Republik Österreich
Datenschutz behörde

Barichgasse 40-42
A-1030 Vienna
Tel.: + 43-1-52152 [redacted]

E-mail: dsb@dsb.gv.at

GZ: D085.067
2021-0.787.597

Clerk: [redacted]

[redacted]

Notification of personal data breaches to the supervisory authority
(Art. 33 GDPR, "Data Break Procedure")
[redacted]

by e-mail

Subject: Cessation of the procedure

By notification of 21 August 2021 and the follow-up notifications of 15 September 2021 and 10 November 2021, [redacted] controllers), represented by [redacted], informed that they reported the breach of the protection of personal data.

In summary, it was found on 21 August 2021 that the companies' IT systems were the target of a massive "cyber attack", apparently by means of so-called crypto-lockers. At night, domain controllers and file servers were encrypted.

A very large part of the encrypted data of the controllers can be restored from backups. Some files, mainly accounting data and only very limited personal data, have been downloaded by the polluters.

The forensic investigations found that the polluters used the tools [redacted] and [redacted]

Overall, the following groups of people were affected by the incident:

- Employees (active and former)
- Independent trade agents/representatives appointed by the responsible persons
- Business customers (shoe dealers) with whom the responsible parties are in business relations
- Recipient/sender of correspondence stored on the e-mail server

The persons responsible have around 150 employees in Austria. It is expected that around 3,000 (company) customers are affected. Data from consumer customers (especially from the webshops) are not affected.

Data of the categories

- E-mail systems of the responsible persons:
  - E-mail addresses of the employees of the responsible persons
  - E-mail addresses of recipients of professional correspondence (mainly representatives of corporate customers)
  - Data contained in e-mail correspondence (business correspondence)
- ERP system:
  - Contact details of contact persons of corporate customers
  - (individual) Order data from individual contractors
- Fileserver:
  - Accounting data (e.g. expense statements; not, however, payroll)
  - Employee lists
  - (individually) employment contracts
  - Commercial Agent List
  - Passport copies stored in the [redacted]
  - Other data that employees had stored on the local memory of their work equipment (there is no indication to date that this would include sensitive personal data)

was affected by encryption.

Data of the first controller has been downloaded, this relates to data relating to personal data of the categories

- List of employees; it contains names, address and contact details, birth dates, social security numbers; this also applies to former employees whose data is still stored due to legal retention obligations or legitimate retention interests;
- Individual service contracts; this includes names, addresses, birth dates, social security numbers, data on KV classification and the salary agreed upon;
- List of commercial agents; analogous to employee lists, but without storing the respective social security number;
- Customer database (shoe dealer); this includes company and contact details, order history (only for individual companies to be considered personal data);
  - Copies of the identity of officers and members of the board of directors, who, however, are provided with a watermarked notice for storage by the respective controllers and the purpose of use (e.g. visa application or [redacted] notification), and

- Personal data, which have either been communicated by the data subjects by e-mail or have been stored privately by the data subjects themselves (employees) despite prohibited private use. According to current findings, the latter concerns a very small group of people.

The controller has taken the following measures to remedy the injury or mitigate possible adverse effects and to prevent such incidents in the future:

— Shutting down all servers

— Disconnect all network connections

— Analysis of the incident by IT specialists and forensics from Austria and Germany, assisting them in reducing the impact of the attack, restoring the systems and identifying the causes of the breach

— Close contact with those affected and on-going information about the level of knowledge

— Recovery of affected data (especially from backups)

— Reimbursing a criminal complaint

— Investing in Cyber Security

— Employee training

— VPN access only with two-factor authentication

The controller has notified the data subjects in accordance with Art. 34 (1) GDPR.

The controller has taken appropriate steps to minimise the risk and to eliminate the adverse consequences of the security breach as far as possible. Further measures of the Data Protection Authority iSd. Art. 58 para. 2 lit. e GDPR (instruction) Notification of data subjects) or § 22(4) DSG (mandatory notice in case of risk in default) are not required.

The procedure before the Austrian Data Protection Authority is therefore finalised and to conclude this is brought to the attention of the controller.

16. Mai 2023

Für die Leiterin der Datenschutzbehörde:

[redacted]