Candis

Cybersecurity & Datenschutz bei Candis

Kurzübersicht für Medizinische Versorgungszentren
Candis ist technisch und organisatorisch so aufgestellt, dass auch besonders schützenswerte personenbezogene Daten – einschließlich sensibler Daten nach Art. 9 DSGVO – sicher verarbeitet werden können. Die nachfolgende Übersicht gibt einen kompakten Einblick in unsere Sicherheitsarchitektur und Datenschutzmaßnahmen.

1. Rechtliche & organisatorische Grundlage

Candis verarbeitet Daten ausschließlich im Rahmen der vertraglich vereinbarten Leistungserbringung. Eine eigenständige Nutzung von Kundendaten erfolgt nicht.

Unsere Sicherheits- und Datenschutzmaßnahmen orientieren sich an:

- EU-Datenschutz-Grundverordnung (DSGVO)
- Bundesdatenschutzgesetz (BDSG)
- IDW PS 880 (durchgeführtes Audit)
- ISO/IEC 27001 Kontrollzielen (strukturelle Ausrichtung)
- Auftragsverarbeitungsvertrag (Art. 28 DSGVO)
- Technisch-organisatorische Maßnahmen (TOM)
- Mitarbeiterverpflichtung zur Verschwiegenheit
- Transparente Subunternehmerliste

2. Hosting & Infrastruktur

Candis betreibt seine Plattform als Software-as-a-Service (SaaS) auf:
Amazon Web Services (AWS); Region: Frankfurt am Main (EU)

Sicherheitsmerkmale:

- Verarbeitung und Speicherung innerhalb der EU
- Mandantentrennung (logische Isolation)
- Redundante Infrastruktur
- Hochverfügbarkeitsarchitektur
- Netzwerksegmentierung

3. Zugriffskontrolle & Identitätsmanagement

Der Zugriff auf Systeme und Daten erfolgt nach dem Prinzip der minimalen Rechtevergabe (Least Privilege).

Maßnahmen:

- Rollenbasierte Zugriffskontrolle (RBAC)
- Individuelle Benutzerkonten und privilegierter Zugriff Policy
- Multi-Faktor-Authentifizierung (MFA) für administrative Zugriffe
- Regelmäßige Überprüfung von Berechtigungen
- Sofortige Entziehung von Zugriffsrechten bei Rollenwechsel oder Ausscheiden

4. Verschlüsselung & Datensicherheit

Candis setzt aktuelle kryptographische Standards ein:

- TLS 1.2 oder höher für Datenübertragung
- AES-256 Verschlüsselung für gespeicherte Daten
- HTTPS-gesicherte Kommunikation
- Absicherung aller API-Schnittstellen

Damit wird Vertraulichkeit und Integrität der Daten sichergestellt.

5. Logging, Monitoring & Auditierbarkeit

Sicherheitsrelevante Ereignisse werden zentral protokolliert und überwacht:

- Infrastruktur-Logging (Cloud-Ebene)
- Applikations-Logging
- Audit-Trails für sicherheitskritische Aktionen
- Anomalie-Erkennung
- Regelmäßige Log-Reviews

Auf berechtigte Anfrage können relevante Audit-Informationen bereitgestellt werden.

6. Vulnerability Management & Penetration Tests

Candis betreibt ein kontinuierliches Schwachstellenmanagement:

- Regelmäßige externe Penetrationstests
- Automatisierte Vulnerability-Scans
- Strukturierter Patch-Prozess
- Dokumentierte Remediation identifizierter Schwachstellen
- Secure Software Development Lifecycle (SDLC)

Identifizierte Schwachstellen werden risikobasiert priorisiert und zeitnah behoben.

7. Incident Response

Candis verfügt über einen dokumentierten Incident-Response-Prozess.
Dieser umfasst:

- Erkennung und Klassifizierung von Sicherheitsvorfällen
- Definierte Eskalationswege
- Interne Verantwortlichkeiten
- Kundeninformation gemäß DSGVO-Anforderungen
- Post-Incident-Analyse zur kontinuierlichen Verbesserung

In den letzten fünf Jahren gab es keine meldepflichtigen Datenschutzvorfälle.

8. Business Continuity & Disaster Recovery

Zur Sicherstellung der Verfügbarkeit bestehen dokumentierte Notfall- und Wiederanlaufpläne.

- Regelmäßige Datensicherungen
- Getestete Wiederherstellungsverfahren
- Recovery Time Objective (RTO): 12 Stunden
- Recovery Point Objective (RPO): 12 Stunden

Damit kann der Betrieb im Störungsfall strukturiert wiederhergestellt werden.

9. Subunternehmer & Transparenz

Candis setzt ausgewählte, vertraglich gebundene Subunternehmer ein, u. a.:

- Amazon Web Services (Hosting)
- Gini GmbH (Dokumentenerkennung)
- Mailjet SAS (System-E-Mails)
- Google Cloud (KI-Services)

Alle Subunternehmer sind datenschutzrechtlich verpflichtet und verarbeiten Daten ausschließlich im Rahmen der Weisung von Candis.

10. Schulung & Sensibilisierung

Mitarbeitende werden regelmäßig geschult:

- Mindestens jährliche Datenschutzschulung
- IT-Sicherheits-Trainings
- Entwickler-Onboarding mit Security-Fokus
- Sensibilisierung für Social Engineering

Alle Mitarbeitenden sind schriftlich zur Vertraulichkeit verpflichtet.