The following contract is concluded between the seventhings customer (client) and seventhings by ITEXIA GmbH (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 connected with the use under §1 Paragraph 2 and in which employees of the contractor or persons authorised by the contractor may come into contact with the client's personal data.

(2) The term of this agreement corresponds to the term of the contract. Termination of the Contract shall automatically terminate this agreement. An isolated termination of this agreement is excluded.

§ 1 Subject matter, duration and specification of the order

(1) The SEVENTHINGS software is used as a SaaS solution (cloud) on the contractor's servers. The subject matter and terms of this agreement are defined in the contract. The client alone is responsible for assessing the permissibility of the 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 customer on the customer's behalf and by the customer's instructions in connection with the provision of services for the SEVENTHINGS software.

(2) Product Description:
We help companies to eliminate the high effort of manual inventory of furniture, IT equipment, machines, etc., by digitising and automating inventory management. The inventory is provided with machine-readable labels (barcode, QR code or RFID tag). During the inventory, the labels are scanned with a mobile data capture device (smartphone, industrial scanner or RFID reader) in conjunction with the SEVENTHINGS MDT app or SEVENTHINGS Smartphone app and added to the data inventory. This way, we create a simple overview of all items (inventories) in the company. The checked inventory data can then be transferred from the SEVENTHINGS software directly into 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 in the SEVENTHINGS software. Change and retirement logs are no longer necessary. The circle of those affected can include,

☒ Persona; employees including volunteers, appointees, temporary and casual workers
☒ Students and pupils

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

Type of client data	Types of processing	Purpose of data collection, processing or use	Circle of those affected
Name, first name Technical data on devices with possible personal reference, e-mail address	Assignment to the respective inventory/object	The Contractor shall perform inspection activities for the Client during which the possibility of access to personal data cannot be excluded. For authentication and authorisation	Client/employee

§ 2 Scope of application and responsibility

(1) If applicable, the contractor shall 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 shall be solely responsible for compliance with the statutory provisions of the data protection laws, in particular for the lawfulness of the transfer of data to the contractor, as well as for the legality of the data processing.

(2) The contractor shall not use the data provided for any purposes other than the performance of the contract. If an exception of Art. 28 para. 3 lit. a GDPR applies, and the contractor shall inform the client immediately.

(3) The instructions shall initially be determined by this agreement and may then 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 charge. The client shall bear the justified costs. The contractor shall immediately draw the client's attention to the fact that an instruction issued by the client violates statutory provisions in his opinion. The contractor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the responsible person at the client after review.

The recipients of instructions on the part of the contractor are the following:

- The commissioning specialist department or individuals:
  Customer Success Management (CSM),
- (or separately named 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 in the run-up to the award of the contract before the start of the processing, in particular about the specific execution of the agreement, and shall hand them over to the client for inspection. If the client accepts, the documented measures shall become the basis of the contract.

(2) The contractor shall establish security under Art. 28 (3) lit. c, 32 GDPR, particularly in connection with Art. 5 (1), (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 confidentiality, integrity, availability and resilience of the systems. State of the art, the implementation costs and the nature, scope and purposes of the processing as well as the varying likelihood and severity of the risk to the rights and freedoms of natural persons within the meaning of Article 32 (1) of the GDPR shall 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 adequate alternative measures if necessary. In doing so, the security level of the specified measures must not be undercut. Significant changes shall be documented and communicated to the client without delay.

§ 4 Duties of the Contractor and Quality Assurance

In addition to compliance with the provisions of this order, the contractor shall have statutory obligations under Articles 28 to 33 of the GDPR; in this respect, the contractor shall, in particular, ensure compliance with the following requirements:

a) The contractor shall process Personal Data only as contractually agreed or as instructed by the client unless the contractor is legally obliged to carry out a specific processing operation. If such obligations exist for the contractor, the contractor shall notify the client of these before the processing unless the notification is prohibited by law.

b) Written appointment of a data protection officer who performs his or her duties in accordance with Articles 38 and 39 of the GDPR. The current contact details of the data protection officer are easily accessible on the Contractor's website.

