Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Berlin, 16 November 2021

535.2907 / 631.447

Final Decision

The Berlin DPA closes the case.

1. Facts concerning the data breach

- **Controller:** Delivery Hero SE
- **Incident**: Due to a manual configuration error at the food delivery service Delivery Hero, stored photos of rejected orders were publicly accessible; on 19,000 photos, the invoice was also displayed. In about 400 of the photos with invoices, the name and telephone number of the person placing the order were also visible. A breakdown by country was not provided.
- **Date of occurrence**: 4 March 2021 – 20 July 2021
- **Date of acknowledgement of the incident**: 20 July 2021
- **EU/EEA Member States concerned, with the number of data subjects concerned**: Bulgaria, Croatia, Cyprus, Czech Republic, Finland, Greece, Hungary, Norway, Sweden, Romania
- **Category of data subjects**: Customers
- **Category of the data types/data records concerned**: Pictures of delivered dishes, partly with customer data (name, phone number, NO delivery addresses)
- **Likely consequences of the violation of the protection of personal data**: Probably little or no consequences, as no unusual accesses and especially no accesses on a large scale to the cloud storage were detected. In addition, only relatively uncritical personal data was affected, in the majority even only images without any personal reference. Possible consequences: Identity theft, unwanted calls

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

Due to a manual configuration error, between 4.3.2021 and 20.7.2021, 170,000 photos of rejected orders stored in a cloud bucket were publicly accessible, on 19,000 of which the receipt was also shown. About 2% of the photos with receipts also showed the name and telephone number of the person placing the order. There are therefore about 400 data subjects. There was no breakdown by country. Retrieving the photos also required knowledge and manipulation of the corresponding URLs.

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)

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

- Erasure of the cloud bucket, moving the data to a storage that cannot be accessed without authentication.
- Checking all other buckets for faulty configuration
- 4-eyes principle for the configuration of access rights has been implemented
- Automated analysis of the photos to see whether the photos contain a receipt and whether personal data can be read on the receipt.
- In the future, the company will draw customers' attention to the fact that such receipts should not contain any personal data when using the app function for uploading pictures.

We consider the measures to be sufficient and effective.

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

Notification of the data subjects is not mandatory, as there is no high risk due to the non-critical data and it is unlikely that unauthorised access to personal data has occurred.

No read logging was (inadvertently) set up on the bucket (cloud storage area), so no object-level analysis is possible. However, coarser data traffic analyses did not show any anomalies such as large-scale data retrievals.

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

For services and other storage, automated erasure rules generally apply for erasure after 6 months. In the present case, however, this functionality had not been activated by mistake.

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. Intended measures by the LSA Berlin DPA

In the light of the above-mentioned considerations, the Berlin DPA closes the case.