## The following contract is concluded between the seventhings customer (Client) and seventhings (Contractor).

### Preamble

(1) This agreement specifies the data protection obligations of the contracting parties arising from the commissioned processing. It shall apply to all activities related to the utilisation under Section 1 (2) and in which employees of the Contractor or persons commissioned by the Contractor may come into contact with the Client's data.

(2) The term of this agreement corresponds to the term of the contract. Cancellation of the contract shall automatically result in cancellation of this agreement. Isolated cancellation of this agreement is excluded.

### § 1 Object, duration, and specification of the order

(1) The SEVENTHINGS software is a SaaS solution (cloud) on the Contractor's servers. The subject matter and terms of this agreement are defined in the contract. The Client is solely responsible for assessing the permissibility of data collection/processing/use and for safeguarding the rights of the data subjects. This agreement specifies the data protection obligations of the contracting parties arising from the commissioned data processing of the SEVENTHINGS software. The collection, processing or use of personal data by the Contractor for the Client on the Client's behalf and by the Client's instructions in connection with the provision of services for the SEVENTHINGS software.

(2) Product Description:
By digitising and automating inventory management, we help companies eliminate the high cost of manual furniture inventory, IT equipment, machines, etc. The inventory is labelled with machine-readable tags (barcode, QR code or RFID tag). During stocktaking, the labels are scanned with a mobile data capture device (smartphone, industrial scanner or RFID reader) in conjunction with the SEVENTHINGS MDT or SEVENTHINGS smartphone app and added to the database. This allows us to create a simple overview of all items (inventories) in the company. The verified inventory data can then be transferred directly from the SEVENTHINGS software to existing third-party systems. The person responsible for the inventory receives an up-to-date target/actual comparison via their access and can process any deviations themselves in the SEVENTHINGS software. Change and issue logs are no longer necessary.

(3) The group of affected persons may include
☒ Persona: employees, including volunteers, authorised representatives, temporary workers and temporary staff
☒ Students and pupils

(4) This agreement regulates the measures required by Art. 28 GDPR between the client and the contractor to protect personal data.

| Type of client data | Types of processing | Object and purpose of the processing | Circle of those affected |
|---|---|---|---|
| Surname, first name. Technical data on devices with possible personal reference, e-mail address, location | Assignment to the respective inventory/object | Provision of inventory software as a SAAS solution. If necessary, data migration and provision of the Circularity Hub module for offers to sell inventory. | Client/ Employee |
| Private address and e-mail | Offer and sale of inventory | | |

### § 2 Scope of application and responsibility

(1) The Contractor may process personal data on behalf of the Client by the contract and its service description and as specified in this agreement. Within the scope of this agreement, the client is solely responsible for compliance with the statutory provisions of data protection laws, in particular for the lawfulness of data transfer to the contractor and for the legality of data processing.

(2) The Contractor shall not use the data provided for purposes other than the fulfilment of the contract. Should an exception to Art. 28 para. 3 lit. a GDPR apply, the contractor shall inform the client immediately.

(3) This agreement initially defines the instructions and may subsequently be amended, supplemented or replaced by the client in writing or text form by individual instructions (individual instructions). Instructions beyond the contractually agreed service shall be treated as a request for a service change. The Client shall bear the justified costs. The Contractor shall notify the Client

immediately if, in its opinion, an instruction issued by the Client violates statutory provisions. The Contractor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the person responsible at the Client following a review.

Recipients of instructions from the contractor are:

- The commissioning specialised department or individuals:
  Customer Success Management (CSM)
- (or separately nominated deputy/successor)
  Steffen Prasse

## § 3 Technical and organisational measures

(1) The Contractor shall document the implementation of the technical and organisational measures set out and required before the award of the contract and before the start of processing, in particular, about the specific execution of the agreement, and submit them to the Client for review. If accepted by the client, the documented measures shall form the basis of the order.

(2) The Contractor shall establish security by Art. 28 para. 3 lit. c, 32 GDPR, particularly in conjunction with Art. 5 para. 1, para. 2 GDPR. Overall, the measures to be taken are data security measures and measures to ensure a level of protection appropriate to the risk to the confidentiality, integrity, availability and resilience of the systems. The state of the art, the implementation costs, the nature, scope and purposes of the processing, and the varying likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of Art. 32 para. 1 GDPR must be taken into account. [Details in Annex 2].

