Konformitätserklärung zur EU AI Act & DSGVO Compliance

Letzte Aktualisierung: November 2025
Dokumentenklassifikation: Vertraulich (C2) – Nur für Compliance-Zwecke

1. Regulatorische Compliance

Enneo GmbH bestätigt die vollständige Konformität ihrer KI-gestützten Kundenservice-Plattform mit:

- DSGVO (EU 2016/679): Vollständige Einhaltung aller Bestimmungen, einschließlich Art. 28 zur Auftragsverarbeitung
- EU AI Act (EU 2024/1689): Klassifizierung als KI-System mit begrenztem Risiko, Transparenzverpflichtungen erfüllt
- BDSG: Konformität mit nationalen Datenschutzbestimmungen

2. Technische Architektur

- Hosting: Selbstgehostete Infrastruktur auf dedizierten Servern bei Hetzner und Aixit (Deutschland)
- Cloud-Dienste: Microsoft Azure, AWS, Google Cloud – ausschließlich unter EU-Datenschutzbedingungen
- Verschlüsselung: AES-256 bei Speicherung, TLS 1.3 bei Übertragung
- Datenklassifikation: C0–C4, wobei C3 und C4 besonders schutzbedürftig sind (z. B. Kundendaten, Bankdaten, Gehaltsdaten)
- Netzwerkzonen: Dev-, Produktions- und Admin-Netzwerke mit Firewall-Segmentierung
- Zugriffsrechte: Rollenbasiert, mit 2FA und Named Accounts, Zugriff nur nach Freigabe durch Gründer

3. Auftragsverarbeitung

- Rolle: Enneo agiert als Auftragsverarbeiter gemäß Art. 28 DSGVO
- Rechtsgrundlage: AVV mit Kunden und Subunternehmern
- Subunternehmer:
- Hetzner, Aixit – Hosting
- Microsoft, AWS, Google – KI-Dienste
- OpenAI, Cohere, Groq, Eleven Labs – KI-Modelle (nur bei expliziter Kundenfreigabe)
- Twilio Sendgrid, A&O Fischer – Nur wenn E-Mail bzw. Briefversand über Enneo direkt (und nicht über den Kunden) Teil des Leistungsumfangs ist

4. Betroffenenrechte

- Technische Umsetzung: Auskunft, Berichtigung, Löschung, Datenportabilität
- Löschung auf Anfrage: Innerhalb von 30 Tagen
- Standardlöschfrist: 4 Jahre nach letzter Aktivität
- Kontakt: datenschutz@enneo.ai

5. Datenverarbeitungsmethodik

- Analyse: KI-gestützte Verarbeitung von Kundenanfragen, keine biometrische Auswertung

- Bias-Minimierung: Durch Design und objektive Kriterien
- Keine Speicherung für Trainingszwecke: KI-Dienste nutzen Daten ausschließlich zur Laufzeit
- Keine Nutzung für Leistungs- oder Verhaltenskontrolle

6. Sicherheitsmaßnahmen

- Zero-Trust-Prinzip
- SOC 2 Type II Zertifizierung (in Vorbereitung)
- Penetrationstests: Regelmäßig durch externe Anbieter
- Monitoring: 24/7 automatisierte Überwachung
- Vorfallreaktion: DSGVO-konform je nach SLA zwischen 2 und 72 Stunden
- Backup:
- Tägliche verschlüsselte Backups
- Validierung durch Backup-Skripte
- Live-Synchronisation für Premium-Kunden

7. Überwachung & Updates

- Compliance-Audits: Regelmäßig durch interne und externe Stellen
- Risikobewertung: Kontinuierlich
- DSFA-Updates: Bei wesentlichen Änderungen der Architektur oder Datenverarbeitung

8. Rechtliche Verbindlichkeit

- Anwendbares Recht: Bundesrepublik Deutschland
- Verantwortlich für Datenschutz: Dr. Richard Lohwasser
- Gültigkeit: Bis auf Widerruf
- Nächste Überprüfung: November 2026