c) Maintain confidentiality under Art. 28 (3) sentence 2 lit. b, 29, 32 (4) GDPR. When carrying out the work, the contractor shall only use employees who have been obligated to maintain confidentiality and who have previously been familiarised with the relevant data protection provisions. The contractor and any person subordinate to the contractor who has access to personal data may process this data exclusively by the client's instructions, including the powers 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 contract by Art. 28 (3) sentence 2 lit. c, 32 GDPR [details in Annex 2].

e) The contracting authority and the contractor shall cooperate with the supervisory authority to perform its duties upon request.

f) The principal shall be informed of control actions and measures of the supervisory authority insofar as they relate to this order.

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

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 adequate alternative measures if necessary. In doing so, the security level of the specified measures must not be undercut. Significant changes shall be documented and communicated to the client without delay.

§5 Correction, restriction and deletion of data

(1) The contractor shall not correct, delete or restrict the processing of data processed under the contract on its authority, but only by documented instructions from the client. As a data subject contacts the contractor directly in this regard, the contractor shall forward this request to the client.

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

§6 Subcontracting relationships

(1) Subcontracting relationships within the meaning of this provision shall be understood to be those services which relate directly to the provision of the leading service. This does not include ancillary services which the contractor uses, for example, 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 implement appropriate and legally compliant contractual agreements and control measures to ensure data protection and data security of the client's data, also in the case of outsourced ancillary services. All contractual regulations in the contractual chain shall also be imposed on any further subcontractor.

(2) The contractor shall only engage subcontractors (further processors) with the client's prior written or documented consent.

(3) The client consents to the commissioning of the subcontractors under Annex 1 subject to the condition of a contractual agreement by Article 28 (2-4) of the GDPR.

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

(5) If the subcontractor provides the agreed service outside the EU/EEA, the contractor shall ensure that it is permissible under data protection law by taking appropriate measures. The same shall apply if service providers are within the meaning of para. 1 sentence 2 is to be used.

(6) The processing of personal data by subcontractors in a third country is generally not permitted. If the processing of personal data is carried out in a third country in special exceptional cases and after prior approval by the client, then this may only occur if the unique requirements of Art. 44 et seq. GDPR are fulfilled. Furthermore, this shall be carried out 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 Principal authorises the Contractor to enter into a contract on its behalf (Principal) with subcontractors of the Contractor based in third countries by the Standard Contractual Clauses. In this context, the principal responsible for the data processing is considered the data exporter and the subcontractor established in the third country is regarded as the data importer.

(7) All contractual provisions in the contractual chain shall also be imposed on the further subcontractor.

§ 7 Rights and Duties of the Principal

(1) The Principal is responsible under this Agreement for compliance with the relevant data protection laws, in particular related to the obligations as principal for the lawfulness of the award of the processing of personal data to the Contractor as well as for the lawfulness of the processing of personal data.

(2) The client shall comply with the contractor's technical and organisational data security measures before data processing and, after that, regularly. The client shall suitably document the result. The client shall be responsible for ensuring that these provide an appropriate level of protection for the risks of the data to be processed.

(3) The instructions shall initially be determined by the contract and this agreement and may be amended, supplemented or replaced by the client in writing or text to the body designated by the contractor by individual instructions (so-called individual instructions). Changes to the object of processing or modifications to the process shall be jointly agreed upon and determined by the

client in writing or text form by sentence 1. The final decision-making authority shall lie with the client.

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

☒ About the performance of the contract

☒ About other data backup measures

☒ About the procedure for data protection breaches

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

(6) If the persons authorised to give instructions or the primary contact persons at the Client change, the client shall notify the contractor in writing.

(7) The client shall inform the contractor immediately and in full if it discovers errors or irregularities in the order results regarding data protection provisions.

(8) In the event of a claim being made against a contracting party by a data subject in respect of any claims under Article 82 of the GDPR about data processing under this agreement or connection with it, the contracting party against which a claim is made undertakes to inform the other contracting party without delay. The Contracting Parties shall assist each other in defending the claim.

