Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

Berlin, 30 April 2020

535.1014
631.125
IMI A56ID 92258
DD 110613
FD 122414

**Final Decision**

1. **Facts concerning the data breach**

   - **Controller**: Delivery Hero SE
   - **Description of the data breach:** see 3.
   - **Time and date of the incident**: 15 July 2019, 18:00 o'clock
   - **Time and date of awareness of the incident**: 15 July 2019, 20:00 o'clock
   - **Affected data subjects**: 1446 employees in the EEA, of which 1035 are in Germany
     - Delivery Hero SE (Germany): 1035
     - Click Delivery SA (Greece): 98
     - Online Delivery AE (Greece): 43
     - Delivery Hero Austria GmbH: 100
     - Delivery Hero Finland: 24
     - Foodora Finland Oy: 7
     - Foodora AB (Sweden): 21
     - Foodora Norway AS: 46
     - Foodpanda Bulgaria Ltd: 40
   - **Category of the data types/data records concerned:** login credentials for the in-house communication platform
   - **Likely consequences of the violation of the protection of personal data:** Takeover of work-related platforms through password guessing

2. **Measures taken by the LSA Berlin DPA**

   The case has been closed. In support of this, we refer to the statements under 3 - 6, where it is pointed out that the data subjects concerned were informed of the incident.

3. **Cause of the data breach**

   Due to a faulty configuration of the development environment by an employee, a token for the in-house communication platform Slack was published on the Internet. Due to the publication of the token, personal data of the employees' login credentials were publicly accessible for a short time. The token was tested in the development

**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

environment and was to be imported into Slack to make a technical change. This is where the error occurred.

**4. Security measures taken by the controller at the time of awareness of the data breach**

After the data protection violation became known, the token in question was immediately revoked. This meant that the contents of the token could no longer be accessed. Furthermore, all security measures were analysed again. No further vulnerabilities in the default settings could be identified.

**5. Technical and organisational measures that the controller has taken to address the data protection violation**

The Tech Department was assigned to another data protection and information security training course, which took place on 24 July 2019. In addition, random samples of the data published on the Internet were examined for publication. This would be an indicator that other people have seen and downloaded this data or forwarded it to other third parties.

**6. Analysis of the effectiveness of these measures, especially with regard to prevent a new data breach in the future**

Both the immediate measures taken (token deactivation) and the subsequent measures can be considered sufficient.

**7. Examination of the underlying data protection violation**

The case has been closed, as it is a minor violation due to a technical fault that is not expected to have serious consequences for the data subjects concerned.

The temporary publication of the information on the Internet can only have resulted in third parties gaining knowledge of who works for the controller and its subsidiaries. The technical error was quickly remedied; the responsible department received follow-up training in data protection law.

Further damage is not foreseeable for the time being, or can only be achieved with additional effort.

The company has contacted the Berlin Commissioner for Data Protection and Freedom of Information to report a violation of the protection of personal data. An unlawful processing of personal data has not taken place, since the token itself does not represent a personal datum, but can only provide access to this data like a key. There was therefore a security risk for the data concerned. Since, to our knowledge, this is not a structural defect or a problem that is likely to recur, we do not see any urgent need for action. Nor is the breach itself serious enough to warrant the imposition of a fine. As

this is not a complaint, we are not obliged to take any action against the company.