applicable, when exercising his or her right of access.

Article 12(3) of the GDPR states that "*The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests.*

The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay".

Article 12(4) states that "*If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action* [...]".

Article 12(6) states that "*Without prejudice to Article 11, 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 additional information necessary to confirm the identity of the data subject*".

In this case, the delegation was informed, during the hearing of your company, that in the event of a request to exercise the right of access, proof of identity is systematically requested for security purposes and in order to avoid any identity theft. Several complaints, from [redacted] ([redacted]), [redacted] ([redacted]) and [redacted] ([redacted]), point to such a practice.

It also emerged from the checks carried out that certain requests to exercise the right of access had not been fulfilled:

- with regard to the complaint by [redacted] the company refused to grant his request for access because he did not wish to provide proof of identity in support of his request;
- with regard to the complaint by [redacted] the company proceeded to delete the complainant's data before granting his request for access, and did not respond favourably to the complainant's subsequent requests for access;
- with regard to the complaint by [redacted], the company stated that it had proceeded to delete the complainant's data, specifying that it did not keep the requests and responses provided in the event of the exercise of rights sent by post, and that it was therefore unable to provide proof that it had responded to the complainant's request for access.

In addition, the investigation into the complaints lodged by [redacted], [redacted] and [redacted] revealed that, while the company did provide an initial response to their request, it did not respond to the complainants' subsequent requests for access to their personal data or confirmation that such data had been deleted.

However, it appears first of all that in the event of doubt as to the claimant's identity, [redacted] may ask the person concerned to prove his or her identity by means that are less intrusive than providing proof of identity, for example by logging on to his or her personal space or by asking for the customer ID included in any mail received.

Secondly, in the aforementioned complaints, [redacted] was unable to demonstrate the existence of reasonable doubt as to the identity of the claimant, justifying the collection of an identity document.

Finally, the data controller is required to respond to requests from individuals to exercise their right of access whenever it holds data concerning them, which was not the case in this instance. The data controller must also inform individuals of the measures taken in response to requests to exercise their rights.

I consider that [redacted] has breached the provisions of Article 12 of the GDPR by systematically requesting a copy of the identity document from persons exercising their right of access and by not informing the data subjects of the measures taken following requests to exercise this right.

I also consider that [redacted] has breached the provisions of Article 15 of the GDPR by failing to satisfy the aforementioned requests to exercise the right of access.

4. On the breach of the obligation to respect the right to object

Article 12(2) of the GDPR states that "*The controller shall facilitate the exercise of data subject rights under Articles 15 to 22*".

Article 21(2) and (3) of the GDPR states that "*Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes*".

In light of these provisions, **Recital 70 of the GDPR** states that, with regard to the right to object to the processing of his or her data for direct marketing purposes, "*the data subject should have the right to object to such processing* [....] *at any time and free of charge*".

In this case, the delegation noted that [redacted] carries out marketing operations by post through its partners with customers who have ordered from its website or its paper catalogue.

The delegation noted, on the order form for the French-language paper catalogue, the following statement: "*Si vous ne souhaitez pas recevoir des propositions commerciales de nos partenaires par courrier, merci de cocher cette case*" ("*If you do not wish to receive commercial proposals from our partners by post, please tick this box*") followed by a tick box.

The delegation noted, on the online form, that although the data subjects are informed that they will receive marketing by post from the partners of [redacted], there is no means, such as a tick box, which allows them to object, when providing their data for the order, to receiving further marketing by post.

In this respect, you informed the delegation that data subjects have the possibility of objecting to processing by contacting the DPO via the website contact form or by post.

However, in order to guarantee the effectiveness of the right to object at the time of collection, users of the website should be given the opportunity to exercise this right at the time of collection, for example by ticking a box, in the same way as for the paper order form.

I therefore consider that [redacted] has breached the provisions of Articles 12 and 21 of the GDPR.

5. On the failure to demonstrate compliance of the processing with the GDPR

Article 24(1) of the GDPR states that "*Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary*".

In this case, [redacted] informed the delegation during its hearing in the premises of the CNIL that requests to exercise rights sent by post and the replies provided are not retained by the company once they have been processed. Requests made by telephone are not logged.