(3) The technical and organisational measures are subject to technical progress and further development. In this respect, the Contractor shall implement alternative adequate measures if necessary. In doing so, the security level of the specified measures must be well-rested. Significant changes must be documented and communicated to the client without delay.

## § 4 Obligations of the Contractor and quality assurance

In addition to complying with the provisions of this contract, the Contractor has legal obligations under Art. 28 to 33 GDPR; in this respect, the Contractor guarantees compliance with the following requirements in particular:

a) The Contractor shall process personal data exclusively as contractually agreed or as instructed by the Client unless the Contractor is legally obliged to carry out specific processing. If such obligations exist for the contractor, the contractor shall inform the client of these before processing unless the notification is prohibited by law.

b) Written appointment of a data protection officer who performs their duties by Art. 38 and 39 GDPR. Their current contact details are easily accessible on the contractor's website.

c) They are maintaining confidentiality by Art. 28 para. 3 sentence 2 lit. b, 29, 32 para. 4 GDPR. When carrying out the work, the Contractor shall only use employees who have been obliged to maintain confidentiality and have been familiarised with the relevant data protection provisions in advance. The Contractor and any person subordinate to the Contractor with access to personal data may only process this data by the Client's instructions, including the authorisations granted in this contract, unless they are legally obliged to process it.

d) The implementation of and compliance with all technical and organisational measures required for this order by Art. 28 para. 3 sentence 2 lit. c, 32 GDPR [details in Annex 2]. The necessary measures exist to support the client by Art. 28 para. 3 lit. e, 32 GDPR.

e) The Client and the Contractor shall cooperate with the supervisory authority to fulfil their tasks upon request.

f) The client shall be informed about inspection activities and measures of the supervisory authority insofar as they relate to this order.

g) If the Client is subject to an inspection by the supervisory authority, administrative offence or criminal proceedings, a liability claim by a data subject or a third party or any other claim in connection with the commissioned processing at the Contractor, the Contractor shall support the Client.

h) The Contractor shall regularly monitor the internal processes and the technical and organisational measures to ensure that the processing in its area of responsibility is carried out by the requirements of the applicable data protection law and that the protection of the rights of the data subject is guaranteed.

i) The technical and organisational measures are subject to technical progress and further development. In this respect, the Contractor shall implement alternative adequate measures if necessary. In doing so, the security level of the specified measures must be well-rested. Significant changes must be documented and communicated to the client without delay.

## §5 Correction, restriction and deletion of data

(1) The Contractor shall not process, rectify, erase or restrict the processing of the data processed on behalf of the Client without authorisation, but only by documented instructions from the Client - including the transfer of personal data to a third country or an international organisation. Given the nature of the processing, the Contractor shall support the Client in fulfilling its obligation to respond to requests to exercise the rights of the data subject referred to in Chapter III of GDPR.

(2) If included in the scope of services, deletion concepts, rights to be forgotten, corrections, data portability and information are ensured directly by the contractor by documented instructions from the client.

## §6 Subcontracting relationships

(1) Subcontracting relationships within the meaning of this provision are those services directly related to the provision of the leading service. This does not include ancillary services which the Contractor utilises, e.g. as telecommunications services, postal/transport services, maintenance and user service or the disposal of data carriers, as well as other measures to ensure the confidentiality, availability, integrity and resilience of the hardware and software of data processing systems. The Contractor undertakes to take appropriate and legally compliant contractual agreements and control measures to ensure the data protection and security of the Client's data, including in the case of outsourced ancillary services. All contractual regulations in the contractual chain shall also be imposed on any further subcontractors.

(2) The Contractor shall only commission subcontractors (other processors) with the Client's prior written or documented consent. The Contractor shall not process, rectify, erase or restrict the processing of the data processed on behalf of the Client, but only by documented instructions from the Client - including transferring personal data to a third country or an international organisation. Given the nature of the processing, the Contractor shall assist the Client in fulfilling its obligation to respond to requests to exercise the rights of the data subject referred to in Chapter III of GDPR.

(3) Suppose the Contractor engages a subcontractor to carry out specific processing activities (on behalf of the Client). In that case, this engagement must be by way of a contract that essentially imposes the same data protection obligations on the subprocessor as those that apply to the Contractor under this Agreement. The Contractor shall ensure that the sub-processor fulfils the duties to which the Contractor is subject under this Agreement and the GDPR.

