Republik Österreich
Datenschutz
behörde

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

E-mail: dsb@dsb.gv.at

GZ: D155.049
2022-0.699.832

Desk Officer: [redacted]

Notification of personal data breaches to the supervisory authority
(Art. 33 GDPR, "Data Break Procedure")
[redacted]AD56ID 180318)

Via IMI

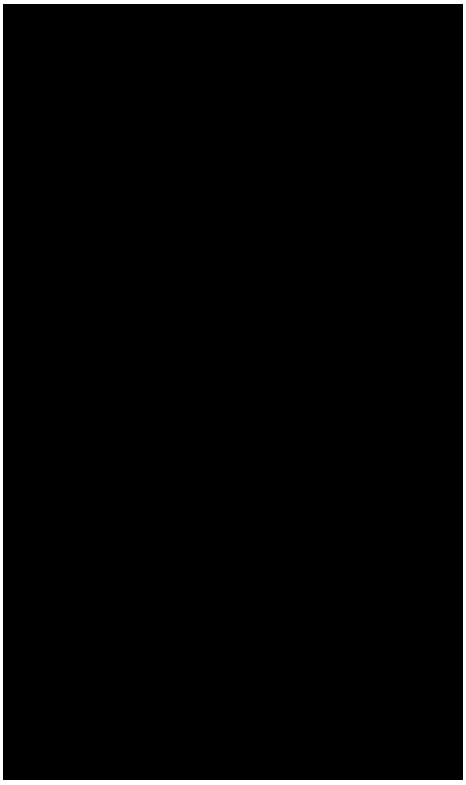
Subject: Closing of the procedure

By notification of 26 January 2021 and the follow-up notifications of 21 February 2021 and 13 April 2021, [redacted] (controller) informed that it was reporting the personal data breach.

According to the controller, on 24 January 2021 (date of knowledge: 25 January 2021) it came to the effect that the controller was the target of a cyber attack. By means of "cryptolockers", the data of the controller's systems were encrypted. Encryption affected the systems [redacted]. The servers of these systems would contain employee data from [redacted] branches in [redacted]. Personal data of customers, suppliers, interested parties, business contacts and employees would be affected.

To the knowledge of the controller, the databases concerned did not contain sensitive data pursuant to Article 9 GDPR or credit card information. Furthermore, there would be no indication from the system logs that these databases were copied or transferred and that no increased data transfer to the outside could be detected. In addition, the analysis of the transmission protocols of the firewalls involved showed that there was no increased external traffic during the period of the attack. Therefore, consulted experts would assume that there was no data outflow. The systems have been restored after payment of the requested ransom.

Only with regard to employee data, there is an indication of possible access. There are 6729 employees with the following country distribution:



In this respect, an Article 34 notification has been issued and the staff have been informed.

They are employee data of the categories

- First name
- Last name
- Company
- User name
- Company e-mail address
- Company Phone Number
- Position
- Department

that were affected.

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

- Reset all passwords
- Introduction of “multifactor authentication”
- Review of admin roles
- Instruction of the staff.

The controller has taken the following measures to prevent such incidents in the future:

- Extension of the controllers “data governance tool”

- Introduction of “change audit tools”
- [redacted]
- [redacted]
- Training of IT employees
- Training of employees with IT access
- Development of extended guidelines for the use of IT.

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 pursuant to Article 58(2) GDPR is not required at this moment. The Data Protection Authority reserves the right to conduct a data protection review in accordance with Article 58(1)(b) GDPR in the future.

The procedure will therefore be closed and this will be brought to the attention of the responsible parties.

16.6.2023

On behalf of the Head of the Austrian Data Protection Authority:

[redacted]