CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS
The Chair

Recorded delivery letter
AR ref. no:

[redacted]
For the attention of the Management
[redacted]

Paris, 22 May 2024

Our ref.: [redacted]
Case No: [redacted]
To be quoted in all correspondence

Dear Sir/Madam

As part of the cooperation and consistency mechanism set forth in Chapter VIII of the General Data Protection Regulation (hereinafter "GDPR"),[1] the French Data Protection Authority (CNIL) was asked by the data protection authority of the Land of Bavaria, Germany (Bavarian Lander Office for Data Protection Supervision or BayLDA) to investigate the complaint filed by Mr [redacted] (hereinafter the "complainant") against [redacted] and [redacted] (hereinafter the "companies").

The privacy policy appearing on the website [redacted] designates these companies as co-controllers of the personal data of users of this website, which the companies have not disputed in exchanges with the CNIL.

As the latter are established at [redacted] France, the CNIL is competent to act as lead supervisory authority within the meaning of Article 56(1) GDPR.

1. Reminder of the facts

Following an order placed on the website [redacted] and by email dated 27 July 2022, the complainant sent the companies a request to erase all personal data related to his customer account.

By two separate emails dated 3 August and 23 August 2022, the companies replied that they could only respond to this request on the condition that the complainant sent a copy of his identity document by return email.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJEU L.119.

On 10 October 2022, the complainant replied that he did not wish to provide his identity document but was willing to provide further information to confirm his identity. However, this proposal remained unanswered by the companies.

Considering this request as neither reasonable nor necessary, the complainant referred the matter to the Bavarian Data Protection Authority, which forwarded its complaint to the CNIL under the "one-stop-shop" procedure set forth in Article 56 GDPR.

By email of 20 March 2023, the CNIL contacted the companies, in their capacity as controllers within the meaning of Article 4(27) GDPR, and requested clarification on the reasons why the complainant was asked to provide a copy of his identity document to examine his request for erasure.

In their response of 13 April 2023, the companies explained that, until October 2022, the procedure for managing requests to exercise rights provided for an enhanced identity verification for any request for access, erasure and major modification resulting in a change in the first name and last name of the data subject.

According to the companies, this identification procedure was intended to protect their customers against any fraudulent request that would have harmful consequences for them given the significant risk to their privacy in the event of disclosure or deletion of their personal data. However, the companies specified that between 24 November 2022 and the end of December 2022, a new identification procedure based on the cross-checking of two to three pieces of information previously provided by the person wishing to exercise his/her rights had been put in place for the entire [redacted] network.

The companies added that, as part of this procedure, all the necessary measures to preserve the security and confidentiality of the identity documents collected were taken: firstly, data subjects were informed from their first contact with the companies of the purpose of this verification and the security measures put in place, secondly, no copy or storage of the copy of the identity document was carried out by the companies and, finally, the agents in charge of processing requests for the exercise of rights were regularly trained and made aware of the protection of personal data and bound by an obligation of confidentiality.

With regard to the particular case of the complainant, the companies confirmed that they had deleted his customer account on 13 April 2023 and informed him of this by email of the same day.

By email of 9 May 2023, the CNIL requested clarification concerning the new identification procedure implemented by the companies definitively from January 2023.

In their response of 16 May 2023, the companies explained that since that date, the identification had been based on the confirmation, by the person wishing to exercise his/her rights, of the information previously provided. Thus, for a right of access request, the applicant was asked to recall three pieces of information from the following elements:

- email address,
- postal address,
- phone number,
- date of birth and
- the last purchase made through his/her customer account.

If the applicant is able to confirm the information requested, then his/her identity is considered verified.

The possibility for the companies to request the disclosure of an identity document was ultimately maintained only in two specific cases, i.e. in the case of a request to exercise rights on behalf of a third party and when there was reasonable doubt as to the identity of the applicant who did not provide three of the pieces of information listed above.

The companies specified that when a copy of the applicant's identity document was requested, all the measures previously implemented to ensure the confidentiality and security of this document, as described above, had been maintained

By email of 7 July 2023, the CNIL noted that this new method of verification of the three control points was likely to present a risk to the security of processing since the information requested could easily be provided by a third party.

