CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

The President

[redacted]
MR PRESIDENT
[redacted]

Paris, April 25th 2024

Our ref.: [redacted]
Formal notice decision No [redacted]
To be stated in all correspondence
By recorded delivery letter No [redacted]

Dear Sir

The [redacted] sells jewellery to private individuals under several brands, including [redacted] manages the Group's activity in France. In particular, it manages approximately [redacted] physical distribution points of the '[redacted] brand and the merchant website of this brand, [redacted].

It has more than [redacted] customers or prospects who have requested a quote on the company's website or via one of its distribution points: the majority reside in France but [redacted] people are in Belgium, [redacted] in Italy, [redacted] in Germany and [redacted] in Luxembourg.

In accordance with Decision No 2022-147C of 29 September 2022, on 18 October 2022 the Commission Nationale de l'Informatique et des Libertés (CNIL) carried out an online inspection of the processing operations accessible from the '[redacted] and '[redacted] domains, which was followed on 27 and 28 October 2022 by an inspection at the premises of [redacted] located at [redacted] and the [redacted] located at [redacted].

The purpose of these inspections was to verify compliance by [redacted] Group and its subsidiaries, including [redacted] with all the provisions of Law No 78-17 of 6 January 1978 ("Loi Informatique et Libertés") and Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 ("GDPR"). In particular, this involved following up on referral No [redacted] relating to the exercise of the applicant's right to rectification, which closed on 23 November 2022.

[redacted] sent the Delegation additional information on 18 November 2022, as well as on 6 January, 2 February, 20 March, 6 April, 2 June and 28 September 2023, to keep it informed of the compliance actions undertaken, such as the designation of a Data Protection Officer to the Commission services on 8 February 2023.

As a result of the observations made and the additional information provided, I have drawn attention to the following points in this decision.

In this respect, it should be noted that, as part of the cooperation procedure, a draft decision was submitted to the authorities concerned on the basis of Article 60 GDPR on XXX.

This project did not give rise to any relevant or substantiated objections.

I. By way of introduction, on the use of tracking pixels by [redacted] and its compliance with Article 82 of the French Data Protection Act

1. On the applicability of Article 82 of the French Data Protection Act to tracking pixels

In law, it follows from Article 82 of Law No 78-17 of 6 January 1978 (LIL) that any operation to read information recorded in a terminal or write in this terminal may only take place provided the user, duly informed, has previously expressed his/her consent. However, such prior consent is not necessary in two circumstances:

- the operations carried out are strictly necessary for the provision of the service requested by the user;
- the sole purpose of the operations carried out is to enable or facilitate communication by electronic means.

Tracking pixels, which enable the sender of the message or any of its partners to obtain information relating to the visit to a web page or the reading of an email by any given user, are images, usually small in size, which are not contained directly in the web page or email but are hosted on remote servers. To display them in a web browser or email client software, a request must be made over the network, using the URL provided in the body of the message. This URL, along with the technical information needed to manage exchanges on the network (e.g. the timestamp), is read on the user's terminal and sent to the server where the image is hosted. The image URL usually includes individualised parameters relating to the user or the context in which the image appears. In response to this call, the image in question is then generally downloaded and written to the memory of the user's terminal, so that the browser or email client can display it.

These elements show that such tracking pixels are used to obtain information about the user and his/her terminal. This information is communicated via the parameters of the request (IP address of the requester, individual name of the image, etc.) and is processed by the server hosting the image, which results in a read and/or write operation on this same terminal, so that the aforementioned Article 82 applies.

Insofar as these operations make it possible to obtain information about the user or his/her terminal for purposes other than those linked to the establishment of an electronic communication, it is up to you to analyse whether the purposes pursued by the use of tracking pixels are really necessary for the operation of the service. Otherwise, users should be informed of the existence of read and/or write operations carried out by means of the pixels inserted in the emails sent (e.g. when the information relating to the sending of emails is presented) and their consent to such operations should be obtained beforehand.

In particular, in the event that the information collected and/or read using this technology is used for advertising targeting, said trackers will be excluded from the exemption from the requirement to obtain consent within the meaning of the aforementioned Article 82.

Lastly, I would like to inform you that the CNIL has launched a consultation to draw up guidelines to define the scope of the exemption from consent for the application of Article 82 of the law of 6 January 1978 to tracking pixels. I invite you to consult the documents tol be put out to consultation at the end of this work.

2. <u>On the presence of tracking pixels in the emails sent by [redacted]</u>

In this case, [redacted] sent the delegation a certain number of commercial prospecting emails sent to its customers and prospects, in particular in its letter of 18 November 2022. The Delegation noted the presence within these emails of images, of the size of zero or one pixel, displayed from a remote server accessible from URLs composed in the form "https://[redacted]**xxx**" or "https://[redacted]**yyy**", **xxx** and **yyy** being unique alphanumeric values for each email.

