Deliberation n° 46/RECL13/2024 of 26 July 2024 of the National Data Protection Commission, in a plenary session, on complaint file n° 7.439 lodged against the company [redacted] via IMI Article 61 procedure 318600

Having regard to 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 (the '**GDPR**');

Having regard to the Act of 1 August 2018 on the organisation of the National Data Protection Commission and the General Data Protection Regime (hereinafter referred to as the '**Law of 1 August 2018**');

Having regard to the Rules of Procedure of the National Data Protection Commission adopted by Decision No 3AD/2020 of 22 January 2020 (hereinafter referred to as the '**ROP**');

Having regard to the complaints procedure before the National Data Protection Commission adopted on 16 October 2020 (hereinafter referred to as the **'Complaint Procedure before the CNPD**');

Having regard to the following:

I. Facts and procedure

1. In the framework of the European cooperation, as provided for in Chapter VII of Regulation (EU) 2016/679 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 (General Data Protection Regulation or GDPR), the Supervisory Authority of Bavaria (Germany) for the private sector submitted to the National Data Protection Commission (hereinafter: "the CNPD") the complaint of [redacted] (national reference of the concerned authority: LDA-1085.3-2179/21-I) via IMI in accordance with Article 61 procedure - 318600.

2. The complaint was lodged against the controller [redacted] (hereafter '[redacted] who has its main establishment in Luxembourg. Under Article 56 GDPR, the CNPD is therefore competent to act as the lead supervisory authority.

3. The original IMI claim stated the following:

"*The complaint has repeatedly tried to have his personal data deleted such as telephone number, mail address, address, at* [redacted] *This is about a customer account that he hasn't used for more than 7 years.*
On 5.11.2020 various orders via this account were made abusively by an unknown person.This abuse was confirmed in a letter dated 06.11.2020 by [redacted]
Furthermore, a completely foreign bank account was deposited with this customer account. The account was blocked, but not deleted.

The confidence in the security of his data at [redacted] is no longer available. Several times he tried to have his data deleted at [redacted] via the contact on the [redacted] web page, by phone and with 2 letters by registered letter. [redacted] does not comply with this obligation."

4. In essence, the complainant asked the CNPD to request [redacted] to delete his personal data.

5. The complaint is therefore based on Articles Article 5 (1) (f) and 17 GDPR.

6. On the basis of this complaint and in accordance with Article 57(1)(f) GDPR, the CNPD requested the company [redacted] by a first letter to take a position on the complainant's request and confirm whether the complainant's [redacted] account or any of his data processed by [redacted] has been unlawfully accessed and if so, inform the CNPD of the origin, nature and circumstances of the unlawful access, including measures taken to prevent such incidences in the future.

7. The CNPD received the requested information within the deadlines set.

II. In law

1. Applicable legal provisions

8. Article 77 GDPR provides that "*without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, (...) if the data subject considers that the processing of personal data relating to him or her infringes this Regulation*."

9. Pursuant to Article 17 GDPR, a data subject may request the erasure of his or her personal data and the controller must erase the data subject's personal data without undue delay if one of the grounds provided for in Article 17 (1) GDPR applies unless the controller can demonstrate that the processing falls within the scope of one of the exceptions set out in Article 17 (3) GDPR.

10. Article 5(1) (f) stipulates that *"personal data shall be […] processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')*".

11. Article 56(1) GDPR provides that "(…) *the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60*";

12. According to Article 60(1) GDPR, "*The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other*";

13. According to Article 60(3) GDPR, "*The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views*";

2. In the present case

14. Following the intervention of the Luxembourg supervisory authority, the controller confirmed that:
    - The controller was in contact with the [redacted] regarding the suspected unauthorised access to his account in November 2020 and [redacted] specialised team immediately secured the complainant's account, including blocking the complainant's password to prevent further access to the account;
    - The following day, the complainant was informed that his password was deactivated, changes reverted, open orders cancelled and potential payments reimbursed;
    - [redacted] states that it has security software in place to detect fraudulent behaviour and train its customer service agents to assist its customers in case they suspect unauthorized access to their account. [redacted] maintains physical, electronic and procedural safeguards in connection with the collection, storage and disclosure of personal customer information;
    - There are incidents whereby malicious third parties log into a customer's [redacted] account using the customer's [redacted] account login details obtained through illicit means (for example, through a phishing or data theft outside of [redacted] According to [redacted] these events are beyond

[redacted] control, although the company does take multiple measures to reduce the impact of these events on its customers, including through deployment of detection processes that seek to identify irregular account activity, teams that investigate such activity, and steps to remedy incidents proactively;

- [redacted] was therefore unable to determine how the bad actor gained access to [redacted] account. However, [redacted] could confirm that there were no further unauthorized orders since 5 November 2020 and any bad debt on the complainant's account was cleared so that there was no financial damage;
- The complainant sent his request for account closure and data deletion on 7th of November 2020, where the cancellation of the initiated orders starting on 5th of November 2020 was still in progress. This overlap caused a delay in [redacted] systems, since open orders typically mean that an account cannot be closed. The complainant was informed correspondingly by mail on 8th of November;
- On 6th of January 2021, the complainant sent a follow-up request to [redacted] via letter, but the address mentioned in this letter did not match the address connected to the customer account, so that [redacted] customer service was not able to verify [redacted] identity. Therefore, the complainant was referred to the self-service tool in his customer account;
- By 14 January 2021, the complainant explained that he could not access the self-service tool as his account was deactivated. That request was not transferred to the correct team. [redacted] apologised for this error in this case and assured to take steps to remind the relevant teams of how to recognise a request for account closure and data deletion, and how to ensure that these are routed to the correct team.

15. After a second intervention by the CNPD, [redacted] further informed the CNPD that:
    - [redacted] specialist team had unblocked [redacted] account and contacted the latter explaining the exact steps which allowed him to close his account and delete the personal data once he had verified himself as the account holder via log-in;
    - The complainant has made use of this self-service tool and has closed his account on 24 May 2022, thereby initiating the deletion process.

3. Outcome of the case

16. The CNPD, in a plenary session, therefore considers that, at the end of the investigation of the present complaint, the controller has taken appropriate measures to grant the complainant's right to erasure in accordance with Article 17 GDPR as well as his right to integrity and confidentiality, in accordance with Article 5 (1) (f) of the GDPR by securing the complainant's account, i.e. by blocking his password in order to prevent further access to the account, and by deleting his personal data after the complainant had verified himself.

17. Thus, in the light of the foregoing, and the residual nature of the gravity of the alleged facts and the degree of impact on fundamental rights and freedoms, it does not appear necessary to continue to deal with that complaint.

18. The CNPD then consulted the supervisory authority of Bavaria (Germany), pursuant to Article 60(1), whether it agreed to close the case. The Supervisory Authority of Bavaria (Germany) has responded that the complainant has indicated that the case is now closed for him. The CNPD has therefore concluded that no further action was necessary and that the cross-border complaint could be closed.

In light of the above developments, the National Data Protection Commission, in a plenary session, after having deliberated, decides:

- To close the complaint file 7.439 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD and after obtaining the agreement of the concerned supervisory authority.

Belvaux, dated 26 July 2024

The National Data Protection Commission

[redacted]

Indication of remedies

This Administrative Decision may be the subject of an appeal for amendment within three months of its notification. Such an action must be brought by the interested party before the administrative court and must be brought by a lawyer at the Court of one of the Bar Associations.