In response to this concern, the companies explained in an email of 7 August 2023 that they had strengthened the level of security of this identification system by systematically requesting the email address associated with the applicant's user account and sending him/her an email containing a confirmation link. Failing to click on this link, the request will not be considered verified and will expire automatically within 30 days. As a precautionary measure, a reminder is sent 24 hours after the first confirmation email is sent if the applicant has not yet clicked on the link. The companies specify that this new procedure was put in place from 21 July 2023 in France.

In an email of 29 December 2023, the companies specified that the deployment of this new procedure internationally was planned for the first week of 2024.

Finally, as part of the investigation of this complaint, it was noted that the two emails sent by the companies in response to the complainant's request for erasure of 27 July 2022 did not propose to the latter to communicate the copy of his identity document via a secure channel. On the contrary, the responses from the companies of 3 and 23 August 2022 invited the complainant to communicate this document by simple return of email.

In this respect, the companies were reminded that, in the absence of appropriate measures, email exchanges, in particular *via* consumer messaging systems, represented a risk in terms of data security, whether in human terms (handling error, etc.) or technical terms (access to sending and receiving servers, etc.). The transmission of a copy of an identity document therefore requires the use of a secure communication channel or, at the very least, the implementation of additional measures to ensure the security of transfers by email.

When questioned on this subject, the companies indicated in their response of 7 August 2023 that they had introduced, as of 1 August 2023, a new transmission procedure via a secure portal enabling the data subject to download a copy of his/her identity document. After consultation by the team in charge of processing requests to exercise rights, the companies specified that this document was automatically deleted.

The exchanges with the companies lead me to note the following elements.

2. Analysis of the facts in question

2.1. Breach of the principle of data minimisation

Pursuant to GDPR, personal data subject to processing must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Article 5(1)(c) GDPR).

While it is accepted that the controller may request from the person wishing to exercise his/her rights the information necessary to confirm his/her identity (Article 12(6) GDPR), the method used for authentication must, however, be relevant, appropriate and proportionate. In doing so, the controller must take into account the type of personal data processed (e.g. special categories of data or not), the nature of the request, the context in which the request is made, as well as any damage that may result from inappropriate disclosure.

Consequently, the fact that the exercise of a right is systematically conditional on the applicant providing a copy of his/her identity document cannot generally be considered as an appropriate and proportionate means of authentication.

Such a requirement is likely to lead the controller to process excessive data with regard to the purposes pursued.

Several alternative methods may be considered to confirm the identity of the data subject. For instance, in an online context, the authentication mechanism may be based simply on the connection of the applicant to his/her user account. In this circumstance, the latter's entry of his/her username and password is considered sufficient to authenticate him/her without it being necessary to request additional information or to provide a copy of his/her identity document. Similarly, and still by way of example, the identification procedure may consist of asking the applicant about a set of pieces of information previously entered with the controller (account creation date, personal information, information concerning the latest orders, secret question, etc.), provided the combination of pieces of information requested is known only to the applicant.

Consequently, it is only in the event that reasonable doubts as to the identity of the applicant remain that additional information may be requested by the controller to confirm his/her identity.

In this case, it emerges from the information obtained during the investigation that the authentication mechanism initially put in place by the companies had been based on the systematic verification of the identity document of the applicants for any request for access, erasure or major modification of the customer account information. The requests in question therefore concerned data processed in the context of the e-commerce activities of the companies, were part of simple requests to exercise rights (right of access, right to erasure and right to rectification) and did not concern special categories of personal data. Therefore, such a reinforced authentication procedure, given the nature of the data concerned and the context of the request, cannot be considered adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

It was only from January 2023 that a procedure based on the verification of information entered by customers in their user account was put in place throughout the [redacted] network. Since then, a copy of the applicant's identity document has only been requested if, at the end of this first stage of verification, there remains a reasonable doubt as to his/her identity.

In view of the foregoing, I therefore consider that during the period before October 2022, the companies did not comply with the principle of minimisation set forth in Article 5(1)(c) GDPR.

