Baden-Württemberg
THE COMMISSIONER FOR DATA PROTECTION AND FREEDOM OF INFORMATION

LfDI Baden-Württemberg · P.O. Box 10 29 32 ·D-70025 Stuttgart

[redacted]

Notification of a personal data breach

Dear [redacted]

Thank you very much for your notification of a personal data breach of February 15, 2019, in which you state the following:

On February 13, around 12.30pm, all employees of [redacted] received an e-mail from the account [redacted] with a PDF attachment. This was reported to IT because the text in the e-mail was in English and this employee otherwise never communicates in English. There was a fake DocuSign link in the PDF with the aim of account phishing.

In the account of [redacted] there was a rule activated in the inbox which deletes all incoming e-mails immediately. Therefore it is to be assumed that the account was compromised and that there is no mail spoofing.

The phishing e-mail sent also went to external e-mail addresses. In total (external and internal) approximately 850 e-mail accounts.

As possible consequence you reported that identity theft may be possible if the recipient has fallen for the phishing attachment.

You explained that as corrective actions the password of the affected account was changed immediately. All employees were informed and the danger of the e-mail was pointed out. All recipients who were read out via the Microsoft log would be informed on the day of the notification.

A support ticket was opened with Microsoft today to identify the attacker via IP.

You write that the personal data breach has been communicated to the data subjects and that it was recommend to delete the e-mail and, in case that the attachment has already been opened and the own account data have been entered there, to change the account password.

The notification had been submitted within 72 hours after having become aware of it and it describes the nature of the personal data breach as well as its likely consequences and the measures taken to address the data breach as required in Article 33(1) and (3) GDPR. Also, the concerned data subjects have been informed as per Article 34 GDPR.

From our point of view, the corrective measures taken by you are in order.

Unless new and relevant findings will occur in this matter, we hereby close the case.

Yours sincerely
on behalf
[redacted]