Republik Österreich
Datenschutz
behörde

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

E-mail: dsb@dsb.gv.at

GZ: D155.030
2023-0.216.359

[redacted]

«Anrede»
«Titel»«Vorname» «Nachname» «Nachgestellter_Titel»
«Name»
«zH»

«Straße» «ON»
«Postleitzahl» «Ort»
«Land»

[redacted] (A56 ID145641)

by e-mail «emailadresse»

**Subject: Final decision, termination of the procedure;**

1. By notification of 8 July 2020 and the follow-up notifications of 20 July 2020, 19 October 2022, 18 November 2022, 5 January 2023 and 2 February 2023, [redacted] announced that it is reporting the personal data breach.

[redacted] operates a virtual machine with a web server and a web application from [redacted], which is used for the registration of event participants of [redacted] According to a contractual agreement dated July 5, 2018, the server will be administrated and maintained by [redacted]. This company has its registered office at [redacted], Germany.

The event participants would have the opportunity to register via the web application. These registrations would then be transmitted (after the end of the registration phase) via an interface to other systems of [redacted]. This could then, for example, make a printout of lists of participants.

The data would then no longer be needed in the web application and would be deleted from the database after successful transmission to [redacted]. However, this function appears to have not been implemented or incorrectly implemented by [redacted]. It should be noted that the main database was not attacked, but the table of the web interface responsible for recording the bookings. After booking, the data would be transferred to the main database and deleted from the temporary tables.

As a result, it would be on 2 July 2020 (date of knowledge: 6 July 2020 at 9:15 a.m.) that due to a programming error (data storage, form apparently vulnerable to SQL injection) data could have been read from the system. [redacted] was informed of this error by an external person who claimed an amount of 1,500 bitcoins. If this amount is not paid, the person would inform the data subjects and at the same time sell the data. They are affected by event participants. In total, there are between 2,232 and 2,239 datasets. The discrepancy between the number of data sets should be explained because seven of them were double-registered and were not corrected in the original census of 8 July 2020. A dataset counts for a data subject.

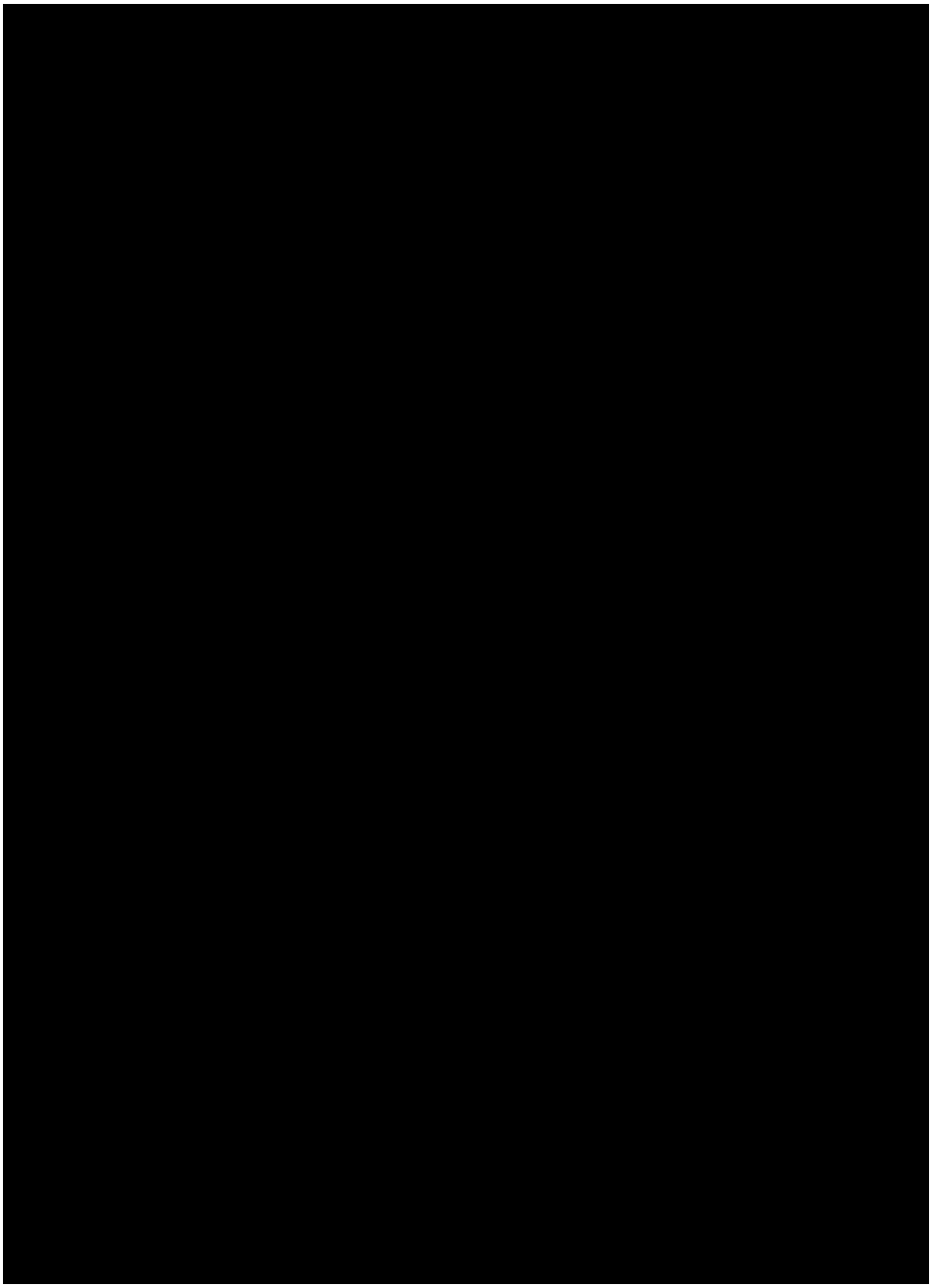
36 records are credit card data, but on the one hand no CVV or CVC numbers have been stored and the validity period expired between 2013 and 2017.

