



Deliberation No 60_RECL54_2025 of 26 June 2025 of the National Data Protection Commission, in a plenary session, on complaint file No 12.634 lodged against the company [REDACTED] via IMI Article 61 procedure 672852

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 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 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 Brandenburg (Germany) submitted to the National Data Protection Commission (hereinafter: "the CNPD") a complaint (national reference of the concerned authority: 136/24/1345) via IMI in accordance with Article 61 procedure - 672852.
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 main issue is that the complainant's company was asked to provide all its bank statements for the last few months in order to continue using the account."
4. In essence, the complainant asks the CNPD to advise him whether [REDACTED] data processing is lawful.
5. The complaint is therefore mainly based on Article 5 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 provide its analysis in order to demonstrate its compliance with Article 5 GDPR.
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. Article 5 (1) (a) GDPR stipulates that personal data shall be “processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’)”
10. Article 5 (1) (b) GDPR sets out that personal data shall be “collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’)”;
11. Article 5 (1) (c) GDPR stipulates that personal data shall be *“adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).”*
12. Article 5 (1) (d) GDPR stipulates that personal data shall be “accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’)”;
13. Article 5 (1) (e) GDPR stipulates that personal data shall 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

14. 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')"*.
15. 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"*;
16. 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"*;
17. 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

18. [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.

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

- The complainant states that [REDACTED] has asked him to provide his customers account statements coupled with a threat of an account restriction should he not comply with the request. The complainant believed this practice of requesting extensive personal information about his buyers to be disproportionate and extortionate and violates the principles of data minimization and purpose limitation of the GDPR.
- The CNPD has requested that [REDACTED] investigate the matter described by the complainant and provide an analysis in order to demonstrate its compliance with Article 5 GDPR. Furthermore, the CNPD requests a copy of all correspondence between [REDACTED] and the complainant.
- [REDACTED] has identified a business account registered for a private corporation under the email address [email] with the complainant listed as the primary contact and user. [REDACTED] noted that this matter, along with the placement of payment 'reserves', has been the subject of correspondence between the complainant and the CSSF, as well as with his company's solicitor. Previous communications with the complainant primarily related to the placing of payment reserves on the business account, and considerations regarding the privacy of his customers were also mentioned.
- For full context, a 'reserve' is the process of holding funds to off-set potential losses and is a common control measure used across the payment industry. A reserve consists of funds that will remain on the account balance as a form of security to ensure [REDACTED] can cover any potential losses, possibly due to payment reversals, buyer complaints, chargebacks or other payment issues associated with the account. These funds are not available for withdrawal or for payment and it appeared this is the form of 'restriction' to which the complainant referred.
- The complainant claimed that he has been asked to provide his customer account statements coupled with a threat of an account restriction should he not comply with the request. [REDACTED] asserted that this is incorrect, and the complainant was asked to provide the latest bank statements for his company to assess the latest liquidity position and strength of the business, and the possible placement of reserves is not a threat as such. Furthermore, the information about the buyers which is visible on his company bank statement would be minimal — the name of the buyer and transaction information, however, [REDACTED] has no objection in this

Deliberation No 60_RECL54_2025 of 26 June 2025 of the National Data Protection Commission, in a plenary session, on complaint file No 12.634 lodged against the company [REDACTED] via IMI Article 61 procedure 672852

case if the name of the buyer and transaction information is masked as it is the visibility of the cash movements in the bank statements that allows [REDACTED] to understand if there are any large incoming or outgoing movement of funds that would impact its decision to place reserves on his account. [REDACTED] communicated this to the complainant.

- With regard to the principles relating to the processing of personal data, in particular the principle of 'data minimization' - which is the most relevant principle to the subject of this complaint, [REDACTED] is only collecting sufficient information which is necessary to fulfil the purpose of assessing the financial risks associated with the seller's account, and is doing so with a view to determining if the reserves on the account can be reduced.
- A copy of the communication was sent to the CNPD.

3. Outcome of the case

20. The CNPD, in a plenary session, therefore considers that, at the end of the investigation of the present complaint, the controller has demonstrated the lawfulness of the processing.
21. 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.
22. The CNPD then consulted the supervisory authority of Brandenburg (Germany), pursuant to Article 60(1), whether it agreed to close the case. The Supervisory Authority of Brandenburg (Germany) has Since the complainant did not provide them with any feedback within the deadline set for this purpose, they assume that the complaint has been settled to his satisfaction and therefore ask the CNPD to issue a draft decision. 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 12.634 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD and after obtaining the agreement of



**Deliberation No 60_RECL54_2025 of 26 June 2025 of the
National Data Protection Commission, in a plenary session, on
complaint file No 12.634 lodged against the company [REDACTED]
[REDACTED] via IMI Article 61 procedure 672852**

the concerned supervisory. 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

[REDACTED]
Commissioner

[REDACTED]
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.