WidasConcepts GmbH
Maybachstraße 2
71299 Wimsheim

T: +49 7044 95103 100
E: datenschutz@widas.de

www.widas.de

Status: April 2026

Technical and organizational measures (TOM)

The technical and organizational measures are implemented jointly by the Contractor and the Widas Group in accordance with Art. 32 GDPR. The Contractor and the Widas Group continuously refine these measures in line with feasibility and the state of the art - including in the context of their active ISO 27001 certification - and raise them to a higher level of security and protection.

1. Confidentiality

1.1. (Physical)Access Control

Technical measures	Organizational measures
✓ Alarm system ✓ Automatic access control ✓ Fraud detection for access control ✓ Electronic locking system ✓ WidasCloud security door (T 90-1-FSA steel fire door tested in accordance with DIN 4102 and no windows). ✓ Video surveillance of entrances ✓ Motion detectors and video surveillance of interior areas	✓ Key Management Policy/List ✓ Visitor Log/Digital Visitor Record ✓ Visitors accompanied by Staff ✓ Careful selection of Cleaning Services ✓ Information Security Policy ✓ Operational Safety Work Instruction ✓ Access Control Work Instruction ✓ Certification Documents for Subcontracted Data Processors

1.2. Authentication

Technical measures	Organizational measures
✓ Use of antivirus software ✓ Use of a hardware firewall ✓ Use of a web application firewall ✓ Authentication via at least a username and strong password, including fraud detection ✓ Encryption of data storage media ✓ Automatic desktop lock ✓ Two-factor authentication in data center operations and for all IT systems	✓ User Permissions Management ✓ User Profiles ✓ Information Security Policy ✓ Operational Safety Work Instruction ✓ Access Control Work Instruction ✓ Work Instruction for the Use of End Devices (Mobile Device Policy) ✓ Fine-grained rights assignment

WidasConcepts GmbH
Maybachstraße 2
71299 Wimsheim

T: +49 7044 95103 100
E: datenschutz@widas.de

www.widas.de

✓ Use of VPN technology	

1.3. Authorization

Technical measures	Organizational measures
✓ Document shredder ✓ Physical destruction of data storage media ✓ Logging of access to the application when data is entered, modified, or deleted (event-driven architecture) ✓ Encrypted SSH access ✓ Certified SSL encryption	✓ Implementation of Authorization Concepts ✓ Fine-grained authorization management via cidaas ✓ Number of administrators reduced to the bare minimum ✓ User authorizations managed by administrators ✓ Information Security Policy ✓ Work Instruction on Communication Security ✓ Work Instruction on Handling Information and Assets

1.4. Separation Control

Technical measures	Organizational measures
✓ Separation of production and test systems ✓ Logical client separation (via virtualization) ✓ Logical separation of customer systems ✓ Staging environment prior to development, test, and production environments	✓ Management of the authorization framework ✓ Definition of database permissions ✓ Information Security Policy ✓ Data Protection Policy ✓ Operational Safety Work Instruction ✓ Work Instruction on Security, including Quality Assurance in Software Development

1.5. Pseudonymization

Technical measures	Organizational measures
✓ In the case of pseudonymization: Separation of identifying data and storage in a separate, secure system (possibly encrypted)	✓ Internal Policy: Where possible, personal data must be pseudonymized prior to disclosure ✓ Data Protection Policy ✓ Information Security Policy ✓ Cryptographic Measures Policy

WidasConcepts GmbH
Maybachstraße 2
71299 Wimsheim

T: +49 7044 95103 100
E: datenschutz@widas.de

www.widas.de

2. Integrity

2.1. Disclosure Control

Technical measures	Organizational measures
✓ Use of VPN ✓ SSL/TLS encryption for secure transmission ✓ Recording of accesses and retrievals	✓ Disclosure in anonymized or pseudonymized form ✓ Information Security Policy ✓ Data Protection Policy

2.2. Input control

Technical measures	Organizational measures
✓ Logging of data entry, modification, and deletion ✓ Manual or automated review of logs (in accordance with the Information Security Policy)	✓ Assignment of rights to enter, modify, and delete data via defined roles in the authorization scheme ✓ Traceability of data entry, modification, and deletion through individual user names (not user groups) ✓ Information Security Policy ✓ Work Instructions for Users ✓ Overview and monitoring of when and how specific entries, changes, and deletions were made

