WORTMANN
TELECOM GMBH

terra

Annex 3

Technical and organizational Measures, Art.32 GDPR of WORTMANN TELECOM GmbH:

1. Preamble

The legislator has (General Data Protection Regulation) arranged in Art. 32 para (1) of the GDPR that the measures to safeguard the data processing operations of data processing are be observed.
The client has to count with disregard of this with sensitive fines up to the prohibition of data processing.
WORTMANN TELECOM GmbH (hereinafter referred to as „Contractor") supports the client in complying with these legal requirements by enabling the client with this General Privacy Policy to implement the statutory requirements of Art. 32 para (1) GDPR.

2. Confidentiality (Art. 32 (1) according to GDPR)

Entry control

Measures to prevent unauthorized persons from gaining access to the data processing equipment also used to process personal data:

The grounds and the building are camera-monitored around the clock. The videos are saved according to the retention period of the security concept. There are motion detectors that switch on the lights outside and trigger an alarm inside. Outside the operating hours, external service providers provide Security guards. Windows and doors are alarm-protected. The alarm system also has a connection to the police.
The building with administrative rooms is fenced and locked outside of working hours. Visitor access to the company is coordinated (including technicians and customers) exclusively through the head office. The doors to the supplier's approach to the data center are unlocked from here for the access of authorized and registered persons. According to the service instructions, visitors and service providers never move around the building alone and permanently carry a visitor badge or a service provider badge. ALL visitors must register at the reception.
The access logging of ALL visitors is done here. All technicians and customers must register their visit 24 hours in advance so that the legitimacy of the can be verified. Unattended access to the building (for employees only) is via RFID token combined with a password/PIN in the data center building and an electronic door system with PIN in the main building.

Access to the data centre

The server systems are in our data center, in the TERRA CLOUD GmbH Housing area. Access to the staircase (to the housing area) is barred. Motion detectors and Cameras additionally protect this Area.

Access to the server corridors of the Housing area is via tokens / PIN, are managed centrally. The allocation of RFID tokens is subject to a documented authorization process. (Employees of the Terra Cloud have a master key for emergencies that is securely locked away). All doors within the data center will alert if they are open for longer than the allowed time (a few seconds). This is monitored on a video wall.
The server room of the contractor has no connection to the outer skin of the building. Access to the server room of the contractor is automatically logged. All access logs are stored according to the retention period of the security concept. There are also daily security patrols (attention is paid to possible problems and changes).

Access Housing
Access is via RFID & PIN as well as additional keys to the cage. All access is logged. The individual server cabinets are surrounded by cages. The key to the cage lies with the administrative team of WORTMANN AG.

Room access for (Hardware) Support
Access is via electronic door lock system via PIN. All access is logged.

Access control

Measures to prevent unauthorized persons from using the data processing equipment and procedures:
All internal systems of WORTMANN AG are connected to an Active Directory. The accesses are particularly secure and have special requirements for the passwords:

- Mind. 8 characters
- Consists of uppercase and lowercase letters, numbers and special characters
- Change every 90 days
- The passwords can 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 (which are supplied from 2 federal states). These connections are secured by several central firewall systems. The rules of this firewall are revised at short intervals. The firewalls are maintained externally by a professional provider and monitored internally and externally. This ensures early automatic attack detection. The different network areas are separated by VLAN. In addition, there is an upstream firewall, which accesses connections to/from external.

Access control

Measures to ensure that data collected for different purposes can be processed separately.
There is a user-related authorization concept that is implemented in Active Directory. The authorization structure implemented relates to the entire system of the company: The authorizations can be differentiated to files, to data records, to application programs and the operating system, and to restrict the read, change and delete rights. It ensures that each user can access only the data to which he has access. The authorization concept, which is based on the positions of the employees, is recorded in writing (documentation about the Active Directory).
Furthermore, the authorization concept is programmatically in the application, stored in the Active Directory. All user access is logged. The systems pay close attention to the need for employee access. All access by employees is logged. Protection against external unauthorized access is achieved by using multi-level firewall architecture and network segmentation.

Data processing

Measures to 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), each of which represents a separate fire section. For particularly critical systems, the backup data are additionally stored in a second location.
In Housing, the cabinets and servers are installed inside a cage. The backup system has its own power supply and is secured by 256-bit AES encryption. The password used is only known by the administrators

of WORTMANN AG and cannot be reset or read by external persons.
Systems and programs are used which enable a necessary client separation to implement the database principle of separation via access regulations. Test and production environments or test and production data are separated from each other.

Pseudonymization

The processing of personal data takes place in such a way that the data can no longer be assigned to a specific data subject without the need for additional information, provided that such additional information is kept separate and subject to appropriate technical and organizational measures.

