Datenschutz-Folgenabschätzung (DSFA)

Letzte Aktualisierung: August 2026

1. Zusammenfassung

Enneo GmbH bietet eine KI-gestützte Kundenservice-Plattform, die Kundenanfragen aus allen gängigen Kanälen (E-Mail, Chat, Telefonie, Post) automatisiert erkennt, bewertet und – je nach Automatisierungsgrad – vollständig löst oder menschliche Agenten durch Co-Pilot-Funktionen unterstützt. Diese Datenschutz-Folgenabschätzung (DSFA) wurde von Enneo als Auftragsverarbeiter proaktiv und nach der Systematik des Art. 35 DSGVO erstellt; sie berücksichtigt die Empfehlungen der Artikel-29-Datenschutzgruppe (WP 248) sowie des Europäischen Datenschutzausschusses. Sie beschreibt die Verarbeitungsvorgänge der Plattform systematisch, bewertet Notwendigkeit und Verhältnismäßigkeit, identifiziert Risiken für die Rechte und Freiheiten betroffener Personen und dokumentiert die zu ihrer Eindämmung getroffenen Abhilfemaßnahmen.

Kernaussagen:

Thema	Beschreibung
Rolle dieses Dokuments	Enneo erstellt diese DSFA proaktiv als Auftragsverarbeiter (Art. 28 Abs. 3 lit. f DSGVO). Sie dokumentiert die plattformseitigen Verarbeitungsvorgänge, Risiken und Abhilfemaßnahmen vollständig, sodass der Verantwortliche datenschutzrechtliche Prüfungen zum Einsatz der Plattform — einschließlich einer etwaigen eigenen DSFA — im Wesentlichen auf dieser Grundlage durchführen kann.
DSGVO-Risikobewertung	Datenschutzrisiken wurden durch technische und organisatorische Maßnahmen auf ein akzeptables Niveau reduziert. Kein Risiko verbleibt in der Kategorie „hoch“.
EU KI-Gesetz	Enneo ist nach eigener Bewertung kein Hochrisiko-KI-System i.S.v. Anhang III des AI Act; die Transparenzpflichten nach Art. 50 werden durch aktivierte Voreinstellungen umgesetzt (Abschnitt 3.3).
Infrastruktur	Betrieb ausschließlich in Deutschland (Hetzner); Backups in Deutschland und Finnland (Aixit bzw. Hetzner); dedizierte Instanz mit eigener Datenbank je Mandant.
KI-Verarbeitung	Multi-Modell-Architektur; Standardbetrieb ausschließlich über EU-Rechenzentren (Microsoft Azure Schweden, Google Belgien, AWS Frankfurt, Mistral Frankreich, Nebius Finnland, Media Trooper Deutschland/Niederlande).
Digitale Souveränität	Rein europäische KI-Anbieter (Mistral AI, Nebius, Media Trooper) reduzieren die Abhängigkeit von US-Anbietern; Notbetrieb ohne KI als reines Vorgangsbearbeitungs- und Telefoniesystem möglich.
Datenspeicherung	Verschlüsselte Speicherung, automatisierte und je Mandant konfigurierbare Löschfristen, Protokoll- und Netzwerkdaten stets nach 30 Tagen gelöscht.

2. Zweck, Geltungsbereich und Methodik

2.1 Anlass und Erforderlichkeit der DSFA

Gemäß Art. 35 Abs. 1 DSGVO hat der Verantwortliche eine DSFA durchzuführen, wenn eine Form der Verarbeitung – insbesondere bei Verwendung neuer Technologien – voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Ob dies für den konkreten Einsatz der Enneo-Plattform der Fall ist, beurteilt der Verantwortliche im Rahmen seiner eigenen

Prüfung; das Ergebnis hängt maßgeblich von der von ihm gewählten Ausgestaltung ab (u. a. angebundene Kanäle, Automatisierungsgrade, Gesprächsaufzeichnung, Umfang der übertragenen Daten). Merkmale der Plattform, die bei dieser Prüfung typischerweise zu betrachten sind:

- Einsatz neuer Technologien: große Sprachmodelle (LLMs) zur automatisierten Analyse und Beantwortung von Kundenanliegen
- Verarbeitung der Kundenservice-Kommunikation des Verantwortlichen, je nach Einsatz auch in großem Umfang
- Verarbeitung von Vertrags- und Zahlungsdaten (z. B. Bankverbindung, SEPA-Mandat, Verbrauchsdaten), soweit der Verantwortliche diese überträgt
- Optionale automatisierte Einzelfallbearbeitung (Dunkelverarbeitung) mit konfigurierbarer menschlicher Aufsicht

Unabhängig vom Ergebnis dieser Prüfung erstellt Enneo diese DSFA proaktiv: Sie beschreibt die Verarbeitungsvorgänge der Plattform systematisch, bewertet Notwendigkeit und Verhältnismäßigkeit und dokumentiert Risiken und Abhilfemaßnahmen, sodass der Verantwortliche seine Prüfung — und, soweit er eine eigene DSFA durchführt, auch diese — im Wesentlichen auf dieses Dokument stützen kann. Sie erfüllt zugleich die Unterstützungspflicht des Auftragsverarbeiters aus Art. 28 Abs. 3 lit. f DSGVO.

2.2 Methodik

Die Risikobewertung folgt der Systematik Risiko = Eintrittswahrscheinlichkeit × Schwere der Auswirkung. Beide Dimensionen werden qualitativ auf einer vierstufigen Skala bewertet (sehr niedrig / niedrig / mittel / hoch). Für jedes identifizierte Risiko werden die vorhandenen Abhilfemaßnahmen dokumentiert und das danach verbleibende Restrisiko bewertet. Ein Restrisiko gilt als akzeptabel, wenn es durch Maßnahmen nach dem Stand der Technik soweit reduziert wurde, dass ein hohes Risiko im Sinne des Art. 35 DSGVO nicht mehr besteht. Die DSFA wird jährlich sowie anlassbezogen bei wesentlichen Änderungen der Architektur, der Subunternehmer oder der Verarbeitungszwecke überprüft und fortgeschrieben.