(4) The transfer of the client's data to the subcontractor and the subcontractor's initial activities shall only be completed once all requirements for subcontracting have been met.

(5) If the subcontractor provides the agreed service outside the EU/EEA, the contractor shall ensure that the service is permissible under data protection law by taking appropriate measures. The same applies to service providers within the meaning of para. One sentence, 2, is to be used.

(6) Subcontractors' processing of personal data in a third country is generally not permitted. Suppose the processing of personal data is carried out in a third country in special exceptional cases and after prior authorisation by the client. In that case, this may only occur if the unique requirements of Art. 44 et seq. GDPR are fulfilled. Furthermore, this is done exclusively based on the standard contractual clauses for processors in Implementing Decision (EU) 2021/914 for transferring personal data to processors established in third countries. The client responsible for data processing is the data exporter, while the subcontractor based in the third country is the data importer.

(7) All contractual provisions in the contractual chain must also be imposed on the other subcontractor.

## § 7 Rights and obligations of the client

(1) Within the scope of this agreement, the client is responsible for compliance with the relevant data protection laws, particularly the obligations as a client for the lawfulness of the assignment of the processing of personal data to the contractor and the legality of the processing of personal data.

(2) The Client shall comply with the technical and organisational data security measures taken by the Contractor before the start of data processing and then regularly after that. The Client shall suitably document the result. The client shall ensure that these offer appropriate protection for the data's processing risks.

(3) The contract and this agreement initially define the instructions. They may be amended, supplemented, or replaced by the Client in writing or text to the body designated by the Contractor using individual instructions (so-called individual instructions). Changes to the object of processing or procedural changes must be jointly agreed upon and specified by the Client in writing or text form by sentence 1. The final decision-making authority lies with the client.

(4) The Client has the right to issue additional instructions to the Contractor, in particular to the following extent:

☒ About the fulfilment of the contract

☒ About additional data backup measures

☒ About the procedure for data protection breaches

(5) The Contractor shall name the contact person for data protection issues arising within the scope of this agreement to the Client upon request.

(6) If the persons authorised to issue instructions or the primary contact persons at the Client change, the Client shall inform the Contractor of this in writing.

(7) The Client must inform the Contractor immediately and in full if it discovers errors or irregularities in the order results about data protection regulations.

(8) If a data subject makes a claim against a contracting party about any claims under Art. 82 GDPR about data processing under this agreement or in connection with it, the contracting party against whom the claim is made undertakes to inform the other contracting party immediately. The contracting parties shall support each other in the defence of the claim.

## § 8 Notification of violations

The Contractor shall support the Client in complying with the obligations set out in Articles 32 to 36 of the GDPR regarding the security of personal data, reporting obligations in the event of data breaches, data protection impact assessments and prior consultations. This includes, among other things

a) ensuring an adequate level of protection through technical and organisational measures that take into account the circumstances and purposes of the processing as well as the predicted probability and severity of a possible breach through security vulnerabilities and enable the immediate detection of relevant breach events;

b) the obligation to report personal data breaches to the client without delay;

c) the obligation to support the client within the scope of its duty to inform the data subject and to provide the data subject with all relevant information in this context without delay;

d) the support of the client for its data protection impact assessment;

e) supporting the client in the context of prior consultations with the supervisory authority.

## § 9 Control obligations of the client

The Contractor shall provide all information necessary to demonstrate compliance with the obligations set out in this Agreement and in data protection law, shall enable and contribute to audits - including inspections - carried out by the Client or another auditor authorised by the Client.

Before commencing data processing, the client shall regularly check the technical and organisational measures taken by the contractor and document the result.

- For this purpose, he can, for example, obtain information from the contractor.
- Or, after timely coordination, during regular business hours without disrupting operations, personally inspect the goods or have them checked by a competent third party, provided that the latter is not in a competitive relationship with the Contractor.
- The Contractor warrants that, if necessary, it will cooperate in these checks by Art. 28 para. 3 sentence 2 lit. h, 32 GDPR. Any additional expenses are to be borne by the client.

## §10 Deletion and return of personal data

(1) Copies or duplicates of the data are not created without the client's knowledge. Excluded are backup copies insofar as necessary to ensure proper data processing and data required to comply with statutory retention obligations.