3. Availability and reliability

3.1. Availability Control

Technical measures	Organizational measures
✓ Air-conditioned rooms, particularly server rooms ✓ Smoke detection and fire alarm system / emergency alarm system ✓ Monitoring of temperature and humidity in server rooms ✓ Gas fire suppression systems in server rooms ✓ Local uninterrupted power supply (UPS and emergency power generator) ✓ Optimized circuit configuration	✓ Backup & Recovery Strategy ✓ Monitoring of the backup process ✓ Backups are stored in a secure location ✓ Service manager at partner data centers, if applicable ✓ Existence of a contingency plan ✓ Server deployment planning ✓ Automated provisioning processes ✓ Information security policy ✓ Continuous monitoring and health checks

WidasConcepts GmbH
Maybachstraße 2
71299 Wimsheim

T: +49 7044 95103 100
E: datenschutz@widas.de

www.widas.de

✓ Surge protection ✓ Remote fault indication ✓ Redundancy in the technical infrastructure ✓ Distribution across multiple data centers	✓ No plumbing connections in or above the server room Regular testing of the diesel generator ✓ Standby service

4. Procedures for regular review, assessment, and evaluation

4.1. Data protection measures

Technical measures	Organizational measures
✓ ISO 27001 security certification ✓ Annual review of the effectiveness of the TOM, including updates ✓ Risk assessment, including data protection checkpoints ✓ Centralized documentation of all data protection and security policies, with access for employees	✓ Employee confidentiality and data privacy obligations ✓ Regular employee security awareness training ✓ Data Protection Officer and Information Security Officer ✓ Data Protection Impact Assessments are conducted as needed ✓ ISO 27001 certification and annual surveillance audits ✓ The organization complies with the information obligations under Art. 13 and 14 GDPR ✓ Formal process and responsibilities for the follow-up of security incidents

4.2. Incident-Response-Management

Technical measures	Organizational measures
✓ Use of a firewall and regular updates ✓ Use of a spam filter and regular updates ✓ Intrusion detection system ✓ Web application firewall ✓ Communication Management in CMI	✓ Documented process for detecting and reporting security incidents (including reporting requirements to regulatory authorities) ✓ Documented procedure for handling security incidents ✓ Involvement of DSB in security incidents

WidasConcepts GmbH
Maybachstraße 2
71299 Wimsheim

T: +49 7044 95103 100
E: datenschutz@widas.de

www.widas.de

	✓ Formal Process and Responsibilities for the Follow-Up of Security Incidents

4.3. Privacy-friendly default settings

Technical measures	Organizational measures
✓ No more personal data is collected than is necessary for the specific purpose and for protection, as determined by the customer where applicable ✓ Easy exercise of the right of withdrawal through a user-friendly interface (defined by the customer) ✓ Out-of-the-box consent management ✓ Fine-grained assignment of rights and roles	✓ Data Protection Policy: “Privacy by Default/Design”

4.4. Task Control

Technical measures	Organizational measures
✓ Logging and Monitoring of Remote Access by External Users	✓ Prior review of the security measures implemented by the contractor, including certifications where applicable ✓ Work instructions for supplier management and evaluation ✓ Selection of contractors is conducted in accordance with due diligence principles, including documentation of the evaluation in electronic form ✓ Conclusion of the necessary data processing agreement ✓ Regulations governing the use of additional subcontractors ✓ Ensuring the destruction of data upon completion of the contract

WidasConcepts GmbH
Maybachstraße 2
71299 Wimsheim

T: +49 7044 95103 100
E: datenschutz@widas.de

www.widas.de

	✓ Requiring the contractor's employees to maintain data confidentiality ✓ Requiring the contractor to appoint a data protection officer if such an appointment is mandatory ✓ For long-term collaborations: Ongoing review of the contractor and its level of data protection

5. Certification

The Widas Group is ISO 9001 and ISO 27001 certified. Quality management in accordance with ISO 9001 and information security management in accordance with ISO 27001 are integral parts of Widas' services. With the "Software Hosted in Germany" seal of approval, we guarantee the use of German data centers and German contract law. Furthermore, it certifies compliance with the German standard for data protection in accordance with the GDPR. Companies awarded the "Software Hosted in Germany" seal submit the current status of their technical and organizational measures regarding data protection (see GDPR) to BITMi e.V. According to BITMi, the seal stands for German quality, best-in-class availability, future-proofing, and trust in data protection.

Measure	Comments
✓ (Physical) Access Control	ISO27001 and ISO9001 certified
✓ Authentication	ISO27001 and ISO9001 certified
✓ Authorization	ISO27001 and ISO9001 certified
✓ Disclosure Control	ISO27001 and ISO9001 certified
✓ Input Control	ISO27001 and ISO9001 certified
✓ Task Control	ISO27001 and ISO9001 certified
✓ Availability Control	ISO27001 and ISO9001 certified
✓ Separation Control	ISO27001 and ISO9001 certified
✓ Internal Organization	ISO27001 and ISO9001 certified