CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Registered letter with acknowledgement of receipt

No. AR: [redacted]

[redacted]
For the attention of the president
[redacted]

File processing:
[redacted]
Ref: [redacted]
Complaint No. [redacted]
(to be included in all correspondence)

Paris, on 18th September 2024

Mr president,

I am following up on the exchanges that have taken place between the services of the Commission nationale de l'informatique et des libertés (CNIL) and [redacted]'s data protection officer, as part of the investigation of Mrs [redacted]'s complaint forwarded by the Spanish Data Protection Authority *(Agencia Española de Protección de Datos)*, in application of the mechanism for cooperation between European authorities pursuant to Articles 56 et seq. of the General Data Protection Regulation (GDPR).

As a reminder, the complainant lodged a complaint against the company [redacted] relating to a security and confidentiality issue in the processing of his personal data.

Indeed, the complainant states that she had sold an item initially purchased on the [redacted] website to a third party through her customer account linked to the [redacted] e-mail address. She states that this third party asked for proof of purchase. The complainant provided her with a copy of the purchase invoice, which showed her surname, first name, address, telephone number and postal address. Using this document, the complainant indicated that this third party would have obtained a refund for the item since it was still under warranty. To do so, [redacted] would have modified the complainant's credit card details. The complainant therefore criticises the company for failing to check the identity of the person requesting reimbursement for the item.

The services of the CNIL contacted the [redacted]'s data protection officer, by letter of 2nd December 2021, to question the company about the facts brought to its attention.

In letters of 22nd December 2021 and 24th April 2022, [redacted] confirmed that this third party had invoked the legal guarantee of conformity for the item in order to obtain reimbursement and, to this end, had provided her bank details. [redacted] acknowledges that it has modified the bank details in the complainant's personal account, replacing them with those of the third party.

Following the intervention of the CNIL, [redacted] indicated in response that it had adopted measures to prevent such a situation from recurring. For example, in the case of a refund request made by a member registered on the [redacted] website, the company said that the member is invited to enter his IBAN directly into his personal account.

With regard to the specific case of warranty claims brought by a third party, the owner of a second-hand item initially purchased on the [redacted] website, the company stated that the request for reimbursement is now forwarded to its accounting department, which makes the reimbursement to the third party by bank transfer. Consequently, refund requests made by third parties are processed without any connection to the personal accounts of the company members who originally purchased the items concerned by the warranty claims.

These facts lead me to remind you that, it is your responsibility as data controller to:

- implement, taking into account the nature, scope, context and purposes of the processing, as well as the varying degrees of risk to the rights and freedoms of natural persons, the appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Article 24(1) of the GDPR;

- implement measures to ensure the ongoing confidentiality, integrity, availibility and resilience of processing systems and services in accordance of Article 32 of the GDPR;

- in the event of a personal data breach, to notify the CNIL of the breach without undue delay and, if possible, no later than 72 hours after having become aware of it in accordance with Article 33 of the GDPR. As part of its security obligations, the data controller shall set up a procedure to manage personal data breaches, with the aim of preventing, detecting and reacting appropriately to limit the risks and avoid future breaches.

You will find more information on these subjects on the CNIL website:

- https://www.cnil.fr/fr/les-violations-de-donnees-personnelles
- https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

In agreement with the other European data protection authorities concerned, in view of the answers provided by [redacted], the measures adopted in the past with regard to the specific situation of the complainant and which the company will undoubtedly adopt in the future in order to ensure the security of the processing operations it implements and, in particular, that the facts which are the subject of the present procedure do not recur, I hereby inform you that this complaint is being closed.

In the event of further complaints, the CNIL reserves the right to use all the powers granted to it by the GDPR and the amended Act of 6th January 1978.

Yours sincerely

For the President of the CNIL and by delegation,

[redacted]

Subject to the applicant's right to bring an action, CNIL decisions may be appealed to the Conseil d'Etat within two months of their notification, extended by:

- one month for residents of 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 Territories;

- two months for people living abroad.