Konformitätserklärung zur EU AI Act & DSGVO Compliance

Letzte Aktualisierung: August 2026

1. Regulatorische Compliance

Enneo GmbH verarbeitet personenbezogene Daten im Rahmen ihrer KI-gestützten Kundenservice-Plattform nach Maßgabe der folgenden Rahmenwerke:

- DSGVO (EU 2016/679): Verarbeitung nach Maßgabe der Anlagen AVV und TOM, einschließlich Art. 28 zur Auftragsverarbeitung
- EU AI Act (EU 2024/1689): nach eigener Bewertung kein Hochrisiko-System im Sinne von Anhang III; Transparenzpflichten nach Art. 50 durch aktivierte Voreinstellungen umgesetzt; Deaktivierung nur durch ausdrückliche Kundenentscheidung mit Verantwortungsübergang (Einzelheiten: DSFA Abschnitt 3.3 und 6.5)
- BDSG: Konformität mit nationalen Datenschutzbestimmungen

2. Technische Architektur

- Hosting: Selbstgehostete Infrastruktur auf dedizierten Servern — Betrieb: Deutschland (Hetzner); Backup: Deutschland und Finnland (Aixit bzw. Hetzner)
- 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: Die vollständige, verbindliche Liste der Unterauftragsverarbeiter — Hosting-, KI- sowie Versand- und Telefonie-Dienstleister, einschließlich Anschriften und Einsatzbedingungen (Standardbetrieb, nur nach expliziter Kundenfreigabe, nur wenn beauftragt) — enthält AVV Ziffer 7.1 (docs.enneo.ai/de/legal/avv). Sie wird ausschließlich dort gepflegt und in diesem Dokument nicht dupliziert.

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
- Jährliche interne Sicherheitsaudits und Selbstauskunft gemäß AVV Ziffer 9.3; eine SOC 2- oder ISO-27001-Zertifizierung durch eine unabhängige Instanz wird evaluiert, ist derzeit aber nicht abgeschlossen
- Penetrationstests: Regelmäßig durch externe Anbieter
- Monitoring: 24/7 automatisierte Überwachung
- Vorfallreaktion: Meldung von Datenschutzverletzungen an den Auftraggeber unverzüglich (AVV Ziffer 6.6), zur Wahrung der 72-Stunden-Frist des Art. 33 DSGVO; Incident-Reaktionszeiten im Übrigen gemäß SLA Abschnitt 3.1
- Backup:
- Tägliche verschlüsselte Backups
- Validierung durch Backup-Skripte
- Aufbewahrung und Recovery-Kennzahlen je Service Level: siehe Anlage „Service Level Agreement“ (Abschnitt 3.1)

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
- Interne Datenschutz-Governance: Geschäftsführung (Dr. Richard Lohwasser); Funktions-Kontaktstelle datenschutz@enneo.ai (siehe DSFA Abschnitt 3.2)
- Gültigkeit: Bis auf Widerruf
- Nächste Überprüfung: August 2027