In this respect, the investigation of **several complaints**[3] lodged with the CNIL, relating to difficulties encountered by complainants in exercising their right of access and deletion, revealed that [redacted] was unable to provide proof of the responses provided to these requests.

However, pursuant to Article 24 of the GDPR, the data controller is required to implement appropriate technical and organisational measures so as to be able to demonstrate that the processing complies with the GDPR, and in particular to prove that the rights conferred on the data subjects have been respected. It is therefore incumbent on [redacted] to establish the means to provide proof that requests to exercise rights have been properly taken into account.

I therefore consider that [redacted] has breached the provisions of Article 24 of the GDPR.

However, it is clear from the findings carried out during the hearing that the complainants' requests to have their data deleted have been granted.

6. On the breach of the obligation to ensure data security

Article 32 of the GDPR requires that the 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, [...] 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 of the GDPR. For example, it is necessary to ensure that a password used to authenticate to a system cannot be divulged, and the data controller must store user passwords in a sufficiently secure manner to prevent them from being compromised and to protect the personal data that may be consulted and collected when accessing accounts.

Given the current state of the art, the CNIL has set out specific recommendations in its developer's guide[4], recommending that passwords should be stored "*as a hash using a proven library, such as Argon2, yescrypt, scrypt, balloon, bcrypt and, to a lesser extent, PBKDF2*". On the other hand, the MD5 algorithm is a hash function with a known vulnerability that can be immediately exploited by attackers (risk of collision). It has not been considered state of the art since 2004, and its use in cryptography or security is likely to constitute a breach of the obligations of Article 32 of the GDPR.

Furthermore, the implementation of a robust authentication policy is a basic security measure that contributes to compliance with the obligations of Article 32 of the GDPR.

[3] Complaints lodged by [redacted]

[4] CNIL, *Guide RGPD pour l'équipe de développement*, « Fiche n° 6 : Sécuriser vos sites web, vos applications et vos serveurs », https://lincnil.github.io/Guide-RGPD-du-developpeur

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, in order 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 twelve characters including upper case, lower case, numbers and special characters to be chosen from a list of at least thirty-seven possible special characters, or be composed of at least fourteen 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 (for example with a "captcha" system) or the blocking of the account after several unsuccessful authentication attempts (maximum ten).

In this case, the delegation was informed that customer account passwords are stored using the MD5 hash function.

The delegation also noted that creating an account on the "[redacted]" website required entering a password containing at least eight characters, including at least one lower case letter, one upper case letter and one number.

It follows from the above that the storage of passwords in your website's database does not comply with the state of the art at the date of this decision. Consequently, you are required to store passwords using a proven hash algorithm, such as those cited in the CNIL developer's guide.

In addition, the minimum complexity of the passwords protecting access to user accounts on the "[redacted]" website is insufficient with regard to the data processed.

I therefore consider that [redacted] has breached the provisions of Article 32 of the GDPR on these points.

7. <u>On the breach of the obligation to demonstrate collection of the consent of the data subjects for the implementation of electronic marketing</u>

Article L. 34-5 French Postal and Electronic Communications Code states that "*direct canvassing by means of an automated electronic communications system [...], a fax machine or electronic mail using, in any form whatsoever, the contact details of a natural person [...] who has not previously expressed his/her consent to receive direct canvassing by this means is prohibited.*

For the purposes of this article, consent means any free, specific and informed expression of will by which a person accepts that personal data concerning him/her may be used for the purposes of direct marketing. [...]".

Article 4(11) of the GDPR states that, "*consent*" of the data subject means "*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*".

Article 7(1) of the GDPR states that "*Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data*".

In this case, with regard to the complaint lodged by [redacted], the complainant stated that he had not given his consent for his personal data to be processed for marketing purposes by the company or its partners. In this respect, the delegation noted, in the customer database management tool, that the complainant's account had been configured to receive electronic marketing from [redacted] and its partners.

When questioned on this point, the company was unable to prove that it had obtained the consent of the individual in question to receive electronic marketing.

However, pursuant to Article 7 of the GDPR, [redacted] must be able to prove that it has the consent of the data subjects.

I therefore consider that [redacted] has breached the provisions of Article 7(1) of the GDPR, as clarified by Article 4(11) of the GDPR, by configuring its account to enable the processing of personal data for the purposes of electronic marketing without being able to provide proof of the complainant's consent to the processing of this data for such purpose.

