Datenschutz-Folgenabschätzung (DSFA)

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

1. Zusammenfassung

Enneo GmbH bietet eine KI-gestützte Kundenservice-Plattform, die Kundenanfragen automatisiert beantwortet oder menschliche Agenten durch Co-Pilot-Funktionen unterstützt. Diese DSFA wurde gemäß Artikel 35 DSGVO erstellt und berücksichtigt die Empfehlungen der Artikel-29-Datenschutzgruppe sowie des Europäischen Datenschutzausschusses.

Kernaussagen:

Thema	Beschreibung
DSGVO-Risikobewertung	Datenschutzrisiken wurden durch technische und organisatorische Maßnahmen auf ein akzeptables Niveau reduziert.
EU KI-Gesetz	Enneo wird als System mit begrenztem Risiko eingestuft.
Infrastruktur	Hosting ausschließlich in der EU (Hetzner, Aixit).
Datenspeicherung	Verschlüsselte Speicherung, automatisierte Löschfristen.

2. Umfang und Rechtsrahmen

2.1 Regulatorische Compliance

- DSGVO Artikel 35: Verpflichtende DSFA
- DSGVO Artikel 6, 9, 28: Rechtmäßigkeit der Verarbeitung, besondere Datenkategorien, Auftragsverarbeitung
- EU KI Act Artikel 50–56: Transparenz und menschliche Aufsicht
- BDSG: Nationale Ergänzungen

2.2 Beziehung Verantwortlicher / Auftragsverarbeiter

- Kunde: Verantwortlicher gemäß Art. 4 Nr. 7 DSGVO
- Enneo: Auftragsverarbeiter gemäß Art. 4 Nr. 8 DSGVO
- Rechtsgrundlage: AVV gemäß Art. 28 DSGVO
- Haftung: Klare Zuweisung gemäß AVV

3. Datenverarbeitungsvorgänge

3.1 Kategorien personenbezogener Daten

- Standarddaten: Name, E-Mail, Benutzerkonten, Rollen, Zugriffsrechte
- Kommunikationsdaten: Kundenanfragen, Chatverläufe, Ticketinhalte
- Technische Daten: IP-Adressen, Logdaten, Netzwerkverbindungen
- Besondere Kategorien: Sprachaufzeichnungen (sofern aktiviert)

3.2 Verarbeitungsaktivitäten

- Automatisierte Analyse und Beantwortung von Kundenanfragen
- Unterstützung menschlicher Agenten durch KI-Vorschläge
- Speicherung und Protokollierung zur Qualitätssicherung
- Aggregierte Auswertungen zur Systemoptimierung

4. Technische Architektur & Sicherheit

4.1 Infrastruktur

- Hosting: Hetzner (Deutschland), Aixit (Backup)
- Datenklassifikation: C3 (GDPR-relevant), C4 (besonders sensibel)
- Netzwerksicherheit: TLS 1.3, Firewall-Zonen (Dev, Prod, Admin)
- Zugriffsrechte: Rollenbasiert, 2FA, Named Accounts

4.2 KI-Integration

- KI-Modelle via Microsoft, Google, OpenAI, Anthropic, Meta
- Datenverarbeitung über REST-API, keine Trainingsnutzung
- EU-Datenresidenz bei Microsoft und Google garantiert

5. Risikobewertung & Risikominderung

Risiko	Auswirkung	Wahrscheinlichkeit	Maßnahme	Restrisiko
Unbefugte Offenlegung	Hoch	Niedrig	Verschlüsselung, Zugriffskontrollen	Akzeptabel
KI-Bias	Mittel	Niedrig	Transkript-only, menschliche Kontrolle	Akzeptabel
Technische Sicherheitsverletzung	Hoch	Sehr niedrig	Penetrationstests, Monitoring	Akzeptabel
Internationale Datenübertragung	Hoch	Niedrig	EU-Hosting, vertragliche Garantien	Akzeptabel

6. Betroffenenrechte

- Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit
- Umsetzung über Support-Kanäle und Datenschutzbeauftragten
- Löschfristen: Standard 4 Jahre, auf Anfrage sofortige Löschung

7. Lieferantenmanagement

- Subunternehmer: Hetzner, Aixit, Microsoft, Google, Microsoft
- Vertragliche Absicherung: AVV mit allen Dienstleistern
- Auditrechte: gemäß AVV und DSGVO
- Datenverarbeitung ausschließlich in der EU oder mit SCCs

8. Überwachung & kontinuierliche Verbesserung

- Monatliche Überprüfung der Sicherheitsverfahren
- Quartärliche Überprüfung des KI-Bias

- Jährliche Überprüfung der DSFA
- Monitoring: 24/7, automatisierte Vorfallreaktion
- Audits: Regelmäßige interne und externe Prüfungen
- Backup: Tägliche verschlüsselte Backups, 30 Tage Retention
- Vulnerability Management: Snyk-Scans, CI/CD-Integrationen

9. Fazit

Enneo GmbH erfüllt die Anforderungen der DSGVO und des EU KI Acts durch eine datenschutzfreundliche Architektur, strenge Zugriffskontrollen und transparente Prozesse. Die DSFA zeigt, dass die Risiken der Datenverarbeitung durch Enneo auf ein akzeptables Maß reduziert sind.