

Technische, organisatorische Maßnahmen (TOMs)



Vertragspartner	SEEWARA GmbH und der jeweils betroffene Nutzerkreis gemäß Dokumenttitel
Anwendungsbereich	medicalseign.de und app.medicalseign.de
Hinweis	Arbeitsfähige Erstfassung für den operativen Plattformbetrieb

I. Risikoorientierter Ansatz

SEEWARA trifft unter Berücksichtigung von Stand der Technik, Implementierungskosten, Art, Umfang, Umständen und Zwecken der Verarbeitung sowie Eintrittswahrscheinlichkeit und Schwere möglicher Risiken angemessene Maßnahmen. Wegen möglicher Berufsgeheimnisse und besonderer Datenkategorien wird für MedicalSign ein erhöhtes Vertraulichkeits- und Berechtigungsschutzniveau zugrunde gelegt.

II. Zutritts- und Infrastrukturkontrolle

- Betrieb in professionellen Rechenzentrumsumgebungen;
- physische Sicherheitsmaßnahmen des Infrastrukturproviders;
- kein regulärer physischer Zugriff von Anwendungspersonal auf Serverhardware;
- Dokumentation wesentlicher Infrastruktur- und Providerabhängigkeiten.

III. Zugangskontrolle

- personalisierte Benutzerkonten;
- starke Passwortspeicherung mittels zeitgemäßer Hashverfahren;
- 2FA für administrative und – soweit vorgesehen – Nutzerzugänge;
- Sitzungsmanagement, Sperr- und Rate-Limit-Mechanismen;
- Protokollierung sicherheitsrelevanter Login- und Authentifizierungsereignisse.

IV. Zugriffskontrolle und Mandantentrennung

- rollen- und organisationsbezogene Berechtigungen nach Least-Privilege;
- logische Trennung von Mandanten, Organisationen und Vorgängen;
- administrative Zugriffe nur für autorisierte Personen und nur bei betrieblichem Bedarf;
- regelmäßige Überprüfung privilegierter Rechte;
- technische Maßnahmen gegen IDOR, unberechtigte Objektzugriffe und mandantenübergreifende Datenabfragen.

V. Verschlüsselung und Übertragung

- TLS-verschlüsselte Übertragung;
- verschlüsselte oder angemessen geschützte Speicherung besonders sensibler Secrets und Tokens;
- keine Übermittlung produktiver Mandatsdaten an nicht freigegebene Drittanbieter;
- gesicherte APIs, tokenisierte Links und zeitlich begrenzte Zugriffsmittel, soweit eingesetzt.

VI. Eingabe-, Änderungs- und Nachvollziehbarkeitskontrolle

- Auditierung wesentlicher Account-, Rollen-, Status- und Sicherheitsereignisse;
- Versionierung oder Änderungsnachvollziehbarkeit für kritische Vorgangsdaten, soweit technisch vorgesehen;
- Zeitstempel und Zuordnung von Nutzeraktionen;
- Schutz von Logs vor unbefugter Veränderung und unangemessen langer Speicherung.

VII. Verfügbarkeit und Wiederherstellung

- regelmäßige Datensicherungen nach dokumentiertem Sicherungskonzept;
- Wiederherstellungsprozesse und stichprobenartige Restore-Tests;
- Monitoring zentraler Dienste und Fehlerzustände;
- Incident- und Eskalationsprozesse;
- Notfallmaßnahmen für kompromittierte Konten, Tokens oder Zugangsdaten.

VIII. Datenschutz durch Technikgestaltung

- Datenminimierung und zweckbezogene Felder;
- Standardkonfigurationen mit restriktiven Berechtigungen;
- Trennung von Produktiv-, Test- und Entwicklungsdaten;
- keine Verwendung realer sensibler Daten in Entwicklung/Test, soweit vermeidbar;
- Anonymisierung/Datensuppression für Analytics, sobald Personenbezug nicht erforderlich ist.

IX. Organisation

- Vertraulichkeitsverpflichtung und gegebenenfalls §203-Verpflichtung eingebundener Personen;
- Need-to-know und dokumentierte Admin-Berechtigungen;
- Vulnerability-, Patch- und Updateprozesse;
- Prozess für Datenschutzverletzungen und Sicherheitsvorfälle;
- regelmäßige Überprüfung der Angemessenheit des Schutzniveaus.

X. AI/OCR und externe Verarbeitung

AI-/OCR-Dienste dürfen Produktivdaten nur erhalten, wenn sie für den konkreten Zweck freigegeben, datenschutzrechtlich vertraglich eingebunden und hinsichtlich Datenstandort, Training/Weiterverwendung, Löschung und Zugriff angemessen bewertet sind. Produktivdaten dürfen nicht stillschweigend für Modelltraining eines Drittanbieters freigegeben werden.