(2) After completion of the contractually agreed work or earlier at the request of the Client, the Contractor shall hand over to the Client all documents, processing and utilisation results and data about the contractual relationship that have come into its possession or, after prior consent, destroy them by data protection regulations. The same applies to test and scrap material. The deletion log can be submitted.

(3) Documentation that serves as proof of proper data processing by the order shall be retained by the contractor beyond the end of the contract by the respective retention periods.

## § 11 Miscellaneous

(1) Additional agreements must be made in writing.

(2) Should individual parts of this agreement be or become invalid, this shall not affect the validity of the remainder of the contract.

(3) German law shall apply. Dresden is agreed as the place of jurisdiction.

[As of: March 2024]

Attachments:

| | |
|---|---|
| Annex 1: | Subcontractors |
| Annex 2: | Description of the technical and organisational measures for the operation of the inventory manager |
| Annex 3: | Description of Telekom's technical and organisational measures for the operation of the data centre and server hosting |

## Annex 1 Subcontractor

| Name and address of the subcontractor | Description of the partial services |
|---|---|
| Open Telekom Cloud from Deutsche Telekom AG<br>T-Systems International GmbH, Hahnstraße 43d, 60528 Frankfurt am Main, Germany | Infrastructure-as-a-Service, Hosting |
| TeamViewer Germany GmbH, Bahnhofsplatz 2, 73033 Göppingen | Remote maintenance |
| Strato AG, Pascalstr. 10, 10587 Berlin | Infrastructure-as-a-Service, Hosting |

# Annexe 2 Description of the technical and organisational measures for operating the inventory manager.

## Details of the controller (Art. 30 para. 1 lit. a GDPR):

## Responsible person:

## Zwischen dem seventhings Kunden (Auftraggeber) und der seventhings GmbH (Auftragnehmer) wird nachfolgender Vertrag geschlossen.

### Präambel

(1) Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der Auftragsverarbeitung ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit der Nutzung gemäß §1 Absatz 2 in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten des Auftraggebers in Berührung kommen können.

(2) Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des Vertrags. Eine Kündigung des Vertrages bewirkt automatisch die Kündigung dieser Vereinbarung. Eine isolierte Kündigung dieser Vereinbarung ist ausgeschlossen.

### § 1 Gegenstand, Dauer und Spezifizierung des Auftrags

(1) Die Nutzung der Software SEVENTHINGS erfolgt als SaaS-Lösungen (Cloud) auf den Servern des Auftragnehmers. Gegenstand und Laufzeit dieser Vereinbarung ist im Vertrag definiert. Für die Beurteilung der Zulässigkeit der Datenerhebung / -verarbeitung / -nutzung sowie für die Wahrung der Rechte der Betroffenen ist allein der Auftraggeber verantwortlich. Diese Vereinbarung konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der Auftragsdatenverarbeitung der Nutzung der Software SEVENTHINGS ergeben. Die Erhebung bzw. Verarbeitung oder Nutzung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber in dessen Auftrag und nach dessen Weisung im Zusammenhang mit der Erbringung von Servicedienstleistungen für die Software SEVENTHINGS.

(2) Produktbeschreibung:
Wir helfen Unternehmen den hohen Aufwand der manuellen Inventarisierung von Mobiliar, IT-Equipment, Maschinen, etc. zu beseitigen, indem wir die Inventarverwaltung digitalisieren und automatisieren. Das Inventar wird mit maschinenlesbaren Etiketten versehen (Barcode, QR-Code oder RFID-Tag). Bei der Inventur werden die Etiketten mit einem mobilen Datenerfassungsgerät (Smartphone, Industriescanner oder RFID Reader) in Verbindung mit der App SEVENTHINGS MDT oder App SEVENTHINGS Smartphone gescannt und zum Datenbestand hinzugefügt. Damit schaffen wir einen einfachen Überblick über alle Gegenstände (Inventare) im Unternehmen. Die geprüften Inventurdaten können dann aus der Software SEVENTHINGS direkt in bestehende Dritt-System übertragen werden. Der Inventarverantwortliche erhält über seinen Zugang einen aktuellen Soll-Ist-Vergleich und kann auftretende Abweichungen selbst in der Software SEVENTHINGS bearbeiten. Änderungs- und Abgangsprotokolle sind nicht mehr nötig.

