WORTMANN
TELECOM GMBH

terra

Appendix 3

Technical and organisational measures according to Art. 32 GDPR of WORTMANN TELECOM GmbH:

1. Preamble

The legislator has stipulated in Art. 32 Para. 1 of the GDPR (General Data Protection Regulation) that the measures for securing the data processing operations of commissioned data processing must be complied with. In the event of non-compliance, the client must expect severe fines up to and including a ban on data processing. WORTMANN TELECOM GmbH (hereinafter: Contractor) supports the Client in complying with these legal requirements by enabling the Client to implement the legal requirements of Art. 32 para. 1 GDPR with these General Terms and Conditions for Data Protection.
32 (1) GDPR.

2. Confidentiality (Art. 32 para. 1 lt. B GDPR)

Access control

Measures to prevent unauthorised persons from gaining access to the data processing systems used to process personal data:

The premises and the building are monitored by cameras around the clock. The videos are stored in accordance with the
stored in accordance with the security concept. There are motion detectors that switch on the lights outside and trigger an alarm inside. Outside of operating hours, security guards for buildings are employed by external service providers. Windows and doors are alarm-protected. The alarm system is connected to the police. The building with administrative rooms is fenced in and locked outside of operating hours. Visitors (including technicians and customers) can only access the company via the control centre. The doors to the supplier entrance to the data centre are unlocked from here for access by authorised and registered persons. According to the service instructions, visitors and service providers are never alone in the building and always wear a visitor badge or service provider badge. Every visitor must register at reception. Access by external persons is logged at this point. All technicians and customers must register their visit 24 hours in advance so that the legitimisation of the visit can be checked. Unattended access to the building (for employees only) is via RFID tokens in combination with a password / PIN in the data centre building and via an electronic door system with PIN in the main building.

Access to the data centre

The server systems are operated in our own data centre, TERRA CLOUD GmbH, in the main building area. Access to the stairwell (to the housing area) is barred. Motion detectors and cameras provide additional security for this area.

Access to the server corridors in the Housing area is via tokens/PINs, which are managed centrally. The allocation of RFID tokens is subject to a documented authorisation process. (TERRA CLOUD employees have a master key for emergencies, which is kept locked away). All doors within the data centre sound an alarm if they remain open for longer than the permitted period (a few seconds). This status is monitored on the video wall.

The contractor's server room has no connection to the outer shell of the building. Access to the

WORTMANN TELECOM GmbH
Hankamp 2
32609 Hüllhorst
Germany

Fon +49 5744.944-4500
Fax +49 5744.944-4519
Mailinfo@wortmann-telecom.de Web
www.wortmann-telecom.de

Local court Bad Oeynhausen,
HRB 14584
FinA Lübbecke 331/5886/0508
VAT ID No. DE301288295

Managing Director
Siegbert Wortmann
Stefan Bollmann

Bank details
Volksbank Bad Oeynhausen-HF e.G
IBAN DE40 4949 0070 7106 4263
00 BIC GENODEM1HFV

The contractor's server room is logged automatically. All access logs are stored in accordance with the retention period of the security concept. Daily inspections are carried out (attention is paid to possible problems and changes).

Housing access

Access is via RFID & PIN as well as additional keys to the cage. Access is logged. The individual server cabinets are surrounded by a cage. The key to the cage is held by the administrative team at WORTMANN AG.

Access to rooms for (hardware) support

Access is via an electronic door lock system using a PIN. Access is logged.

Access control

Measures to prevent unauthorised persons from using the data processing systems and procedures:

All internal WORTMANN AG systems are connected to an Active Directory. The access points are specially secured and have special password requirements:

- At least 8 characters
- Consisting of upper and lower case letters, numbers and special characters
- Change every 90 days
- Passwords must not consist of names, words or keyboard patterns

If the user is inactive, the screen lock must be activated as specified. All systems are connected to the outside world via redundant Internet lines (supplied from 2 federal states). These connections are secured by several central firewall systems. The rules of these firewalls are revised at short intervals. The firewalls are maintained externally by a professional provider and monitored both internally and externally. This ensures that attacks are automatically recognised at an early stage. The various network areas are separated from each other via VLANs. In addition, there is an upstream firewall that takes effect for connections from/to the outside.

