WidasConcepts GmbH
Maybachstraße 2
71299 Wimsheim

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

www.widas.de

Stand: April 2026

Technische und organisatorische Maßnahmen (TOM)

Die technischen und organisatorischen Maßnahmen werden gemeinsam von Auftragnehmer (AN) und der Widas Gruppe entsprechend Art. 32 DSGVO umgesetzt. Sie werden vom AN und der Widas Gruppe laufend nach Machbarkeit und Stand der Technik, unter anderem auch im Sinne der aktive ISO27001 Zertifizierung, weiterentwickelt und auf ein höheres Sicherheits- und Schutzniveau gebracht.

1. Vertraulichkeit

1.1. Zutrittskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
✓ Alarmanlage ✓ Automatische Zutrittskontrolle ✓ Betrugserkennung bei der Zutrittskontrolle ✓ Elektronisches Schließsystem ✓ Sicherheitstür WidasCloud (T 90-1-FSA Stahl-Feuerschutztür geprüft nach DIN 4102 und keine Fenster. ✓ Videoüberwachung der Eingänge ✓ Bewegungsmelder und Videoüberwachung der Innenräume	✓ Schlüsselregelung/Liste ✓ Protokoll der Besucher/ digitale Besucherakte ✓ Besucher in Begleitung durch Mitarbeiter ✓ Sorgfalt bei Auswahl Reinigungsdienst ✓ Richtlinie Informationssicherheit ✓ Arbeitsanweisung Betriebssicherheit ✓ Arbeitsanweisung Zutrittssteuerung ✓ Zertifizierungsnachweise bei Sub-Auftragsverarbeitungsunternehmen

1.2. Zugangskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
✓ Einsatz von Anti-Viren-Software ✓ Einsatz einer Hardware-Firewall ✓ Einsatz von Web Application Firewall ✓ Authentifizierung mind. über Nutzername/ starkes Passwort inkl. Betrugserkennung ✓ Verschlüsselung von Datenträgern	✓ Verwaltung von Benutzerberechtigungen ✓ Benutzerprofile ✓ Richtlinie Informationssicherheit ✓ Arbeitsanweisung Betriebs-sicherheit ✓ Arbeitsanweisung Zugangs-steuerung

WidasConcepts GmbH
Maybachstraße 2
71299 Wimsheim

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

www.widas.de

✓ Automatische Desktopsperre ✓ 2-Faktor-Authentifizierung im RZ-Betrieb und bei allen IT-Systemen ✓ Einsatz von VPN-Technologie	✓ Arbeitsanweisung zur Benutzung von Endgeräten (Mobile Device Policy) ✓ Feingranulare Rechtevergabe

1.3. Zugriffskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
✓ Aktenschredder ✓ Physische Löschung von Datenträgern ✓ Protokollierung bei Zugriffen auf Anwendung bei Eingabe, Änderung und Löschung von Daten (Event-Driven-Architecture) ✓ Zugriffe SSH verschlüsselt ✓ Zertifizierte SSL-Verschlüsselung	✓ Einsatz Berechtigungskonzepte ✓ feingranulares Berechtigungs-management durch cidaas ✓ Auf Notwendigste reduzierte Anzahl an Administratoren ✓ Verwaltung Benutzer-berechtigungen durch Administratoren ✓ Richtlinie Informationssicherheit ✓ Arbeitsanweisung Kommunikationssicherheit ✓ Arbeitsanweisung Umgang mit Informationen und Werten

1.4. Trennungskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
✓ Trennung von Produktiv- und Testsystem ✓ Logische Mandantentrennung (durch Virtualisierung) ✓ Logische Trennung von Kundensystemen ✓ Staging vor Entwicklungs-, Test und Produktivumgebung	✓ Steuerung von Berechtigungskonzept ✓ Festlegung von Datenbankrechten ✓ Richtlinie Informationssicherheit ✓ Richtlinie Datenschutz ✓ Arbeitsanweisung Betriebs-sicherheit ✓ Arbeitsanweisung Sicherheit inkl. Quality Assurance in der Softwareentwicklung