(3) Kreis der Betroffenen können u.a. sein,

☒ Persona; Beschäftigte einschließlich Freiwilliger, Beauftragte, Zeitarbeitskräfte und Aushilfen
☒ Studenten und Schüler

(4) Diese Vereinbarung regelt die Maßnahmen, die Art. 28 DS-GVO zwischen Auftraggeber und Auftragnehmer zum Schutz personenbezogener Daten verlangt.

| Art der Auftraggeber-Daten | Arten der Verarbeitung | Gegenstand und Zweck der Verarbeitung | Kreis der Betroffenen |
|---|---|---|---|
| Name, Vorname<br>Technische Daten zu Geräten mit ggf. Personenbezug, E-Mail-Adresse, Standort<br>Private Anschrift und E-Mail | Zuordnung zum jeweiligen Inventar/ Gegenstand<br><br>Angebot und Verkauf von Inventar | Bereitstellung einer Software zur Inventarisierung als SAAS-Lösung. Gegeben falls Datenmigration und Bereitstellung des Modul Circularity Hub für Angebote zum Verkauf von Inventar. | Auftraggeber/ Mitarbeiter |

### § 2 Anwendungsbereich und Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet ggf. personenbezogene Daten im Auftrag des Auftraggebers gemäß dem Vertrag und dessen Leistungsbeschreibung und wie in dieser Vereinbarung konkretisiert. Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich.

seventhingsGmbH
Hainstrasse 2, 01097 Dresden (Germany)

### Legal representative:
The management

### Data Protection Officer:
DataOrga® GmbH
E-mail: dsb@seventhings.com

## M.1 Confidentiality measures

### M.1.1 Description of access control:
- See Telekom's TOMs

### M.1.2 Description of access control:
- Authentication with user + password - Authentication with user + password [implemented]
- User authorisations - Manage user authorisations (e.g. when joining, changing, leaving) [implemented]
- Firewall - Use of firewalls to protect the network [implemented]
- MDM - Use of Mobile Device Management [implemented]
- Encryption of data carriers - Encryption of data carriers using state-of-the-art procedures [implemented]

### M.1.3 Description of access control:
- Authorisation concept - Creation and use of an authorisation concept [implemented]
- Password light guidelines - password guidelines incl. length, complexity and change frequency [implemented]
- Secure storage - Secure storage of data carriers [implemented]
- Encryption of data carriers - Encryption of data carriers using state-of-the-art procedures [implemented]

### M.1.4 Description of the transfer control:
- SSL / TLS encryption - Use SSL/TLS encryption for data transmission on the Internet [implemented].
- VPN tunnels - Setting up VPN tunnels for dialling into the network from outside [implemented]

### M.1.5 Description of the separation requirement:
- Logical client separation - Logical client separation (on the software side) [implemented]
- Production and test system - separation of production and test system [implemented]

### M.1.6 Description of pseudonymisation:
- There is no pseudonymisation.

### M.1.7 Description of the encryption:
- Storage - Encrypted data storage (e.g. file encryption according to AES256 standard) [implemented].
- Transmission - Encrypted data transmission (e.g. e-mail encryption using PGP or S/Mime, VPN, encrypted Internet connections using TLS/SSL, use of FTAPI data transfer tool) [implemented].

### M.1.8 Description of the data carrier control:
- Secure storage - Secure storage of data carriers [implemented]

### M.1.9 Description of the user control:
- Password assignment - protection of user accounts with passwords [implemented]
- Blocking ex-employees - Blocking user accounts of former employees [implemented]
- Two-factor authentication - authentication with user name/password and a second factor (e.g. hardware token, SMS, FIDO2) [implemented].

