Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Berlin, 13 July 2020

631.87
535.699
A56ID 74975
CR 82038
RD 129527
FD 135778

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/be-schwerde.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**: Dubsmash Inc. / Mobile Motion GmbH (Software) as sole branch in EU/ EEA
- **Incident**: Offering of personal data hacked at Dubsmash in the Darknet (Dream Market)
- **Time and date of the incident**: unknown
- **Time and date of awareness of the incident**: 8. Feb. 2019
- **Concerned EU-/EEA-member states, each with the number of the affected data subjects**:
    - United Kingdom: 2860348
    - Germany: 2044890
    - Spain: 1624919
    - Italy: 1558241
    - Greece: 703880
    - Czech Republic: 647773
    - Romania: 592149
    - Hungary: 508958
    - Poland: 402999
    - The Netherlands: 378192
    - Belgium: 354687
    - Sweden: 275121
    - Austria: 229702
    - Finland: 223663
    - Portugal: 220004
    - Slovakia: 203469
    - Ireland: 179079
    - Norway: 174624

  - Denmark: 125390
  - Croatia: 105163
  - Bulgaria: 92405
  - Slovenia: 54019
  - Lithuania: 50308
  - Cyprus: 40440
  - Latvia: 36338
  - Estonia: 12952
  - Luxembourg: 11938
  - Iceland: 10423
  - Malta: 9954
  - Gibraltar: 1369
  - Liechtenstein: 596
  - France: 1965728
  - French Southern Territories: 6
  - Vatican: 10

- **Category of data subjects**: Dubsmash users
- **Category of the data types/data records concerned:** User names, passwords, date of birth, telephone number, e-mail addresses and country/language information, if provided by the user
- **Likely consequences of the violation of the protection of personal data:** Disclosure and misuse of the above data

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

The reason why the attackers were able to steal user data and publish it in the darknet could not be determined, partly because no access logs were available at the service provider in the affected period. The compromised database was stored with the Cloud-Hoster Heroku. The access logs to backup data showed no abnormalities. In addition, penetration tests were carried out.

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

The company hired a forensics firm to identify network vulnerabilities, but this was unsuccessful for the reasons mentioned above. In addition, log-in credentials were changed and access controls were reviewed.

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

The concerned data subjects were informed of the incident in writing on 14 February 2019. In addition, press releases were published on the same day (in several languages).

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

The stolen passwords were hashed with PBKDF2-SHA 256 using salt values. A disclosure of the unencrypted passwords on a large scale is therefore hardly possible even with knowledge of the database.

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

Among others, the controller:

- carried out investigations on access control, examining user-accounts and rights management. Access to the authoritative postgres database via the cloud provider's CU was limited to three Dubsmash employees, each of whom has their own personalized accounts.
- erformed forensic examinations of logs, including from Amazon AWS, CloudTrail, Postgres SQL and GitHub, for hints on a possible access to data and their transmission during the period of the alleged data leaks.
    - The Postgres SQL protocols were not available for the November 2018 timespan;
    - The CloudTrail protocols for potential access to the S3-Bucket for the backup of the database showed no accesses and no Data transmissions with regard to the data stored there.
    - The EC2B Backup log information showed for the period of 6. January (only from this date protocols were available) to February 9 (date of analysis) no unauthorised access; no protocol data for November 2018 were available anymore, because the data sets had already been changed by the Linux operating system.
    - The GitHub log analysis showed that there were no suspicious user activities that could lead to unauthorized data transfer from the Postgres database.

Users were advised to change their passwords regularly and to avoid the cross-platform use of passwords. The company has also pointed out additional security measures to prevent the porting of telephone numbers.

A 2-factor authentication was introduced for relevant services. In addition, it is now ensured that all internal communication channels are also TLS encrypted. Also, organisational measures have been taken to ensure that all software components are kept up-to-date on a permanent basis.

7. Measures by the LSA Berlin DPA

Against the background of above considerations regarding Art. 33 and 34 GDPR the Berlin DPA closes this investigation.

Furthermore, the Berlin DPA has not identified any data protection violations.