1.5. Pseudonymisierung

Technische Maßnahmen	Organisatorische Maßnahmen
✓ Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten	✓ Interne Anweisung: personen-bezogene Daten sind im Falle einer

WidasConcepts GmbH
Maybachstraße 2
71299 Wimsheim

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

www.widas.de

und Aufbewahrung in getrenntem und abgesichertem System (mögl. verschlüsselt)	Weitergabe, soweit möglich, zu pseudonymisieren ✓ Richtlinie Datenschutz ✓ Richtlinie Informationssicherheit ✓ Richtlinie kryptografische Maßnahmen

2. Integrität

2.1. Weitergabekontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
✓ Einsatz von VPN ✓ SSL/TLS Verschlüsselung zum sicheren Transport ✓ Protokollierung von Zugriffen und Abrufen	✓ Weitergabe in anonymisierter oder pseudonymisierter Form ✓ Richtlinie Informationssicherheit ✓ Richtlinie Datenschutz

2.2. Eingabekontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
✓ Protokollierung von Eingabe, Änderung und Löschung von Daten ✓ Manuelle oder automatisierte Kontrolle der Protokolle (unter Berücksichtigung Richtlinie Informationssicherheit)	✓ Vergabe von Rechten zur Eingabe, Änderung und Löschung über definierte Rollen im Berechtigungskonzept ✓ Nachvollziehbarkeit der Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) ✓ Richtlinie Informationssicherheit ✓ Arbeitsanweisung für Benutzer ✓ Übersicht, Monitoring, mit wann und wie welche Eingabe, Änderung und Löschung erfolgte

3. Verfügbarkeit und Belastbarkeit

3.1. Verfügbarkeitskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
✓ Klimatisierte Räume insbesondere Serverraum	✓ Backup & Recovery-Konzept ✓ Kontrolle des Sicherungsvorgangs ✓ Datensicherungen sind an sicherem Ort gelagert

WidasConcepts GmbH
Maybachstraße 2
71299 Wimsheim

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

www.widas.de

✓ Rauchfrüherkennungs- und Brandmeldeanlagen/ Gefahren-meldeanlage ✓ Überwachung der Temperatur und Luftfeuchtigkeit in Serverräumen ✓ Gaslöschanlagen in den Serverräumen ✓ Lokale unterbrechungsfreie Stromversorgung (USV und Netzersatzanlage) ✓ Angepasste Aufteilung der Stromkreise ✓ Überspannungsschutz ✓ Fernanzeige von Störungen ✓ Redundanzen in der technischen Infrastruktur ✓ Verteilung auf mehrere Datacenter	✓ Ggfs. Service Manager bei Partnerrechenzentren ✓ Existenz eines Notfallplans ✓ Planung des Servereinsatzes ✓ Automatisierte Provisionierungs-prozesse ✓ Richtlinie Informationssicherheit ✓ Kontinuierliches Monitoring und Health-Checks ✓ Keine sanitären Anschlüsse im oder oberhalb des Serverraums ✓ Regelmäßige Tests des Diesel-aggregates ✓ Bereitschaftsdienst

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1. Datenschutzmaßnahmen

Technische Maßnahmen	Organisatorische Maßnahmen
✓ Sicherheitszertifizierung nach ISO27001 ✓ Überprüfung der Wirksamkeit der TOM mind. jährlich inkl. Aktualisierung ✓ Risk Assessment inkl. Datenschutzprüfpunkte ✓ Zentrale Dokumentation aller Regelungen zum Datenschutz und Sicherheit mit Zugriffsmöglichkeit für Mitarbeiter	✓ Verpflichtung der Mitarbeiter auf Vertraulichkeit/ Datengeheimnis ✓ Regelmäßige Sensibilisierung der Mitarbeiter (Security-Awareness) ✓ Datenschutzbeauftragter und Informationssicherheits-Beauftragter ✓ Die Datenschutz-Folgeabschätzung wird bei Bedarf durchgeführt ✓ ISO27001 Zertifizierung und jährliche Überwachungsaudits ✓ Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach ✓ Formaler Prozess und Verantwortlichkeiten zur