Access control

Measures to ensure that those authorised to use the data processing procedures can only access the personal data subject to their access authorisation:

There is a user-related authorisation concept that is implemented in the Active Directory. The implemented authorisation structure relates to the company's entire system: The authorisations can be differentiated for files, data records, application programs and the operating system and restrict read, change and delete rights. This ensures that each user can only access the data that they are authorised to access. The authorisation concept, which is based on the positions of the employees, is recorded in writing (documentation via the Active Directory). Furthermore, the authorisation concept is stored in the application in the Active Directory. All user access is logged.

WORTMANN TELECOM GmbH
Hankamp 2
32609 Hüllhorst
Germany

Phone +49 5744.944-4500
Fax +49 5744.944-4519
Mailinfo@wortmann-telecom.de Web
www.wortmann-telecom.de

Local court Bad Oeynhausen,
HRB 14584
FinA Lübbecke 331/5886/0508
VAT ID No. DE301288295

Managing Director
Siegbert Wortmann
Stefan Bollmann

Bank details
Volksbank Bad Oeynhausen-HF e.G
IBAN DE40 4949 0070 7106 4263
00 BIC GENODEM1HFV

The systems are very differentiated in terms of the need for access by employees. Every access by an employee is logged. Protection against external unauthorised access is provided by the use of multi-level firewall architecture and network segmentation.

Separation control

Measures that ensure that data collected for different purposes can be processed separately.
The separation requirement is implemented for the spatial separation of housing (server) and the backup system (extra line), whereby these each represent a separate fire compartment. For particularly critical systems, the backup data is also stored in a second location.
In the housing, the cabinets and servers are installed within a cage. The backup system has its own power supply and is secured by 256-bit AES encryption. The password used is only known to the administrators of WORTMANN AG and cannot be reset or read by external persons.
Systems and programmes are used that enable the necessary client separation or implement the database principle of separation via access regulations. Test and production environments or test and production data are separated from each other.

Pseudonymisation

Personal data is processed in such a way that the data can no longer be attributed to a specific data subject without the use of additional information, provided that this additional information is stored separately and is subject to appropriate technical and organisational measures.

3. Integrity (Art. 32 para. 1 lit. B GDPR)

Transfer control

Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorised persons during electronic transmission or during transport or storage on data carriers, and that it is possible to check and determine to which bodies personal data is to be transmitted by data transmission equipment.
The public IP addresses are maintained and assigned by specially trained employees. The VLANs are also only maintained by specially trained employees. An administration team from WORTMANN AG is responsible for maintaining the systems.

There are separate networks for different system areas. These are separated from each other by VLANs. Indirect patching is carried out via WSUS. In addition, server systems with various applications are supplied with updates by a central management system. Furthermore, a central virus scanner is used and systems are scanned using centralised scanning software.

In the Office system, virus protection is implemented on all computers, centrally in the firewall, on the mail server and on the internal servers. The entire virus scanner and the entire configuration are maintained centrally.

Defective or no longer required data storage media will be disposed of by a certified disposal company. In the context of maintenance or warranty claims, customer data carriers are temporarily stored in a secure area until they are handled according to the order.

The use of private data carriers is technically prevented by deactivating the interfaces (USB) on client systems. Exceptions are subject to a logged authorisation process and these client systems are subject to additional technical checks (central scanning software) and logging.

When using transport companies or transport in general, data carriers or systems with data carriers are packaged in such a way that damage to them can be ruled out as far as possible. A verification procedure for dispatch (e.g. accompanying note, dispatch note) and receipt by the recipient (e.g. confirmation of receipt) is used.

Regular backups are made of all critical systems. Physical backups are created as an encrypted stream and stored in another fire compartment where they can be accessed electronically. Encryption of the backup data records is mandatory and is carried out by the customer. The passwords for the encryption are only known to WORTMANN AG and cannot be read or reset by external persons, e.g. the manufacturer of the backup software.

Input control

Measures that ensure that it is possible to subsequently check and determine whether and by whom personal data has been entered, changed or removed from IT systems.

