Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Berlin, 24 March 2021

535.1660
631.257
CR 126887
DD 156313
FD 188955

Final Decision

The Berlin DPA closes the case.

1. Facts concerning the data breach

- **Controller:** AWIN AG (www.awin.com)
- **Incident**: vulnerability in API interface
- **Date of occurrence**: unknown (at the earliest in 2017)
- **Date of acknowledgement of the incident**: 20 March 2020
- **EU/EEA Member States concerned, with the number of data subjects concerned**: total of 309
    - Austria: 2
    - Belgium: 4
    - Denmark: 4
    - France: 17
    - Germany: 106
    - Hungary: 2
    - Ireland: 3
    - Italy: 7
    - Netherlands: 22
    - Norway: 2
    - Poland: 5
    - Portugal: 2
    - Spain: 7
    - Sweden: 7
    - UK: 119
- **Category of data subjects**: customers
- **Category of the data types/data records concerned**: email addresses (no passwords)
- **Likely consequences of the violation of the protection of personal data**: misuse

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

Via an API interface, the above-mentioned personal data could be retrieved for a part of the customer data records. By repeatedly calling up the interface with different search parameters, it was possible to retrieve the personal data of all customer accounts.

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

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)

Immediately after the data leak became known, the corresponding API interface was restricted in such a way that the aforementioned personal data could no longer be retrieved. The data leak was thus permanently closed.

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

All data subjects were informed of the incident by e-mail.

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

Not relevant. However, access to the API interface was also previously transport-encrypted.

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)

See point 3

7. Measures taken by the LSA Berlin DPA

7.1 Measures taken 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 Measures taken regarding data protection violations beyond Articles 33, 34 GDPR

As regards this point as well, the Berlin DPA closes the case, since the data was mainly not sensitive and the underlying technical problem has been solved.