2.2. Breach of the obligation to respond to the request to exercise the right to erasure

Pursuant to GDPR, the data subject has the right to obtain from the controller the erasure, as soon as possible, of personal data concerning him/her (Article 17 GDPR).

The controller is then required to provide the data subject with information on the measures taken following such a request, as soon as possible 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 the number of the requests. The controller will inform the data subject of this extension and the reasons for the postponement within one month of receiving the request (Article 12(3) GDPR).

In addition, if the controller does not comply with the request made by the data subject, it will inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for its inaction and of the possibility of lodging a complaint with a supervisory authority and filing a judicial appeal (Article 12(4) GDPR).

In this case, the complainant refers to a request for erasure sent to the email address [redacted] on 27 July 2022. In response, the companies sent two emails, dated 3 and 23 August 2022 respectively, explaining that the deletion of his customer account required the prior sending of a copy of his identity document.

Subsequently, on 10 October 2022, the complainant wrote to the companies informing them that he did not wish to provide a copy of his identity document but was willing to provide other information to confirm his identity. He received no response from the companies to this second request.

It was only following the intervention of the CNIL, by email of 20 March 2023, that the companies responded to the complainant's request for erasure. Thus the complainant was informed of the effective deletion of his personal data on 13 April 2023, i.e. more than eight months after making his request.

By email of 29 December 2023, the companies explained that this lack of response was due to an error committed by one of their agents during the processing of this second request. However, they specify that their agents have been made aware of this issue so that this situation does not happen again in the future.

Therefore, I consider that by failing to comply with the complainant's request for erasure and by failing to respond to the complainant within the prescribed deadlines, the company breached its obligations under Articles 12 and 17 GDPR.

2.3. Breach of the obligation of security of processing

Pursuant to GDPR, personal data must be processed in a manner that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (Article 5(1)(f) GDPR). Having regard to the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing and the risks to 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 (Article 32(1) GDPR).

In this case, with regard to the communication system provided by the companies for transmitting copies of identity documents, it emerges from the two responses provided to the complainant's request for erasure on 3 and 23 August 2022, that the companies invited him to provide a copy of his identity document by simple return of email.

However, this procedure for the communication of personal data, as it was based on a simple dispatch of an email, represented a significant risk in terms of security, whether from a human or technical standpoint. As indicated to the companies during the investigation, the transmission of a copy of an identity document requires the use of a secure communication channel or, at the very least, the implementation of additional measures to ensure the security of transfers by email.

I therefore consider that this procedure for the transmission of personal data put in place by the companies did not comply with the security obligation set forth in Articles 5(1)(f) and 32 GDPR.

However, I note that the companies have corrected this procedure under investigation by setting up a secure portal enabling data subjects to send a copy of their identity document.

In view of all these factors, and in agreement with the other data protection authorities concerned by this processing which have been consulted, the following corrective action must therefore be issued against [redacted]:

- **A REPRIMAND,** in accordance with the provisions of Article 58(2)(b) GDPR and Article 20.II of Law No 78-17 of 6 January 1978, with regard to the following breaches:
    - breach of the principle of minimisation of personal data;
    - breach of the obligation to respond to a request to exercise the right within a maximum period of one month;
    - breach of the security obligation.

I would like to inform you that in accordance with Article 77 GDPR, the person who referred a complaint to the CNIL behind this case is informed of this decision.

I would add that this decision, which closes the investigation of the complaint referred to above, does not exclude the CNIL from making use, particularly in the event of new complaints, of all the other powers granted to it by the law of 6 January 1978 as amended.

The services of the CNIL ([redacted]) are at your disposal for any additional information.

This decision may be appealed to the Council of State within two months of its notification, increased by:

- one month for persons residing in Guadeloupe, French Guiana, Martinique, Réunion, Saint-Barthélemy, Saint-Martin, Mayotte, Saint-Pierre-et-Miquelon, French Polynesia, the Wallis and Futuna Islands, New Caledonia and the French Southern and Antarctic Lands;

- two months for persons living abroad.

Sincerely

[redacted]

Marie-Laure Denis

Certified copy:

- [redacted] Data Protection Officer, [redacted]