All access to the management systems is logged. Major and/or critical configuration changes are carried out, logged and archived via a project management process.

To ensure input control, the log mechanisms and transaction logs provided by the software manufacturer are available for logging all inputs for all applications. As part of order and support management, the history log and logging of activities included in the system are available.
Logging of activities is available.

4. Availability and resilience (Art. 32 para. 1 lit. B GDPR)

Availability control

Measures to ensure that personal data is protected against accidental destruction or loss.
Backups are carried out according to a backup plan. The backups of all critical systems are located in separate fire compartments. For some critical databases, these are also located in a 2nd location.
location.

The servers are supplied with power via a ring feed. This is contractually guaranteed to the company.

The company uses a redundant uninterruptible power supply (UPS) with integrated lightning and surge protection devices. The effectiveness of the uninterruptible power supply is automatically tested once a quarter. The UPS can supply the entire
data centre with power for 20 minutes. An emergency power generator, supplied by a diesel tank with a capacity of five days, is available to provide additional power in the event of a power failure. The emergency power generator is tested for effectiveness once a month.

The connection to the Internet is realised via two different, physically separate lines from two different federal states.
two different federal states. The two lines are not crossed.

The server rooms are cooled using air cooling for up to 90% of the year. Two air conditioning systems are operated redundantly for this purpose. Both systems are interconnected so that both passive cooling surfaces of the chillers are available. Moisture and leakage sensors are installed throughout the building to protect against water. The company also has water collection trays at all necessary points and drainage systems and drains on the property. There is also a 60 cm high raised floor in the server areas.

The extinguishing system is an N2 extinguishing system with a fire alarm system and early fire detection. The fire alarm system has a direct connection to the fire brigade. There are also special fire extinguishers on site. Regular inspections are carried out by the fire brigade to ensure further fire protection. The fire brigade also conducts regular training courses on extinguishing fires in the data centre.

A centralised patch management system with a physically separate test environment is used. The critical server systems run in a RAID network. Critical systems for order data processing are redundant.

5. Procedures for regular review, assessment and evaluation (Art. 32 para. 1 lit. D GDPR; Art. 25 para. 1 GDPR)

Data protection management

Measures through internal organisation that ensure compliance with data protection requirements and obligations.
pplications of data protection.
When joining the company, employees confirm instructions on data protection obligations, among other things, via a confidentiality agreement. Recurring annual training courses are held on internal organisation and compliance with instructions, followed by a test. Proof of the training is available in the form of a record of its implementation by the employee.

The data protection officer for WORTMANN TELECOM GmbH has been appointed in writing and the data protection officer's specialist certification is available. The data protection officer of WORTMANN TELECOM GmbH is available at https://www.wortmanntelecom.de/de/impressum.

WORTMANN
TELECOM GMBH

terra

Incident response management

This process is defined as part of emergency management. In the course of the annual training communicated or updated to all employees as part of the annual training.

Data protection-friendly default settings (Art. 25 para. GDPR)

Systems are configured in such a way that only the necessary data for data processing is recorded/requested.

Order control

Measures that check that the service provider complies with the client's instructions when processing personal data.
There is a formalised order management system with written contracts and agreements. In the case of (hardware) support services, the handwritten notes or telephone instructions of the customer are taken as the basis for the contractual activities after checking the permissibility of the commissioned data processing.

Service providers are carefully selected according to the level of their technical and organisational measures, among other things. If necessary, security measures are defined which the service service provider must implement. All service providers are audited once a year by the contractor.

WORTMANN TELECOM GmbH
Hankamp 2
32609 Hüllhorst
Germany

Fon +49 5744.944-4500
Fax +49 5744.944-4519
Mailinfo@wortmann-telecom.de Web
www.wortmann-telecom.de

Local court Bad Oeynhausen,
HRB 14584
FinA Lübbecke 331/5886/0508
VAT ID No. DE301288295

Managing Director
Siegbert Wortmann
Stefan Bollmann

Bank details
Volksbank Bad Oeynhausen-HF e.G
IBAN DE40 4949 0070 7106 4263
00 BIC GENODEM1HFV