The delegation noted that no specific consent was obtained from individuals before the insertion of this pixel and that no information was given in advance, either about its purpose or about the means of objecting to it. This information does not appear in the "Personal Data" document on the [redacted] website or in the emails themselves.

It follows from the above that Article 82 is applicable to tracking pixels and it is therefore necessary to verify whether or not consent is required in this case.

3. <u>On the need for prior consent</u>

In its letter of 4 January 2023, your company informed the delegation that "These pixels are used to detect the opening of emails by their recipients (customers or prospects)" and are also involved in "processing for the purpose of analysing [their] behaviour, which includes in particular the behaviour of opening the email". Your company has also indicated that it considers that it is not obliged to obtain the prior consent of the persons concerned for the use of these pixels.

I would like to make the following comments.

Firstly, the first exemption from the requirement to obtain consent set forth in Article 82 of the French Data Protection Act cannot be applied in this case insofar as the purpose described above is not to "enable or facilitate communication by electronic means", as the pixels do not participate in the communication process. Their absence will not prevent the sending or receipt of email.

Secondly, with regard to the second exemption set forth in Article 82 of the French Data Protection Act, I note that the stated purpose (to analyse the recipient's behaviour) does not directly constitute a service requested by the user.

The CNIL considers, however, that certain purposes that are inseparable from the service requested may benefit from exemption from prior consent, in particular when it is a question of ensuring the security of the provision of the service or, under certain conditions, of measuring its audience. In

the case in point, none of the information provided by your company makes it possible to establish how the purpose of analysing the behaviour of the data subject, the recipient of its commercial prospecting emails, is inseparable from the service in question.

Therefore, in this context, I invite you to read paragraphs 12 to 34 of CNIL deliberation No 2020-092 of 17 September 2020 adopting a recommendation proposing practical compliance procedures in the event of the use of "cookies and other trackers" and to **monitor the results of the work on the purposes of tracking pixels that may benefit from an exemption from consent that the CNIL is currently carrying out with organisations representing professionals** and which will enable you to determine any corrective measures that you may have to adopt to enable you, where applicable, to use tracking pixels again depending on the purposes defined.

II. Analysis of the facts in question

1. On the breach of the obligation to process adequate, relevant and limited data

Article 5(1)(c) GDPR provides that personal data must be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')*".

The controller must therefore comply with the principle of minimisation by processing only the data that is necessary for the purposes for which it is to be used.

In the case in point, the delegation noted that if a user of the "[redacted]com" website logged in and initiated a purchase, the delivery address entered during an order was automatically recorded in the "[redacted]" tab of the user's account, even if the purchase was abandoned. The delegation was informed that the purpose of this recording was to "facilitate subsequent purchases made by the account holder on the site".

However, this recording, intended to facilitate future orders, is not justified when the prospect does not ultimately make a purchase likely to lead to the delivery of a good.

I therefore consider that [redacted] disregarded the provisions of Article 5(1)(c) GDPR.

2. On the breach of the obligation to retain the data for a period proportionate to the purpose of the processing

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*".

By way of clarification, in February 2022 the CNIL published a "*Reference framework relating to the processing of personal data implemented for the purposes of managing commercial activities*" which states that "*For commercial activities that involve the creation of an online account by customers [...], the data may be retained until the deletion of the account by the user. However, it is common for users to cease to use these accounts without deleting them, which leads to these accounts continuing indefinitely. In this case, the organisation should determine a reasonable period of time after which the account will be considered inactive and must therefore be deleted. In this respect, a period of two years appears proportionate.*"

In the case in point, the delegation noted that the information document entitled "PERSONAL DATA" specified that the data of persons holding an account on the website "[redacted] was kept for five years from their last positive action, the date of the last order being the only event defined as a positive action in [redacted]s main database.

However, it was found that this database made no distinction between the company's customers and prospects. This database thus contained data on 1,857,508 prospects who had never made a purchase and for whom it was therefore impossible to determine the date of their last positive action. With regard to customers, the inspection delegation also noted the presence of data for 9,486,792 people whose last order was more than five years old and for 6,823,395 customers whose last order was more than eight years old. The delegation was also informed that no automated deletion of data had been carried out within the database.

Thus it appears that the retention periods set for customers had not been complied with and that the data of prospective customers had been kept indefinitely, since no starting point for the retention period had been defined for the latter.

I therefore consider that [redacted] disregarded the provisions of Article 5(1)(e) GDPR.

I note that following the inspection carried out, your company had set a data retention period for prospective customers of three years from their last positive action, defined as the creation of an account on the "[redacted]" website or the request for a quote. Your company also carried out a complete purge of data on customers whose last order was more than five years old and data on prospects whose account was created more than three years ago. I also note that you have set up intermediate data archiving for the purposes of managing disputes and legal obligations.

