Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Berlin, 04 September 2020

535.781
631.91
A56ID 75328
CR 82025
DD 137878
FD 148217

Berlin Commissioner for Data Protection and Freedom of Information

Friedrichstr. 219
10969 Berlin

Visitors' entrance:
Puttkamer Str. 16-18

The building is fully accessible to disabled members of the public.

Contact us

Phone: +49 (0)30 13889-0
Fax: +49 (0)30 215 50 50

Use our encrypted contact form for registering data protection complaints:
www.datenschutz-berlin.de/beschwerde.html

For all other enquiries, please send an e-mail to:
mailbox@privacy.de

Fingerprint of our PGP-Key:

D3C9 AEEA B403 7F96 7EF6
C77F B607 1D0F B27C 29A7

Office hours

Daily from 10 am to 3 pm,
Thursdays from 10 am to 6 pm
(or by appointment)

How to find us

The underground line U6 to Kochstraße / Bus number M29 and 248

Visit our Website

https://privacy.de

Final Decision

The Berlin DPA closes the case.

1. Facts concerning the data breach

- **Controller:** Apassionata World GmbH
- **Incident**: Attack on Microsoft Office 365 account of the managing director, phishing mails
- **Date of occurrence**: Unknown
- **Date of acknowledgement of the incident**: 25 March 2019
- **EU/EEA Member States concerned, with the number of data subjects concerned**:
    - Austria: 8
    - France: 5
    - Germany: 207
    - Hungary: 2
    - Italy: 1
    - Poland: 1
    - Portugal: 1
    - Romania: 2
- **Category of data subjects**: Customers
- **Category of the data types/data records concerned**: Email addresses
- **Likely consequences of the violation of the protection of personal data**: Misuse to send phishing emails

2. Description of the data breach from a technical-organizational perspective

Unauthorized persons have gained access to a Microsoft Office 365 account and manipulated settings. How the unauthorized persons obtained the access-data could not be clarified. Possibly the cause was the receipt of a phishing e-mail of the same type, which was later sent from the account that was also affected, requesting the user to enter the login data for Office 365.

3. Description and analysis of the effectiveness of the measures taken to address the personal data breach or to mitigate its adverse effects (Art. 33 (3) (d) GDPR)

The password for the affected account has been reset; the manipulated rules for deleting incoming emails have been removed. In addition, the end devices used were checked. The computers used have (and had at the time of the attack) up-to-date, state-of-the-art virus protection.

Retraining on how to handle e-mails and in particular on the compliance goals of encryption, access control and forwarding control.

4. Communication to the data subjects concerned or public communication (Art. 34(1) or Art. 34(3) (c) GDPR)

The controller has informed all data subjects concerned without undue delay in written form (German, English and French).

5. Technical and organisational security measures that the controller had already taken when the incident occurred, e.g. encryption (Article 34 (3) (a) GDPR)

See 3.

6. Subsequent measures by which the controller has ensured that a high risk to the data subjects concerned is no longer likely to materialise (Article 34 (3) (b) GDPR)

The cause may have been the receipt of a phishing e-mail of the same type, which was later sent from the account that was also affected, requesting the user to enter the login data for Office 365. Such attacks could be made considerably more difficult if measures were taken to strengthen user authentication, such as 2-factor authentication. However, since it is not apparent that a particularly high number or special types of personal data were affected, we do not consider a corresponding requirement to be appropriate. Nevertheless, the controller was recommended to use measures for stronger user authentication such as 2-factor authentication.

The other IT security measures, in particular those of the service provider Microsoft, should generally be considered sufficient.

7. Intended measures by the LSA Berlin DPA

7.1 Intended measures regarding Articles 33, 34 GDPR

In the light of the above-mentioned considerations regarding Articles 33, 34 GDPR, the Berlin DPA closes the case.

7.2 Intended measures regarding data protection violations beyond Articles 33, 34 GDPR

Furthermore, the Berlin DPA has also not identified any data protection violations beyond Articles 33, 34 GDPR.