WidasConcepts GmbH
Maybachstraße 2
71299 Wimsheim

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

www.widas.de

	✓ Nachbearbeitung von Sicherheitsvorfällen

4.2. Incident-Response-Management

Technische Maßnahmen	Organisatorische Maßnahmen
✓ Einsatz von Firewall und regelmäßige Aktualisierung ✓ Einsatz von Spamfilter, regelmäßige Aktualisierung ✓ Intrusion Detection System ✓ Web Application Firewall ✓ Communication Management in CMI	✓ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde) ✓ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen ✓ Einbindung von DSB in Sicherheitsvorfälle ✓ Formaler Prozess und Verant-wortlichkeit zur Nachbearbeitung von Sicherheitsvorfällen

4.3. Datenschutzfreundliche Voreinstellungen

Technische Maßnahmen	Organisatorische Maßnahmen
✓ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck und dem Schutz erforderlich ggfs. durch den Kunden beschlossen ✓ Einfache Ausübung des Widerrufsrechts durch nutzerfreundliche Darstellung (durch Kunden definiert) ✓ out-of-the Box Einwilligungsmanagement ✓ feingranulare Rechte- und Rollenvergabe	✓ Richtlinie Datenschutz „Privacy by Default/Design“

WidasConcepts GmbH
Maybachstraße 2
71299 Wimsheim

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

www.widas.de

4.4. Auftragskontrolle

Technische Maßnahmen	Organisatorische Maßnahmen
✓ Protokollierung und Überwachung von Remote-Zugriffen Externer	✓ vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen ggfs. über Zertifizierungen ✓ Arbeitsanweisung Lieferantenmanagement und -bewertung ✓ Auswahl der Auftragnehmer wird unter Sorgfaltsgesichtspunkten durchgeführt inkl. Dokumentation der Evaluierung in elektronischer Form ✓ Abschluss der notwendigen Vereinbarung zur Auftrags-verarbeitung ✓ Regelungen zum Einsatz weiterer Subunternehmer ✓ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags ✓ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis ✓ Verpflichtung zur Bestellung eines Datenschutzbeauftragen durch den Auftragnehmer bei Vorliegen einer Bestellpflicht ✓ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

5. Zertifizierung

Die Widas Gruppe ist ISO9001 und ISO27001 zertifiziert. Das Qualitäts-management nach ISO9001 und das Informationssicherheitsmanagement nach ISO27001 sind wesentlicher Bestandteil der Leistungen von Widas. Mit dem Gütesiegel „Software Hosted in Germany“ garantieren wir deutsche Rechenzentren

WidasConcepts GmbH
Maybachstraße 2
71299 Wimsheim

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

www.widas.de

und die Nutzung deutschen Vertragsrechts. Außerdem wird bescheinigt, dass der deutsche Standard beim Datenschutz gemäß DSGVO eingehalten wird. Die mit dem Siegel „Software Hosted in Germany“ ausgezeichneten Unternehmen hinterlegen den jeweils aktuellen Standard ihrer technischen und organisatorischen Maßnahmen in Bezug auf den Datenschutz (vgl. DSGVO) beim BITMi e.V. Das Gütesiegel steht laut dem BITMi für deutsche Qualität, beste Verfügbarkeit, Zukunftssicherheit und Vertrauen in den Datenschutz.

Maßnahme	Kommentare
✓ Zutrittskontrolle	ISO27001 und ISO9001 zertifiziert
✓ Zugangskontrolle	ISO27001 und ISO9001 zertifiziert
✓ Zugriffskontrolle	ISO27001 und ISO9001 zertifiziert
✓ Weitergabekontrolle	ISO27001 und ISO9001 zertifiziert
✓ Eingabekontrolle	ISO27001 und ISO9001 zertifiziert
✓ Auftragskontrolle	ISO27001 und ISO9001 zertifiziert
✓ Verfügbarkeitskontrolle	ISO27001 und ISO9001 zertifiziert
✓ Trennungskontrolle	ISO27001 und ISO9001 zertifiziert
✓ Innerbetriebliche Organisation	ISO27001 und ISO9001 zertifiziert