3. Integrity (Art 32 (1) of the GDPR)

Transfer control

Measures to ensure that personal data cannot be illegally read, copied, altered or removed during electronic transmission or during their transport or storage on data carriers, and that it is possible to verify and determine to which places a transfer of personal data by institutions intended for data transmission.
The public IP addresses are maintained and assigned by specially trained employees. The VLANs are also maintained only by specially trained employees. An administration team of WORTMANN AG ensures the maintenance of the systems.
There are separate networks for different system areas. These are separated from each other by VLANs. Indirect patching is done via WSUS. In addition, server systems with different applications are supplied with updates by a central management system. Furthermore, a central virus scanner is in use or systems are tested via a central scanning software.
With 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 configuration are centrally controlled.
The disposal of defective or no longer required data carriers by a certified disposal company. As part 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) to client systems.
Exceptions occur through a logged approval process and these client systems are subject to additional technical checks (central scanning software) as well as logging.
When using transport companies or general transport, data carriers or systems are packed in such a way that damage to this can be excluded where possible. A proof procedure over the dispatch (for example accompanying note, dispatch note) as well as the receipt with the receiver (for example receipt confirmation) is used.
Regular backups of all critical systems are created. Physical backups are created as an encrypted stream and kept electronically accessible in another section of the fire. The encryption of the backup data sets is obligatory and takes place by the customer. The passwords for encryption are known by WORTMANN AG and cannot be accessed by external persons, e.g. Manufacturer of the backup software, read out or reset.

Access control

Measures to ensure that it is possible to subsequently verify and determine whether and by whom personal data has been entered, altered or removed from computer systems.
Access to the management systems is logged. Large and/or critical configuration changes are made, logged and archived through a project management process.

To ensure input control, there are the log mechanisms and transaction logs brought by the software manufacturer for logging all input for all applications. As part of order or support management, the log of the activities brought in the system or logging is available.

4. Availability and resilience Art. 32 para. 1 GDPR
Availability control

Measures to ensure that personal information is protected against accidental destruction or loss.
EBackups are performed according to a backup plan. The backups of all critical systems are in separate fire protected sections. For some critical databases, these are additionally in a second location.

The power supply of the server is via a ring feed. This is contractually guaranteed to the company.
The company uses a redundant uninterruptible power supply (UPS) that integrates lightning and surge protection devices. The uninterruptible power supply is automatically tested for effectiveness once every quarter. The UPS can power the entire data center for 20 minutes. For the further power supply in the event of a power failure, an emergency generator is available, powered by a diesel tank with a volume of five days. The emergency generator is tested for effectiveness once a month.
The connection to the Internet is via two different, physically separate lines from two different federal states. The two lines are not crossed.

The cooling of the server rooms is implemented up to 90% of the year via air-cooling. For this purpose, two air conditioning systems are operated redundantly. Both systems are interconnected, so both passive cooling surfaces of the chiller are available. Moisture and leakage sensors are installed throughout the building to protect against water. The company also has water drip pans at all necessary locations, drainage systems, and drainage systems on the property. Furthermore, there is a 60 cm high raised floor in the server areas.

The extinguishing system is an N2 extinguishing system with fire alarm system and early fire detection. The fire alarm system has a direct connection to the fire department. There are also special fire extinguishers on site. For further fire, protection regular inspections are carried out by the fire department. The fire brigade also carries out regular training on extinguishing missions in the data center.
It uses a central patch management with a physically separate test environment. The critical server systems run in a RAID array. Critical systems for order data processing are redundant.

5. Procedure for regular review, evaluation and evaluation (Article 32 (1) (d) of the GDPR, Article 25 (1) GDPR.
Privacy Management

In-house organization measures to ensure compliance with data protection requirements and obligations.
Employees confirm instructions, etc., when joining the company. On data protection obligations via a confidentiality agreement. There are annual training sessions on in-house organization and compliance with instructions followed by testing. Evidence of the training is available through a log of the implementation by the employee.
The data protection officer for WORTMANN TELECOM GmbH has been appointed in writing and the expert certificate of the data protection officer is available. The data protection officer of WORTMANN TELECOM GmbH can be found at https://www.wortmanntelecom.de/en/imprint.

Incident-Response Management

In the context of emergency management, this process is defined. In the course of the annual training, this will be communicated or updated to all employees.

Data-protection by default Art. 25 GDPR

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

Contract control

Measures that verify that the service provider adheres to the instructions of the client when processing personal data.
There is a formalized order on management with written contracts and agreements. In the case of (hardware) support services, after checking the admissibility of the order data processing, the handwritten notes or telephone instructions of the customers are the basis for the contract.

There is a careful selection of the service providers, among other things according to the level of its technical-organizational measures. Security measures, which the service provider has to implement. The contractor checks Service providers once a year.