BayLDA Reference	LDA-1085.4-12216/25-T
Recipient SA Reference	EXP202510457
Case transferred via IMI Reference	832341
IMI Case Register	868381
IMI Draft Decision Reference	904175
Date of Complaint	6 June 2025

Data Protection Authority of Bavaria for the Private Sector (BayLDA)
Promenade 18
91522 Ansbach
Phone: 0981/180093 0
Fax: 0981/180093 800
E-mail: poststelle@lda.bayern.de
web: www.lda.bayern.de

Decision

Case description
On 28 May 2025, the complainant received an email from [redacted] informing him/her that there had been unauthorized access to the complainant's personal data through a third-party customer service provider. According to the communication, the data concerned included name, email address, telephone number, gender and date of birth. Although financial data had not been compromised, the complainant considers that this constitutes sensitive personal information that should never have been exposed. Since the incident, the complainant has begun to receive a high number of spam calls, as well as calls in which no one responds. This situation forces the complainant not to answer calls from unknown numbers, which has already caused real harm, such as missing important calls from the bank and the health centre. Furthermore, the complainant complains that [redacted] has not provided sufficient details on how the incident occurred or what specific measures have been adopted to prevent future leaks.

Decision
Notifications of personal data breaches pursuant to Article 33 GDPR are routinely reviewed by our supervisory authority. Whether and to what extent further supervisory measures or investigations are initiated beyond this is decided at our due discretion, taking into account the circumstances of the individual case. As a rule, we do not provide further information on notifications received by us, in particular regarding their specific content or our assessment. We ask for understanding in this regard.

With regard to the security incident concerning [redacted] it can be stated that the controller complied with its obligation to notify the personal data breach within the 72-hour period, and that we conducted a supervisory procedure under data protection law in this context. In the course of this procedure, the technical and organisational measures implemented to prevent similar incidents in the future or to mitigate the potential adverse effects were also explained to us. As already stated above, we do not provide detailed information on this matter.

If, as part of the risk assessment, the controller concludes that there could be a high risk for the data subjects, the controller must provide at least the following information in clear and plain language in accordance with Art. 34 GDPR:

- Name/contact details of the data protection officer or other contact point
- Description of the likely consequences of the data breach
- Description of the protective measures taken and, if required, measures that data subjects can take to protect themselve

The controller is obliged to provide the above information in the event of a high risk. Any additional information about the case is given on a voluntary basis.

According to [redacted] the risk assessment carried out did not identify a high risk to the rights and freedoms of the data subjects. The notification pursuant to Art. 34 GDPR was therefore made as a matter of goodwill and purely as a precautionary measure, and not because of the existence of a high risk in terms of data protection law.

Regardless of whether or not there is a high risk in terms of data protection law, we are unable to act on behalf of the data subject, as the controller is not obliged to provide them with further details about the security incident or the technical and organizational measures taken to prevent future incidents.

To protect against data misuse, we would like to provide the complainant with some basic precautionary measures:

- Monitoring of online accounts.
- Caution with incoming messages (email, SMS, etc.): In particular, messages containing formatting errors, spelling or grammatical mistakes, requests for personal data, or prompts to click on links should be treated with caution. In such cases, it is recommended that the message be deleted—under no circumstances should the included links be clicked. If the message refers to a company that allegedly possesses personal data, that company may be contacted in case of uncertainty in order to verify the authenticity of the message. Please note: Especially where messages contain information that would normally only be available to the data subject and a limited group of persons, they may appear authentic—caution should nevertheless be exercised.
- Caution with file attachments.
- Disabling macros and preventing the execution of active content in Microsoft Office.
- Installation of available security updates.
- Use of unique passwords for all online accounts.
- Where possible, enabling two-factor authentication.
- Use of strong passwords, especially for access to customer accounts with banks, online shops, social media platforms, and email accounts.

With regard to the present complaint, based on the information already available concerning the incident and the investigation already carried out, we currently see no reason to take any supervisory measures beyond the investigation that has already been completed. Therefore, we close the case according to Article 60(7) GDPR.

Ansbach, 27 May 2026