Berliner Beauftragte
für Datenschutz
und Informationsfreiheit

535.1764
631.283
CR 160663
DD 160668
FD 189177

Berlin, 24 March 2021

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:** Hotel Lützow
- **Incident**: Employee revealed the log-in data for booking.com
- **Date of occurrence**: 13 May 2020
- **Date of acknowledgement of the incident**: 13 May 2020
- **EU/EEA Member States concerned, with the number of data subjects concerned**:
    - Belgium: 23
    - Bulgaria: 6
    - Denmark: 40
    - Germany: 882
    - Estonia: 11
    - Finland: 25
    - France: 101
    - Greece: 25
    - UK: 192
    - Ireland: 20
    - Italy: 185
    - Croatia: 2
    - Latvia: 14
    - Lithuania: 12
    - Malta: 12
    - Netherlands: 81
    - Norway: 11
    - Austria: 31
    - Poland: 55
    - Portugal: 31
    - Romania: 19
    - Sweden: 26
    - Slovakia: 2
    - Slovenia: 20
    - Spain: 167
    - Czech Republic: 10
    - Hungary: 21
    - Cyprus: 1

Total: 2033

- **Category of data subjects**: Customers with bookings for the timespan between 15 May 2019 and 31 May 2021
- **Category of the data types/data records concerned**: First name, last name, telephone no., nationality, date of arrival and departure, partially credit card no. (without security number)
- **Likely consequences of the violation of the protection of personal data**:

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

An attacker was given access to the booking.com account of the controller person for about 4 hours. The access data was obtained by a call from the attacker to an employee of the controller, whereby the attacker pretended to be an employee of booking.com. The employee provided the access data by telephone.

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)

- Blocking of the account by boooking.com within 4 hours after the access data has been obtained.
- Changing the access data
- Training of the controller's employees by booking.com.
- Data protection audit by the company's data protection officer

The Berlin DPA considers the measures taken to be sufficient.

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

The data subjects concerned were notified in writing, some of them initially by e-mail. Finally, the controller published a data protection notice on his homepage (German, English, Italian).

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

Booking.com has a system that attempts to detect potentially problematic account accesses. This system has also resulted in the prompt verification and blocking of the account.

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. Taken measures by the LSA Berlin DPA

7.1 Taken measures regarding Articles 33, 34 GDPR

In the light of the above-mentioned considerations regarding Articles 33, 34 GDPR, the Berlin DPA proposes to close the case.

7.2 Taken 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.