Berlin Commissioner
for Data Protection
and Freedom of Information

631.119.2
A56 81640
CR 427592
DD 427633

09 September 2022

Final Decision

1. Core information on the Data breach

- Controller: Care.com Europe GmbH (provider of care services/household help)
- Incident: Unauthorized access to an email inbox of a senior employee with known access data.
- Time of incident: January 26 and 28, 2019.
- Time of awareness of the incident: January 28, 2019.
- EEA member states affected, each with number of data subjects there: See attachment for details
- Category of data subjects: Platform users, employees
- Category of data types/data sets concerned: Primarily (business) contact data; otherwise: Copy of ID (1 data subject in Romania), correspondence with police forces in UK and Germany due to police investigations (1 data subject in Germany, 2 data subjects in UK).
- Probable consequences of personal data breach: Misuse of the above data

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

Access to an e-mail box (online Outlook) of an employee with known access data. The origin of the access data could not be determined.

Berlin Commissioner for Data Protection and Freedom of Information (BlnBDI)
Friedrichstr. 219, 10969 Berlin
Visitors' entrance: Puttkamerstr. 16-18

Phone: +49 30 13889-0
Fax: +49 30 215 50 50

Office hours: Daily from 10 am to 3 pm, Thursdays from 10 am to 6 pm

Mail: mailbox@datenschutz-berlin.de
Web: www.datenschutz-berlin.de

BERLIN

3. Description and analysis of the effectiveness of the measures taken to remedy the data breach or mitigate any negative consequences
(Article 33 (3) d) GDPR)

The company has had the security leak comprehensively investigated, also by involving third parties. In this way, it was possible to limit the scope of unauthorized access to the online Outlook mailbox of an employee. The manipulations to the mailbox (e-mail forwarding) were reversed within 2 hours of the unauthorized access and access to the mailbox was blocked. In addition to resetting the data subject's password, 2-factor authentication was implemented for all employees.

The measures described above are sufficient to prevent unauthorized access in the future. Microsoft's Office online services also offer a sufficient level of IT security.

4. Notification of the data subjects or public announcement
(Article 34 para. 1 or Article 34 para. 3 lit. c) GDPR)

The 4 data subjects mentioned on point 1 (7th indent) were notified in writing. Apart from that, notification was not necessary (no high risk and see points 5 and 6 below).

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

See 3.

6. Subsequent measures by which the controller has ensured that a high risk for the data subjects is unlikely to persist (Article 34 (3) (b) GDPR)

Use of 2-factor authentication for all employees*.

7. Measures intended by the lead Berlin DPA.

Against the background of the above considerations regarding Article 33, 34 GDPR, the Berlin DPA proposes to discontinue the procedure and to close the case.