KISTERS AG
Pascalstraße 8+10
52076 Aachen
Germany
Tel. +49 2408 9385 -0
Fax +49 2408 9385 -555
E-mail: info@kisters.de
Internet: https://www.kisters.de

KISTERS AG

KISTERS AG · Pascalstraße 8+10 · 52076 Aachen · Germany

KISTERS Business Partners
Attn. Data Privacy Officers

Unser Zeichen
hjs
Ansprechpartner
Dr. Heinz-Josef Schlebusch
Telefon
+49 2408 9385 -226
E-Mail
schlebusch@kisters.de

Datum
17. Nov. 2021

Dear Sir or Madam,

You have been named to us as a data protection officer for one or more of our business partners. In order to comply with our duty as a data processor to inform you, we hereby notify you about a possible data protection incident in connection with the cyber attack on KISTERS AG.

1. Type of notification (Art. 33 para. 4)
New notification

2. Data processor (Art. 4 N0. 8)
Name: KISTERS AG
Street: Pascalstraße 8+10
City: 52076 Aachen, Germany
Phone: +49 2408 9385-0
E-Mail: info@kisters.de

3. Point of contact for further information (Art. 33 para. 3 lit. b)
Data Protection Officer
Name: Dr. Heinz-Josef Schlebusch
Street: Pascalstraße 8+10
City: 52076 Aachen, Germany
Phone: +49 172 7181 829
E-Mail: datenschutz@kisters.de

4. Becoming aware of the violation of the protection of personal data
In the night of Nov. 11, 2021, KISTERS AG became the target of a malware attack. The presumed time period of the data data breach is Nov. 10, 2021, between 21:00h and 23:00h. External IT security experts were immediately called in to investigate the incident. In the course of the ongoing forensic investigations, indications emerged yesterday, **Nov. 16, 2021**, that personal data of our clients, which we process or have stored on our IT systems as part of

our services as a data processor, could also be affected by the breach of the protection of personal data.

5. Description of the personal data breach
Nature of the personal data breach (Article 33(3)(a), Article 4(12))
Response: Unauthorized access, data loss
Explanation: According to the current state of the investigation, it cannot be ruled out that there was unauthorized access to and possibly also loss of data files of our clients that contain personal data. It also cannot be ruled out at present that this data has been deleted or downloaded by the group of attackers.
How did the personal data breach occur?
Response: Hacker attack (Virus/Trojan/Phishing)
Explanation: Based on current knowledge, it is not yet possible to say how the attacker group gained access.
Who or what triggered the personal data breach?
Response: Person with intent to harm

6. escription of data subjects and data
Categories of data subjects (Art. 33(3)(a))
Response: persons whose personal data is processed or stored on KISTERS IT systems as part of the provision and execution of our services and for whom our clients are data controllers within the meaning of the GDPR (Art. 4 No. 7):

- Data from productive KISTERScloud systems that are operated for our clients as SaaS or ASP solutions in our data center;
- Data from system images, database dumps, log files or similar, which have been transmitted to us by our clients for the purpose of system analysis or troubleshooting as part of our consulting or support services;
- Data transmitted to us by our clients via our ticket systems or e-mail as part of our support services.

Categories of data concerned (Art. 33(3)(a))
Response: The categories of data concerned depend on the specific application used and the individual use by our clients.
Approximate number of data subjects (Art. 33 Para. 3 lit. a)
Response: Based on our current knowledge, no number can be given yet.
Approximate number of data sets affected (Art. 33 Par. 3 lit. a)
Response: Based on our current knowledge, no number can be given yet.

7. Consequences of the personal data breach
What are the likely consequences of the personal data breach for the data subjects (Art. 33(3)(c)) ?
Response: Identity theft, fraud, loss of control of their personal data.
Explanation: According to the current state of affairs, the breach of integrity and confidentiality of the personal data concerned is possible. Further explanation is not possible at this time.
Based on current knowledge, what is the likely risk to the rights and freedom of data subjects (Art. 33(3)(c))

Response: Risk
Explanation: The severity of the possible consequences for data subjects depends on the categories of the data processed or stored in the specific applications concerned. A more extensive risk assessment can only carried out by the Data Controller.

8. Measures to remedy or mitigate the personal data breach
What measures to remedy the personal data breach has the Processor taken or proposes to take (Art. 33(3)(d))?
Response: The entire KISTERS IT infrastructure has been disconnected from the public network. Currently, large parts of the IT infrastructure are still encrypted by the attacker group, which is why further remediation of the personal data breach cannot yet be undertaken. After becoming aware of the attack, KISTERS commissioned a qualified APT response service provider in accordance with the German Federal Office for Information Security (BSI) to perform an in-depth forensic investigation. To this end, KISTERS is in close contact with the service provider and data protection officer. The service provider has been on site at KISTERS since Nov. 12, 2021 to perform data backups and evaluations. An evaluation of log and metadata as well as other logs and records that could reconstruct the attack is currently not yet available. As a countermeasure and reconnaissance, KISTERS would like to conduct a full digital forensic investigation as previously stated.
KISTERS is also in communication with law enforcement and has filed criminal charges against the cyber attack.
Customers, prospects and business partners have already been notified of the cyber attack through currently available information channels.
In addition, a temporary website with up-to-date information and relevant notices has been set up (www.kisters.de), through which we continue to inform all parties concerned.

Best regards,

Dr. Heinz-Josef Schlebusch
CISO & DPO, KISTERS Group