Berlin Commissioner
for Data Protection
and Freedom of Information

521.14742.12

IMI (56) 305223
IMI CR 308303
IC 394904
DD 430832

11 September 2023

Final Decision

Reprimand
Our hearing of 1 March 2022; your letter of 20 September 2021.

Dear Sir or Madam,

We hereby reprimand your company for an infringement of the General Data Protection Regulation (GDPR).

Justification:

Our decision is based on the following considerations:

I.
We have established the following facts:

Berlin Commissioner for Data Protection and Freedom of Information (BlnBDI)
Alt-Moabit 59-61, 10555 Berlin
Visitors' entrance: Alt-Moabit 60

Phone: (030) 13889-0
Fax: (030) 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

The complainant is employed by your subsidiary [redacted] as a [redacted] She is the contact person and supervisory body for the riders' safety at work. As part of this, she receives and sends confidential e-mails, for example from the Norwegian Occupational Health and Safety Authority.

Since the complainant set up her company e-mail address on a new, private device on 21 January 2021, access to her account was initially blocked. In order to grant her access again, [redacted] HR department submitted a ticket to you. Your central IT department then reset the password of the account and sent the new password to the complainant's supervisor. Furthermore, the IT department created so-called backup codes which were sent to the HR department. In addition, only the complainant's device was authorised for the e-mail address. Only with both passwords on the complainant's device should it be possible to access the account again. The supervisor forwarded the password to the complainant's private Gmail address within seven minutes. She did not receive the backup codes at first, but only after your data protection team was called in.

Access to the account by other persons did not take place during this period.

II.
Legally, we assess the facts of the case as follows: Your company has infringed Art. 32 of the GDPR.

There must be a functioning process for how passwords are transmitted securely and directly to the recipient. Passwords must also be transmitted to the respective employees via a secure channel. End-to-end encrypted messenger services are an example of a suitable transmission channel.

Just as important as the protection of the password is the protection of the second means of authentication, the so-called backup codes, which replace the second factor for a single login. All that is known, is that other employees or positions at the controller were involved in this.

The access data should not, as happened here, be sent exclusively to superiors and the HR department. In this case, it is possible that other persons in the company have access to both components for access and thus to the account. It must therefore be ensured that at least one of the two components is transmitted directly to the data subjects, as described above. Such direct transmission is associated with a low level of effort. A reference to the contact point to be used for this purpose can, for example, be stored in the ticket for the password-reset.

III.
As a result, we have decided not to take any further supervisory measures due to the infringement, but to leave it at a reprimand.

The reprimand is based on Art. 58 (2) (b) GDPR.

Taking into account the specific circumstances of the established facts, we consider a reprimand to be appropriate after the conclusion of our investigation.

In the certain expectation that you will comply with the data protection regulations in the future, we consider the matter closed.

[Information on legal appeal not translated]