### M.1.10 Description of the transmission control:
- Logging - Logging of all retrieval and transmission processes [implemented]

## M.2 Integrity measures

### M.2.1 Description of the input control:
- Personalised user names - traceability of entry, modification and deletion of data through individual user names (not user groups)
- Logging - Logging the entry, modification and deletion of data [implemented]
- Access rights - Personalised access rights for traceability of access. [implemented]

### M.2.2 Description of data integrity:
- Data backup concept - creation of a backup and recovery concept [implemented]

### M.2.3 Description of the memory control:
- Authorisation concept - Definition of authorisations in an authorisation concept [implemented]

- Need-to-know principle - number of authorisations and administrators reduced to the bare minimum
- Logging – the number of authorisations and administrators reduced to the bare minimum [implemented]

## M.3 Measures for availability and resilience

### M.3.1 Description of availability control:

- Antivirus software - use of antivirus software to protect against malware
- Backup and recovery concept - Creating a backup and recovery concept [implemented]

### M.3.2 Description of rapid recoverability:

- Data restores - Regular and documented data restores [implemented]

## M.4 Further data protection measures

### M.4.1 Description of the order control:

- Audits - regular data protection audits by the company data protection officer [implemented]
- Selection - selection of the contractor under due diligence aspects (in particular about data security) [implemented]
- DPA contract - conclusion of an agreement on commissioned processing under Art. 28 GDPR. [implemented]
- Ongoing review - Ongoing review of the contractor and its activities [implemented]

### M.4.2 Description of the data protection management system:

- Audits - Conduct regular internal audits [implemented]
- DPO - Appointment of a data protection officer [implemented]
- Training - Training for all employees with access authorisation. Regular follow-up training sessions. [Implemented]
- Vulnerability analyses - conducting regular IT vulnerability analyses (e.g. penetration test) [implemented]
- Software-supported tools - Use of software-supported tools for compliance with data protection requirements (audatis MANAGER) [implemented]
- Software-supported tools - Use of software-supported tools for compliance with data protection requirements (e.g. audatis MANAGER) [implemented]
- Obligation - Obligation of confidentiality under Art. 28 para. 3 sentence 2 lit. b, Art. 29, Art. 32 para. 4 GDPR [implemented]

### M.4.3 Description of Organisational Control:

- Data protection officer - A data protection officer is appointed, and their contact details are published [implemented]
- Documentation of processing - All processing activities are documented and regularly reviewed [implemented]
- Guidelines - Binding guidelines exist for the handling of personal data
- Sensitisation - employees are regularly sensitised and trained on data protection [implemented]

# Annex 3 Description of Telekom's technical and organisational measures for the operation of the data centre and server hosting

*Note: All SEVENTHINGS Inventory Manager data is stored in the Open Telekom Cloud of Deutsche Telekom AG*

### Details of the controller (Art. 30 para. 1 lit. a GDPR):

**Responsible person:**
seventhings GmbH
Hainstrasse 2, 01097 Dresden (Germany)

**Legal representative:**
The management

**Data Protection Officer:**
DataOrga® GmbH
E-mail: dsb@seventhings.com

## M.1 Confidentiality measures

### M.1.1 Description of access control:

- Alarm system - use of an alarm system (possibly with notification to security service) [implemented]
- Visitor logging - logging of visitors (e.g. visitor book) [implemented]
- Chip cards - Chip card/transponder locking system [implemented]
- Gatekeeper - personal check at the gatekeeper [implemented]
- Key management - essential regulation with documentation of keys (e.g. critical book) [implemented]
- Video surveillance - video surveillance of entrances [implemented]

### M.1.2 Description of access control:

- Authentication with user + password - Authentication with user + password [implemented]
- User authorisations - Manage user authorisations (e.g. when joining, changing, leaving) [implemented]
- Firewall - Use of firewalls to protect the network [implemented]
- Careful staff selection - Careful selection of cleaning and security staff [implemented]
- Encryption of data carriers - Encryption of data carriers using state-of-the-art procedures [implemented]

### M.1.3 Description of access control:

- Authorisation concept - Creation and use of an authorisation concept [implemented]
- Password light guidelines - password guidelines incl. length, complexity and change frequency [implemented]
- Encryption of data carriers - Encryption of data carriers using state-of-the-art procedures [implemented]

### M.1.4 Description of the transfer control:

- SSL / TLS encryption - Use SSL/TLS encryption for data transmission on the Internet [implemented].
- VPN tunnels - Setting up VPN tunnels for dialling into the network from outside [implemented]

### M.1.5 Description of the separation requirement:

- Logical client separation - Logical client separation (on the software side) [implemented]
- Production and test system - separation of production and test system [implemented]

### M.1.6 Description of pseudonymisation:

- There is no pseudonymisation

### M.1.7 Description of the encryption:

- Storage - Encrypted data storage [implemented]
- Transmission - Encrypted data transmission (e.g. VPN, encrypted Internet connections using TLS/SSL, data transfer tool) [implemented].