§ 8 Notification of infringements

The Contractor shall assist the Client in complying with the personal data security obligations, data breach notification obligations, data protection impact assessments and prior consultations referred to in Articles 32 to 36 of the GDPR. This includes, among others

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 likelihood and severity of a potential security breach and allow for the immediate detection of relevant breach events;

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

c) the commitment to support the principal within the scope of his duty to inform the data subject and, in this context, to provide him with all relevant information without delay;

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

e) the help of the principal in the context of prior consultations with the supervisory authority.

§ 9 Control Duties of the Principal

The client shall satisfy itself with the technical and organisational measures taken by the contractor before the commencement of data processing and then regularly document the result.

- For this purpose, he may, for example, obtain information from the contractor.
- Or, after timely coordination, personally inspect the goods during regular business hours without disrupting operations or have them reviewed by a competent third party, provided that such third party is not in a competitive relationship with the contractor.
- The Contractor warrants that it will cooperate in these inspections to the extent necessary. The client shall bear additional expenses.

§10 Deletion and return of personal data

(1) Copies or duplicates of the data shall not be made without the client's knowledge. Excluded from this are security copies, insofar as they are necessary to ensure proper data processing and data required with compliance with statutory retention obligations.

(2) After completion of the contractually agreed work or earlier upon request by the client - at the latest upon the termination of the service agreement - the contractor shall hand over to the client or, after prior consent, destroy by data protection law all documents, processing and utilisation results produced and data files which have come into its possession and which are connected with the contractual relationship. The same applies to testing and rejecting material. The protocol of the deletion may be submitted.

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

§ 11 Miscellaneous

(1) The written form is required for ancillary agreements.

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

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

[As of October 2022]

Attachments:
Annexe 1 Subcontractor
Annexe 2 technical organisational measures - basic security

Annexe 1 Subcontractor

Name and address of the subcontractor	Description of the partial services
Open Telekom Cloud of Deutsche Telekom AG T-Systems International GmbH, Hahnstraße 43d, 60528 Frankfurt am Main, Germany	Infrastructure-as-a-Service, Hosting

Annexe 2 Technical organisational measures - basic security

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

1. Access control

Measures suitable for preventing unauthorised persons from gaining access to data processing systems with which personal data are processed or used.

- ☐ Alarm system
- ☐ Automatic access control system
- ☐ Locking system with code lock
- ☐ Biometric access barriers
- ☐ Light barriers / motion detectors
- ☒ Key regulation (key issue etc.)
- ☐ Logging of visitors
- ☐ Cautious choice of security guards
- ☐ Protection of building shafts
- ☐ Chip card/transponder locking system
- ☒ Manual locking system
- ☒ Video surveillance of the entrances
- ☒ Security locks
- ☒ Person control at the reception
- ☒ Careful selection of cleaning staff
- ☐ Obligation to wear credentials

2. Access control

Measures suitable for preventing data processing systems from being used by unauthorised persons.

- ☒ Assignment of user rights
- ☒ Password assignment
- ☒ Authentication with user name/password
- ☐ Housing locks
- ☐ Create user profiles
- ☐ Authentication with biometric methods
- ☒ Selection of user profiles for IT systems
- ☒ Use of VPN technology

- ☐ Locking external interfaces (USB etc.)
- ☒ Security locks
- ☒ Critical regulation (key issue etc.)
- ☒ Person control at the reception
- ☐ Logging of visitors
- ☒ Careful selection of cleaning staff
- ☐ Cautious choice of security guards
- ☐ Obligation to wear credentials
- ☐ Use of intrusion detection systems
- ☐ Encryption of mobile data carriers
- ☐ Encryption of smartphone content
- ☐ Use of central smartphone administration software (e.g. for external deletion of data)
- ☒ Use of anti-virus software
- ☒ Encryption of data carriers in laptops/ notebooks
- ☒ Use of a hardware firewall
- ☒ Use of a software firewall

3. Access control

Measures to ensure that those authorised to use a data processing system can only access the data subject to their access authorisation and that personal data cannot be read, copied, modified or removed without permission during processing, use and after storage.

