Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

631.285.1

535.1766
IMI (56) 161483
CR 176150
DD 176963
FD 183336

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:** TV SMILES GmbH (online service for quiz games in German language)
- **Incident**: See 2.
- **Date of occurrence**: Between 8. August 2017 and 15 May 2020.
- **Date of acknowledgement of the incident**: 15 May 2020.
- **EU/EEA Member States concerned, with the number of data subjects concerned**: An estimated maximum of 3 million users, of which approximately 96,5 % are German, approximately 2 % Austria and the rest from all over the world. (Specific numbers are not available, as the controller does not generally collect this data).
- **Category of data subjects**: Customers.
- **Category of the data types/data records concerned**: Advertising-ID (IDFA), brand/model of the mobile device (when using the app); partially also name, post/e-mail addresses, phone numbers, date of birth, gender, additional preferences submitted by the user, and usage data of the various services
- **Likely consequences of the violation of the protection of personal data**: Misuse.

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

An unencrypted backup of a database was found in a company controlled public AWS S3 Cloud Storage. The backup was created in August 2017 during maintenance work due to a human error by manual activation. According to the company, this backup should not have been created, stored unencrypted or publicly accessible.

Most of the data sets contained only the advertising IDs issued by mobile operating systems. Although these are to be classified as pseudonyms, they are a comparatively meaningful pseudonym because they are usually permanently connected to a smartphone and thus to the person using it and are also the same across all apps. Users are basically able to prevent the use of the Advertising ID (opt-out solution).

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)

- Deleting the backup
- Blocking of the affected AWS S3 Cloud Storage
- Investigation of all other operated cloud storage. No other personal data with public access was found.
- Written employee information on the necessary security precautions when handling personal data
- A security check was initiated, which did not reveal any indications of unauthorized access and/or misuse of the exposed data.
- Change of all passwords and access codes to the company's own systems and integrated third-party systems.
- extensive deletion of personal data and reboot

The immediate measures taken achieved that the public access to the affected data was terminated. The more far-reaching measures ensure to a sufficient degree that comparable errors will be avoided in the future.

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

The controller informed about the incident with a public announcement on their website at https://www.tvsmiles.de/. It will remain online on the same spot at least until the end of October 2020.

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

The actual data processing of the company was not affected.

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 3.

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.