While these measures now enable your company to comply with the provisions of Article 5(1)(e) above, I would be grateful if you could ensure that these provisions are respected in the future, for example by automating the deletion of data at the end of the set retention period.

In addition, your company told the delegation that it could apply a longer retention period to customers' personal data in certain cases, in particular when customers benefited from a lifetime guarantee on their purchase. I would ask you to carry out a review of these retention periods to ensure that they are limited to what is "necessary for the purposes" specific to these particular cases.

3. <u>On the breach of the obligation of transparency and to provide information to individuals</u>

Article 12 GDPR provides 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 same Regulation sets out a list of information to be provided to data subjects in the event of their data being collected directly. This list includes in particular "*the purposes of the processing for which the personal data are intended as well as the legal basis for the processing*".

In the case in point, the delegation was informed that [redacted] was carrying out commercial canvassing by SMS and email with customers who had made purchases from the [redacted] Group. It also noted that, when making an in-store purchase, customers were asked to fill in an information form which

referred them to the document entitled "PERSONAL DATA" available on the "[redacted] website for further information on processing for commercial prospecting purposes.

However, I note that this document does not include all the mandatory information required under Article 13 GDPR and, in particular, does not inform data subjects of the purpose of commercial canvassing and the corresponding legal basis.

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

4. <u>On breaches of the security obligation</u>

Article 32 GDPR requires 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".*

In the case in point, with regard to access to the databases of [redacted], it was found that [redacted] had used generic accounts shared by nine people for access to the database containing the data of its customers and prospects.

However, the use of non-individual accounts made it impossible to accurately identify users' connections and usage of services.

In the current state of the art, the ANSSI has drawn up specific recommendations in its guide on the secure administration of information systems (https://www.ssi.gouv.fr/uploads/2021/09/anssi-guide-recommandations_architectures_systemes_information_sensibles_ou_diffusion_restreinte-v1.2.pdf), specifying in particular that "*Any person accessing a resource of a sensitive IS must be identified and authenticated by means of an individual account*".

In addition, the documents submitted on 18 November 2022 showed that logging of connections to generic accounts in the database had not been activated and therefore no traceability of access had been implemented.

However, the lack of logging of accesses and connections to information systems makes it impossible, in particular, to identify and contain unauthorised accesses by unauthorised third parties.

By way of illustration, given the current state of the art, the ANSSI has drawn up specific recommendations in its security guide for the architecture of a logging system, which states that the practice of logging is "a technical activity essential to the security of information systems". To this end, the CNIL has adopted a recommendation relating to logging, in which it recommends that "operations involving the creation, consultation, modification and deletion of personal data and information contained in processing operations to which logging is applied should be recorded, including the individually identified author, the timestamp, the nature of the operation carried out and the reference of the data concerned by the operation".

As a result, your security policy does not comply with the state of the art, since there is no traceability of connections.

These facts constitute a breach of the aforementioned Article 32 GDPR. I note that following the inspection, your company deactivated the generic accounts and deployed a single user authentication solution for data access, which logs all database connections. I would therefore ask you to continue to ensure that these provisions are complied with in the future.

III. Corrective measures ordered by the CNIL (articles 20-I and 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]:

- **A REMINDER OF LEGAL OBLIGATIONS,** in accordance with the provisions of Article 20.II of the Law of 6 January 1978, with regard to:

  - **the obligation to retain data for a period proportionate to the purpose of the processing;**

  - **the obligation to ensure data security due to the use of generic accounts to access the database;**

- **FORMAL NOTICE** 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 process only data that is relevant, not excessive and adequate for the purposes pursued, in particular by ceasing to collect the postal addresses of people who initiate a purchase on the company's website but do not complete it;**

  - **to fully inform the data subjects of data processing related to the recording of the delivery addresses of users of the "[redacted]" website, commercial prospecting processing and processing based on the legitimate interests of [redacted] or third parties**, in accordance with Articles 12 and 13 GDPR.

This formal notice, which does not require a response from you, entails the closure of procedure No [redacted]. However, this closure is without prejudice to the right reserved by the Commission to carry out a new verification mission, particularly in the event of new complaints, in order to check that your company has complied with this formal notice on expiry of the time limit.

In the event of a new verification procedure, if your company has not complied with this formal notice, a Rapporteur will be appointed who may ask the Restricted Committee to impose one of the penalties set forth in Article 20 of the French Data Protection Act.

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

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 Commission services, [redacted] and [redacted] are at your disposal for any further information.

Sincerely

[redacted]

Marie-Laure Denis

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

Copy sent by email to Ms [redacted], Data Protection Officer.