- ☒ Creating an authorisation concept
- ☒ Administration of rights by the system administrator
- ☒ The number of administrators was reduced to the "bare minimum"
- ☒ Password policy incl. password length, password change
- ☒ Logging of access to applications, especially when entering, changing and deleting data
- ☒ Secure storage of data media
- ☒ Physical erasure of data carriers before reuse
- ☒ Proper destruction of data carriers (DIN 66399)
- ☒ Use of document shredders or service providers (if possible with data protection seal of approval)
- ☐ Logging of the destruction
- ☒ Encryption of data carriers

4. Transfer control

Measures to ensure that personal data cannot be read, copied, altered or removed by unauthorised persons during electronic transmission or during their transport or storage on data media and that it is possible to verify and establish to which bodies personal data are intended to be transmitted by data transmission equipment.

- ☒ Establishment of dedicated lines or VPN tunnels
- ☐ Disclosure of data in anonymised or pseudonymised form
- ☐ E-mail encryption
- ☐ Create an overview of regular retrieval and transmission processes, monthly log file
- ☐ Documentation of the recipients of data and the time spans of the planned transfer or agreed deletion periods
- ☐ During physical transport: secure transport containers/packaging
- ☒ For physical transport: careful selection of transport personnel and vehicles
- ☒ HTTPS-secured remote maintenance connection

Regulation for remote maintenance:
Remote maintenance is only permitted for contractually agreed care by the service contract (an on-premises solution). Remote maintenance is carried out with the help of the TeamViewer tool.
The SEVENTHINGS employee documents the remote maintenance (who, when, service provider, problem and result).

5. Input control

Measures to ensure that it is possible to check and establish retrospectively whether and by whom personal data have been entered into, modified or removed from data processing systems.

- ☐ Logging the entry, modification and deletion of data
- ☒ Traceability of entry, modification and deletion of data through individual user names (not user groups)
- ☒ Allocation of rights to enter, change and delete data based on an authorisation concept
- ☐ Create an overview showing which applications can be used to enter, change, and delete data.
- ☐ Retention of forms from which data have been transferred to automated processing operations

6. Order control

Measures to ensure that personal data processed on behalf of the principal can only be processed in accordance with the principal's instructions.

- ☒ Selection of the contractor under due diligence aspects (in particular about data security)
- ☒ Written instructions to the contractor (e.g. through a commissioned data processing contract) within the meaning of Section 11 (2) of the Federal Data Protection Act.
- ☒ The contractor has appointed a data protection officer
- ☒ Effective control rights vis-à-vis the contractor agreed
- ☐ Contractual penalties in the event of infringements
- ☒ Prior examination of and documentation of the security measures taken at the contractor's premises
- ☒ Obligation of the contractor's employees to maintain data secrecy (§ 5 Federal Data Protection Act)
- ☒ Ensuring the destruction of data after completion of the order
- ☒ Ongoing review of the contractor and its activities

7. Availability control

Measures to protect personal data against accidental destruction or loss in Telekom's OTC.

- ☒ Uninterruptible Power Supply (UPS)
- ☒ Devices for monitoring temperature and humidity in server rooms
- ☒ Fire and smoke detection systems
- ☒ Alarm message for unauthorised access to server rooms
- ☒ Testing data recovery
- ☒ Air conditioning in server rooms
- ☒ Protective socket strips in server rooms
- ☒ Fire extinguishers in server rooms
- ☒ Creation of a backup & recovery concept
- ☒ Create an emergency plan

- ☒ Keeping data backup in a secure, off-site location
- ☐ In flood zones: Server rooms above the water line
- ☒ Server rooms not under sanitary facilities
- ☒ OTC Deutsche Telekom

8. Separation requirement

Measures to ensure that data collected for different purposes can be processed separately.

- ☐ physically separate storage on separate systems or data carriers
- ☒ Creation of an authorisation concept
- ☐ Providing the records with purpose attributes/data fields
- ☒ Setting database rights
- ☒ Logical client separation (on the software side)
- ☐ Encryption of data sets processed for the same purpose
- ☐ For pseudonymised data: Separation of the attribution file and storage on a separate, secured IT system
- ☒ Separation of productive and test system