Deliberation No 60_RECL51_2025 of 26 June 2025 of the National Data Protection Commission, in a plenary session, on complaint file No 9.037 lodged against the company [redacted] via IMI Article 61 procedure 431998

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 (hereinafter: 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: the "**Act of 1 August 2018**");

Having regard to the Rules of Procedure of the National Data Protection Commission adopted by Decision No 07AD/2024 of 23 February 2024 (hereinafter: the '**ROP**');

Having regard to the complaints procedure before the National Data Protection Commission adopted on 16 October 2020 (hereinafter: 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), the supervisory authority of Brandenburg (Germany) submitted to the National Data Protection Commission (hereinafter: the "**CNPD**") a complaint (national reference of the concerned authority: 136/22/0575) via IMI in accordance with Article 61 procedure – 431998.

2. The complaint was lodged against the controller [redacted] (hereinafter: "[redacted] or the "**controller**"), 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:
"*In a letter dated 01.10.2021, the complainant requested information pursuant to Article 15 of the GDPR and deletion of his data pursuant to Article 17 of the GDPR. Thereupon, he received the message that he had to log in to his user account. However, he has not been able to log in to his account, which he has used for years, for some time (oct 2021), as he only uses a landline number and the confirmation by the control number does not work now. He wants to close the account and delete his data. He also complains that no direct contact address is provided for the data protection officer.*"

4. In essence, the complainant asks the CNPD to request [redacted] to grant him access to his personal data and to close his [redacted] account and delete any related personal data.

5. The complaint is therefore based on Articles 15 and 17 GDPR.

6. On the basis of this complaint and in accordance with Article 57(1)(f) GDPR, the CNPD requested [redacted] to take a position on the facts reported by the complainant and in particular to address the complainant's requests with regard to his right of access and his right to erasure, unless there is a legitimate reason to restrict or limit his rights.

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

II. In law

1. Applicable legal provisions

8. Article 77(1) 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. In accordance with Article 15(1) GDPR "*The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information* (...)".

10. In accordance with Article 17(1) GDPR "*The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies* (…)"..

11. In accordance with Article 12(1) GDPR "*The controller shall take appropriate measures to provide* (…) *any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language,* (…). *The information shall be provided in writing, or by other means, including, where appropriate, by electronic means.* (…). Moreover, Article 12(2) GDPR provides that "*The controller shall facilitate the exercise of data subject rights under Articles 15 to 22.* (…)".

12. Furthermore, in application of Article 12(2) GDPR" *The controller shall facilitate the exercise of data subject rights under Articles 15 to 22*". Recital 59 GDPR emphasises that "*Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means.*"

13. 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.*"

14. 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.*"

15. 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

16. [redacted] is authorised as a Bank in Luxembourg pursuant to the Luxembourg Act of 5 April 1993 on the financial sector, as amended. It is subject to the regulatory framework applicable to banks and supervised by the competent national supervisory authority *Commission de Surveillance du Secteur Financier* (CSSF). [redacted] is also subject to the obligation of professional secrecy set out in Article 41 of the aforementioned Act and shall keep secret all information entrusted to it in the context of its professional activity. The disclosure of such information is punishable, under Article 458 of the Luxembourg Penal Code.

17. Following the intervention of the Luxembourg supervisory authority, the controller confirmed that:

- the complainant was unable to log into his [redacted] account because:
  - His account was impacted by a technical error, which prevented successful two factor authentication (2FA) through his chosen method, a landline telephone.
  - The complainant's landline telephone number received a one-time passcode (OTP) but when he entered the passcode, it was subsequently not recognised as valid by [redacted] systems.
  - The complainant did not have a viable alternate two factor authentication method available, for example a mobile telephone number or the [redacted] mobile app.
  - The result of this scenario is that the complainant could not login to use his [redacted] account as he could not meet the Strong Customer Authentication (SCA) requirement to log in.

- When the complainant sent an email to [redacted] on 1 October 2021 exercising his data subject rights using the specific option for non-users or users who cannot login, the response was sent to the Message Centre within his account that is only accessible after successful login. The Complainant's subsequent email did not receive a response.

- A senior [redacted] customer service representative spoke with the complainant on 14 March 2023 and apologised for the inconvenience caused by this issue. The complainant explained that his data access request extended to receiving his account transaction history; this request was immediately fulfilled, and the information was sent to him by email. The complainant's data erasure was triggered when his account was closed on his behalf, and the deletion of his data will be executed after the expiry of the required retention period. [redacted] provided a copy of this communication to the CNPD.

3. Outcome of the case

18. The CNPD, in a plenary session, therefore considers that, at the end of the investigation of the present complaint, [redacted] has taken appropriate measures to grant the complainant's right of access and his right to erasure.

19. 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.

20. The CNPD then consulted the supervisory authority of Brandenburg (Germany), pursuant to Article 60(1) GDPR, whether it agreed to close the case. The supervisory authority of Brandenburg (Germany) has responded affirmatively, so

that the CNPD has 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 9.037 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD and after obtaining the approval of the concerned supervisory authority. As per Article 60(7) GDPR, the lead supervisory authority shall adopt and notify the decision to the main establishment or single establishment of the controller.

Belvaux, dated 26 June 2025

The National Data Protection Commission

[redacted]

Chair Commissioner Deputy Member

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.