II. Corrective measures ordered by the CNIL (Article 20-II of the Act of 6 January 1978)

Due to all these elements and, in agreement with the other data protection authorities concerned by this processing, it is therefore necessary to order the following corrective measures against [redacted]:

1. **A LEGAL REPRIMAND**, in accordance with the provisions of Article 20, II of the Law of 6 January 1978, regarding the obligation to respond to requests to exercise the rights of individuals within the required deadlines, in accordance with the provisions of Article 12 of the GDPR.

2. **AN ORDER TO COMPLY** in accordance with the provisions of Article 20.II of the Law of 6 January 1978, within **three (3) months of notification of this decision and subject to any measures it may have already adopted, to:**

   - **define and implement a policy regarding the retention period for data relating to your company's customers** which does not exceed the period necessary for the purposes for which they are collected, and in particular, to proceed with the deletion of payment card data collected in paper form upon expiry of the applicable limitation period, in accordance with Article 5(1)(e) of the GDPR;

   - **in accordance with Articles 12 and 15 of the GDPR, comply with the conditions for exercising the rights of individuals with regard to their personal data, in particular by:**
     - ceasing to systematically request proof of identity from the person exercising his or her rights where the latter can be identified by other means, unless there is reasonable doubt as to his or her identity;
     - ensuring that the requests to exercise the right of access referred to in referrals [redacted] and [redacted] submitted by [redacted] and [redacted] are complied with;

- systematically informing data subjects that their request to exercise their rights has been taken into account, or, where applicable, of the reasons why their request has not been acted upon;

- **inform data subjects, in accordance with the provisions of Articles 12 and 13 of the GDPR,** by providing them with complete, concise, transparent, comprehensible and easily accessible information, in particular by supplementing the Personal Data Policy with information on retention periods, by making a reference to it on the order form that can be downloaded from the website "[redacted]" and by ensuring that they are provided with this information when ordering by telephone, including on the processing of recordings of telephone conversations;

- **implement a procedure enabling any request to exercise the right to object to marketing by post to be taken into account effectively**, in accordance with Article 21 of the GDPR, and in particular to give users of the company's website the opportunity to exercise their right to object at the time their data is collected, for example via a specific tick box;

- **implement a procedure to provide proof that requests to exercise rights have been properly taken into account,** for example by providing a technical data sheet making it possible to trace requests and the responses provided, which could include the type of request, the date, the categories of data, the types of media and numbers of documents sent, the size of the file, etc., in accordance with Article 24 of the GDPR;

- **take all security measures**, for all processing of personal data that it implements, to safeguard the security of such data and prevent unauthorised third parties from gaining access to it, in accordance with the provisions of Article 32 of the GDPR, in particular by:
  - implementing a restrictive policy relating to the passwords used by website users, particularly in terms of complexity;
  - storing the passwords of website users in a secure manner that complies with the state of the art in this area, in particular by transforming them using a specialised, non-reversible and secure cryptographic function;

- **in the case of** [redacted] in particular, configure his account such that his personal data is not processed for the purposes of electronic marketing or transmitted to partners for this purpose, insofar as [redacted] has not provided proof of his consent to the processing of his data for this purpose, pursuant to Article 7 of the GDPR.

- **provide evidence of the measures taken to the CNIL.**

The above requirements must be complied with in future. If necessary, the CNIL will carry out subsequent inspections and reserves the right to use all the powers granted to it by the GDPR and by the law of 6 January 1978.

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

Finally, I draw your attention to the fact that, pursuant to Article 77(2) of the GDPR, the CNIL is required to inform complainants of the status and outcome of their complaints. In this regard, the shortcomings identified and the type of measure taken against your organisation are brought to the attention of the complainants, who may make public use of them.

For more information on the formal notice procedure, you can consult the CNIL website at: https://www.cnil.fr/fr/la-procedure-de-mise-en-demeure-0.

The CNIL services, [redacted] lawyer in the inspections department and [redacted] lawyer in the complaints department ([redacted] and [redacted] and [redacted] information systems auditor in the inspections department [redacted] are at your disposal for any further information.

Yours sincerely,

[redacted]
Marie-Laure Denis

Copy sent by email ([redacted]) to [redacted] Data Protection Officer of [redacted].