Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Berlin, 10 June 2020

535.696
631.86
A56ID 74950
DD 109067
FD 131464

Final Decision

1. Facts concerning the data breach

- **Controller**: EyeEm Mobile GmbH (free online platform for sharing photos)
- **Incident**: Offering of personal data hacked at the controller in the dark net (Dream Market)
- **Time and date of the incident**: probably February 2018
- **Time and date of awareness of the incident**: 12 Feb. 2019
- **Concerned EU-/EEA-member states, each with the number of the affected data subjects**:
  - Germany: 54,440
  - Italy: 44,573
  - Spain: 24,232
  - United Kingdom: 24,169
  - France: 20,404
  - Poland: 9,973
  - Netherlands: 8,290
  - Portugal: 7,098
  - Austria: 6,327
  - Hungary: 5,379
  - Romania: 5,017
  - Sweden: 4,303
  - Belgium: 4,299
  - Czech Republic: 3,363
  - Greece: 3,254
  - Bulgaria: 2,496
  - Norway: 2,476
  - Lithuania: 2,459
  - Denmark: 2,354
  - Croatia: 1,888
  - Slovakia: 1775
  - Finland: 1,561
  - Ireland: 1,342
  - Slovenia: 1,274
  - Latvia: 1,271
  - Estonia: 856

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

be Berlin

- Cyprus: 649
- Luxembourg: 405
- Malta: 295
- Iceland: 180
- Liechtenstein: 39

- **Category of data subjects**: customers
- **Category of the data types/data records concerned:** names, e-mail addresses, user account data, encrypted passwords
- **Likely consequences of the violation of the protection of personal data:** Disclosure and misuse of the above personal data

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

An external security auditor (Mauer IT Consulting) identified two possible security vulnerabilities for the data breach: outdated Open-VPN server version, open SSH ports.

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 passwords of affected users were blocked and access tokens (access authorizations created for the respective applications of the users) were deleted. The password hash procedure was changed to Bcrypt. In addition, the security vulnerabilities described under 2. were closed.

These measures will prevent the exploitation of the security gaps found for the future. By resetting all access credentials, the attacker is prevented from further access to accounts that have already been taken over. The measures are considered to be sufficient.

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

The persons concerned were informed about the incident by the controller in several stages, i.e. by two e-mails (in English). In addition, a data protection statement (German/English) was placed on the website of the controller (following our recommendation at least until the end of May 2019).

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

Even before the incident, a salted hash method was used, although SHA1. A bulk decryption of the passwords is therefore more difficult.

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)

See 3.

7. Taken measures by the LSA Berlin DPA

Taking the specific circumstances of the facts determined into account, the Berlin DPA considers the case closed in regard to Art. 33 and Art. 34 GDPR.

Moreover, the Berlin DPA issues a reprimand to the controller with regard to the underlying data protection violation (see attached letter).