### M.1.8 Description of the data carrier control:

- Secure storage - Secure storage of data carriers [implemented]
- Destruction - Proper destruction of data carriers (DIN 66399) [implemented]
- Encryption - Encryption of data carriers [implemented]

### M.1.9 Description of the user control:

- Password assignment - protecting user accounts with passwords [implemented]
- Blocking of ex-employees - Blocking of user accounts of former employees [implemented]

- Two-factor authentication - authentication with user name/password and a second factor (e.g. hardware token, SMS, FIDO2) [implemented].

### M.1.10 Description of the transmission control:

- Logging - Logging of all retrieval and transmission processes [implemented]

## M.2 Integrity measures

### M.2.1 Description of the input control:

- Personalised user names - traceability of entry, modification and deletion of data through individual user names (not user groups) [implemented]
- Logging - Logging the entry, modification and deletion of data [implemented]
- Access rights - Personalised access rights for traceability of access. [implemented]

### M.2.2 Description of data integrity:

- Data backup concept - creation of a backup and recovery concept [implemented]

### M.2.3 Description of the memory control:

- Authorisation concept - Definition of authorisations in an authorisation concept [implemented]
- Need-to-know principle – the number of authorisations and administrators reduced to the bare minimum [implemented]
- Logging – the number of authorisations and administrators reduced to the bare minimum [implemented]

## M.3 Measures for availability and resilience

### M.3.1 Description of availability control:

- Antivirus software - Use of antivirus software to protect against malware [implemented]
- Outsourcing data backup - storage of data backup in a secure, outsourced location [implemented]
- Backup and recovery concept - Creating a backup and recovery concept [implemented]
- Fire alarm systems - Fire and smoke detection systems [implemented]
- Fire extinguishers - CO2 fire extinguishers in server rooms [implemented]
- IT contingency plan - creation and application of IT contingency plans [implemented]
- Air conditioning - Air conditioning in server rooms [implemented]
- Redundant data storage - Redundant data storage (e.g. mirrored hard disks, RAID 1 or higher, mirrored server room) [implemented]
- Protective socket strips - Protective socket strips in server rooms [implemented]
- Temperature monitoring - Devices for monitoring temperature and humidity in server rooms [implemented]
- Uninterruptible power supply - (UPS) Uninterruptible power supply [implemented]

### M.3.2 Description of rapid recoverability:

- Data restores - Regular and documented data restores [implemented]
- Contingency plans - IT contingency plans and restart plans [implemented]

## M.4 Further data protection measures

### M.4.1 Description of the order control:

- Audits - Regular data protection audits by the company data protection officer [implemented]
- Selection - selection of the contractor under due diligence aspects (in particular about data security) [implemented]
- DPA contract - conclusion of an agreement on commissioned processing by Art. 28 GDPR. [implemented]
- Ongoing review - Ongoing review of the contractor and its activities [implemented]

### M.4.2 Description of the data protection management system:

- Audits - Conduct regular internal audits [implemented]
- DPO - Appointment of a data protection officer [implemented]
- Incident response system - Incident response system for the traceability of security breaches and problems [implemented]
- Data protection management system - Data protection management system [implemented]
- Information security management system - Information security management system ISO 27001 [implemented]
- Training - Training of all employees with access authorisation. Regular follow-up training sessions. [Implemented]
- Vulnerability analyses - conducting regular IT vulnerability analyses (e.g. penetration test) [implemented]
- Software default settings - use of software with data protection-friendly default settings by (Art. 25 (2) GDPR) [implemented]

- Software-supported tools - Use of software-supported tools to comply with data protection requirements. [implemented]
- Obligation - Obligation of confidentiality under Art. 28 para. 3 sentence 2 lit. b, Art. 29, Art. 32 para. 4 GDPR [implemented]

### M.4.3 Description of Organisational Control:

- Data protection officer - A data protection officer has been appointed, and their contact details have been published [implemented]
- Documentation of processing - All processing activities are documented and regularly reviewed [implemented]
- Guidelines - Binding guidelines exist for the handling of personal data [implemented]
- Sensitisation - employees are regularly sensitised and trained on data protection [implemented]