

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 framework (hereinafter: 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 Procedure for complaints 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:

# Facts and procedure

- 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 Germany (Brandenburg) submitted to the National Data Protection Commission (hereinafter: "the CNPD") a complaint (national reference of the concerned authority: 136/20/1535) via IMI in accordance with Article 61 procedure - 296775.
- 2. The complaint was lodged against the controller (hereafter "manual"), 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 complainant claims to have been victim of a cyber attack. She states that her identity was stolen and the attacker used her personal data for identification (name, address and birthday) to register for a account. The email address, phone number and the bank account details used for registering are not owned by the complainant. The attacker conducted three purchases using the fake account. The complaint tried to contact several times by email and by chat to request the right



of access and deletion of her personal data. Each time she was passed on another way to contact Since she never owned a secount her identity couldn't be verified by sending a text message to a registered mobile phone number."

- 4. In essence, the complainant asks the CNPD to request to grant the complainant's right of access as well as his or her right to erasure.
- 5. The complaint is therefore based on Article 15 and 17 GDPR.
- 6. On the basis of this complaint and in accordance with Article 57(1)(f) GDPR, the CNPD requested the controller to take a position on the facts reported by the complainant and to provide a detailed description of the issue relating to the processing of the complainant's personal data, in particular with regard to the right of access and the right to erasure.
- 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. In accordance with Article 15 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. 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.
- 11. 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."

- 12. 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":
- 13. 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":
- 14. 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

15.	is authorised a	s a Bank in Lu	embourg purs	suant to the L	uxembourg A	\ct
of 5 Ap	oril 1993 on the f	inancial sector	r, as amended.	It is subject to	the regulate	ory
framev	vork applicable	to banks an	d supervised	by the comp	petent natior	nal
superv	isory authority C	commission de	Surveillance of	lu Secteur Fin	ancier (CSSI	F).
	is also subject	to the obligati	on of professio	nal secrecy s	et out in Artic	cle
41 of t	he aforemention	ed Act and sh	all keep secret	all information	n entrusted to	o it
in the	context of its pr	ofessional act	ivity. The discl	losure of such	n information	is
punish	able, under Artic	le 458 of the L	uxembourg Pe	enal Code.		

- 16. The CNPD have requested that address the following points:
- provide further information regarding the background of the case,
- inform the CNPD why did not provide a comprehensive response to the complainant's requests,



- act on the complainant's requests, or provide the CNPD with the reasons that would justify not acting on the requests,
- inform the CNPD of the measures taken following the phone calls of the complainant in May and July 2020 notifying of the abuse of her personal data.
- inform the CNPD of the reason why the complainant was continuously referred to other communication channels in order to obtain help from
- inform the CNPD of the measures taken to ensure that such an incident will not reoccur in the future,
- provide evidence of the response sent to the complainant.
- 17. Following the intervention of the Luxembourg supervisory authority, the controller confirmed that:
- Two separate accounts were opened in the complainant's name on the 20th of May 2020 listing the complainant's name, physical address and date of birth. The bank accounts and email addresses registered to both accounts do not belong to the complainant. 's records indicate that two payments were sent, one using each account, to the same merchant on the 20th and the 25th of May 2021. The bank debits failed for both transactions, resulting in the respective account balances reflecting a negative balance. The complainant alerted that he or she was the victim of identity theft on the 4th of July 2020 and immediately restricted all functionality of the accounts in question and ceased collections activity.
- It appears that the complainant's previous communications were mishandled by
  the customer service representatives who handled her concerns at the time, as
  they did not understand that the complainant was unable to login to the accounts
  in question. While the correct steps were taken in relation to the reported fraud,
  noted that there was an opportunity to address the complainant's questions
  more effectively.
- then telephoned the complainant directly to confirm the details that belong to her and reassure her that appropriate steps were taken to restrict the accounts in question to prevent further use of his or her personal details on the system. The has authenticated the complainant's identity by telephone to facilitate her data access request and to service it. The last provided a direct point of contact and email address should she have any further questions or concerns in relation to her data subject rights. The CNPD was provided with the latest correspondence with the complainant.



#### 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, the controller has taken appropriate measures to grant the complainant's right of access and right of erasure, in accordance with Articles 15 and 17 GDPR.
- 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. Moreover, the CNPD is of the view that the issue has been resolved in a satisfactory manner.
- 20. The CNPD then consulted the supervisory authority of Germany (Brandenburg), pursuant to Article 60(1), whether it agreed to close the case. The Supervisory Authority of Germany (Brandenburg) has responded affirmatively, so that 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 7.093 upon completion of its investigation, in accordance with the Complaints Procedure before the CNPD and after obtaining the agreement 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 17 January 2025

The National Data Protection Commission



## **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.