

Final decision

The present decision refers to the case/complaint of ██████, lodged with the supervisory authority of Germany, Bavaria, (national reference LDA-1085.3-10025/19-I) and submitted to the Luxembourg supervisory authority via IMI under Article 61 procedure 73786.

The complaint was lodged against the controller ██████ (hereinafter “█████”) which has its main establishment in Luxembourg. Pursuant to Article 56 GDPR, the Luxembourg National Data Protection Commission (“CNPD”) is therefore competent to act as lead supervisory authority.

Scope of the complaint and assessment of the case

In the initial complaint on IMI, the complainant stated that further to his request to close his account and to erase the underlying personal data, ██████ confirmed to have processed his request. The complainant however stated that his attempt to verify the actual closure of the account by logging into such account triggered ██████ two-step verification procedure and that in this context he received a SMS from ██████ containing a security code. In the light of the above, the complainant had doubts as to the actual closure of its account and erasure of the underlying personal data.

The complaint is thus based on Article 17.

Based on said complaint, the CNPD requested ██████ to provide a detailed description of the issue relating to the complainant’s data processing as per Article 58.1 a) GDPR, in particular as regards the complainant’s request to erase his personal data and to explain why the two-step verification procedure was still in place for the complainant’s former account.

The CNPD received the requested information within the set timeframe.

Outcome of the case

Following the enquiry by the Luxembourg supervisory authority, ██████ has confirmed that it had already initiated the complainant’s request for account closure and deletion. As a result, the customer account was not further accessible to the complainant, but unfortunately ██████ have not yet been able to delete the phone number used for two-step verification for the complainant’s customer account due to a technical problem.

██████ informed the CNPD that as background, two-step verification adds an additional layer of security to the ██████ customer account. Instead of simply entering the password when signing in to the ██████ customer account, two-step verification requires the customer to enter a unique security code in addition to the password during sign-in. The customer can receive this security

code in a variety of ways depending on the option select during sign-up, including text message, voice call, or authenticator app. If a phone number is used, that number is associated with the customer account and kept for two-step verification purposes.

In the case of the complainant, ██████ encountered a technical problem which prevented the phone number associated with the complainant's account from being deleted. This is the reason why the complainant still received the security code to his mobile phone when he tried to log in. However, ██████ has immediately addressed this issue and have deleted the associated phone number.

Thus, based on the information that was provided, the CNPD is of the view that the issue has been resolved and/or the exercised right has been attended.

As the complaint had only a limited personal impact, the CNPD has consulted the supervisory authority of Bavaria (Germany) to determine whether the case could be closed. The CNPD and the supervisory authority of Bavaria (Germany) agreed that, in view of the above, no further action is required and that the cross-border complaint should be closed.

Notwithstanding the closure of this case, the Luxembourg supervisory authority might carry out subsequent actions in exercise of its investigative and corrective powers regarding the data processing activities in the event of new and/or similar complaints.

A draft decision has been submitted by the CNPD to the other supervisory authorities concerned as per Article 60.3 GDPR (IMI entry number 295836).

As none of the other concerned supervisory authorities has objected to this draft decision within a period of four weeks, the lead supervisory authority and the supervisory authorities concerned shall be deemed to be in agreement with said draft decision and shall be bound by it.

For the National Data Protection Commission