The systems concerned were updated by the manufacturer and the security gaps were closed. The underlying system components have been updated. The system has also been rebuilt to eliminate any installed backdoors. The previous system has been archived for any further analysis purposes. A deletion is scheduled for July 2023.

In accordance with Article 33(2) of the GDPR, [redacted] has contacted the persons responsible both by telephone and by e-mail. No person responsible has given instructions to notify the data subjects. There is also no feedback from some. [redacted] does not have the information as to whether the controller himself has turned to the data subjects. It should also be noted that the data sets are relatively old data.

2. A two-page statistics were also provided in the annex to the opinion of 8 July 2020, in which the number of persons concerned appears country-specific and in the follow-up notification of 18 November 2022 a list of responsible organisers was included. The reporter had processed the data for the following controllers (organisers):

In total, about 2,232 people were affected by the incident. Country-specific data subjects are to be divided as follows:



They are the data of the categories

- Name, company, professional contact details (email, telephone)
- Name and date of events attended
- 36 credit card numbers (which expired between 2013 and 2017)
- Passwords for older version of the registration portal
- Records (datasets from 2013; Expiry date no later than 11/2016)
- Datasets (in use until 05/2015)

it was affected.

3. Based on the submission, the data protection authority assumes that the reporter of the data breach pursuant to Article 33 GDPR is the processor and not the controller. First of all, this is apparent from the fact that on 19 October 2022, the reporting agent, [redacted], claimed not to be the controller of the processed personal data. Similarly, on 19 October 2022, the latter sent an opinion containing an e-mail showing that [redacted] inquired about the further course of action and asked whether the persons concerned had to be informed.

In the present case, as already stated at the beginning, the reporter of the data protection breach pursuant to Article 33 GDPR is a processor and not the controller. In accordance with Art. 33 para. 2 GDPR, this has informed the persons responsible by telephone and by e-mail.

In the absence of a responsible status of the reporting agent (in accordance with Art. 4 Z 7 GDPR) and especially since the latter has complied with the legal obligations pursuant to Article 33(2) GDPR, the procedure was therefore terminated. The initiation of proceedings against the controllers mentioned above is currently being examined.

***Genehmigungsdatum***

Für die Leiterin der Datenschutzbehörde:

I.A. ***Genehmiger(in)***