

GZ: D084.2680
2023-0.417.694Case handler: [REDACTED]
[REDACTED]

Notification of personal data breaches to the supervisory authority (Art. 33 GDPR, "Data Breach Procedure")

[REDACTED] (A56ID 290800)

FINAL DECISION

Subject: Discontinuation of the procedure

By notification dated 17 March 2021 and subsequent notifications dated 25 March 2021 and 4 May 2021, [REDACTED], [REDACTED] and [REDACTED] (controllers), represented by [REDACTED], informed the AT DPA that they were reporting a personal data breach.

[REDACTED] is the parent company of the two Austrian subsidiaries [REDACTED] and [REDACTED]. [REDACTED] operates the entire IT landscape.

In summary, a **ransomware attack** occurred on 15 March 2021 at [REDACTED], [REDACTED] and [REDACTED]. The attacker abused an MS Exchange vulnerability. The incident led to an **encryption of data**. The company [REDACTED] was commissioned with a forensic investigation of the incident.

In total, about 3,000 suppliers (B2B contacts) and about 250 employees were affected by the incident.

Regarding the suppliers, data of the categories

- Name
- Address
- Telephone number
- E-mail address
- Bank details

and regarding employees, data of the categories

- Name
- Address
- Telephone

- E-mail address
- Bank details
- Health insurance number
- Application documents
- Proof of citizenship
- Passport
- Registration form
- Birth certificate
- Proof of education
- Marital status
- Degree of disability, if applicable
- Religious Confession

were affected.

The forensic investigations have shown that neither personal data were stolen nor unauthorized persons had access to personal data. There was no particular 'traffic' on ██████████'s data line during and after the attack, which is why it could be assumed that no data had been stolen.

The controller has taken the following measures to remedy the injury or mitigate possible adverse effects:

- Forensic investigation
- Information to the affected employees of ██████████ and ██████████
- Implementation of patches with regard to the vulnerability
- External back-ups

The controller has taken appropriate steps to minimize the risk and to eliminate, as far as possible, the adverse consequences of the security breach. Further measures of the Data Protection Authority as of Art. 58(2)(e) GDPR (order the controller to communicate a personal data breach to the data subject) or § 22(4) DSG (order in case of risk) are not required.

The procedure is therefore terminated and this is finally brought to the attention of the controller.

7 August 2023

For the Head of the Data Protection Authority:

██████████