2.3 Referenzdokumente

Diese DSFA ist Teil des Compliance-Dokumentensatzes von Enneo. Die referenzierten Dokumente sind unter docs.enneo.ai/de/legal öffentlich abrufbar:

Dokument	Stand	Inhalt
Auftragsverarbeitungsvertrag (AVV)	August 2026	Vertragsgrundlage nach Art. 28 DSGVO, Datenkategorien, Subunternehmer, Löschfristen
Technische und Organisatorische Maßnahmen (TOM)	August 2026	Maßnahmenkatalog nach den acht Kontrollbereichen (Zutritt bis Trennung)
Datenflussdiagramm	August 2026	Grafische Darstellung der Flüsse personenbezogener Daten
Konformitätserklärung EU AI Act & DSGVO	August 2026	Selbsterklärung zur Konformität mit DSGVO, EU AI Act und BDSG
Leistungsbeschreibung	August 2026	Funktionsumfang der Plattform
Service Level Agreement (SLA)	August 2026	Verfügbarkeits- und Reaktionszeiten
Entfernung personenbezogener Daten aus Ticket-Beispielen	August 2026	Fünfstufiges Verfahren; Restrisiken und Abhilfemaßnahmen in R5 dieser DSFA

3. Rechtsrahmen und Verantwortlichkeiten

3.1 Regulatorische Grundlagen

- DSGVO Artikel 35: Verpflichtende Datenschutz-Folgenabschätzung
- DSGVO Artikel 6, 9, 28: Rechtmäßigkeit der Verarbeitung, besondere Datenkategorien, Auftragsverarbeitung
- DSGVO Artikel 25: Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen
- DSGVO Artikel 32: Sicherheit der Verarbeitung
- DSGVO Artikel 44 ff.: Übermittlungen in Drittländer (nur EU/EWR bzw. mit geeigneten Garantien)
- EU KI Act (EU 2024/1689) Artikel 50–56: Transparenz- und Informationspflichten
- BDSG: Nationale Ergänzungen

3.2 Rollenverteilung

- Kunde (Auftraggeber): Verantwortlicher gemäß Art. 4 Nr. 7 DSGVO; bestimmt Zwecke und Mittel der Verarbeitung, erteilt Weisungen
- Enneo GmbH: Auftragsverarbeiter gemäß Art. 4 Nr. 8 DSGVO; verarbeitet ausschließlich auf dokumentierte Weisung
- Unterauftragsverarbeiter: gemäß AVV Ziffer 7 benannt und vertraglich nach Art. 28 Abs. 4 DSGVO verpflichtet
- Rechtsgrundlage der Auftragsverarbeitung: AVV gemäß Art. 28 DSGVO
- Haftung: klare Zuweisung gemäß AVV und Art. 82 DSGVO

Benannter Weisungsempfänger bei Enneo ist Dr. Richard Lohwasser (richard@enneo.ai). Anfragen zum Datenschutz nimmt Enneo über die Funktions-Kontaktstelle datenschutz@enneo.ai entgegen. Die interne Verantwortung für die Datenschutz-Governance liegt bei der Geschäftsführung (Dr. Richard Lohwasser); ein Datenschutzbeauftragter im Sinne des Art. 37 DSGVO ist derzeit nicht bestellt, da die gesetzlichen Bestellvoraussetzungen nach eigener Prüfung nicht vorliegen (vgl. TOM Ziffer 6.1, AVV Ziffer 6.1).

3.3 Einordnung nach dem EU KI-Gesetz

Enneo ist nach eigener Bewertung kein Hochrisiko-KI-System im Sinne von Anhang III des EU AI Act; „begrenztes Risiko“ ist dabei keine eigenständige gesetzliche Kategorie, sondern eine Einordnungshilfe. Automatisierte Bonitäts- und Mahnentscheidungen sind vertraglich ausgeschlossen (Leistungsbeschreibung, Abschnitt „KI-Einsatz“), sodass sich für die von Enneo angebotene Plattform insoweit keine Ausnahmeprüfung nach Art. 6 Abs. 3 AI Act stellt; die abschließende Einordnung des konkreten Einsatzes verbleibt beim Auftraggeber als Betreiber. Die Transparenzpflichten nach Art. 50 AI Act (Kennzeichnung von KI-Interaktion in Chat, Voice und vollautomatisierter E-Mail, maschinenlesbare Kennzeichnung synthetischer Sprachausgaben) werden durch aktivierte Voreinstellungen umgesetzt; eine Deaktivierung ist nur durch ausdrückliche Konfigurationsentscheidung des Auftraggebers möglich, der insoweit die Verantwortung für die Transparenzpflichten übernimmt (siehe Abschnitt 6.5); Art. 4 AI Act (KI-Kompetenz) wird durch Schulungsunterlagen für Kundenservice-Mitarbeiter des Auftraggebers unterstützt. Details regelt die separate Konformitätserklärung zur EU AI Act & DSGVO Compliance.

4. Beschreibung der Verarbeitungsvorgänge

4.1 Plattformübersicht

Enneo ist eine omnichannel Customer-Service-Plattform: eingehende Kundenanliegen aus E-Mail, Chat, Telefonie und Post (nach Digitalisierung) werden in einer einheitlichen Vorgangsbearbeitung zusammengeführt. Eine KI-Pipeline analysiert jedes Anliegen, erkennt das Thema, identifiziert den Kunden im angebundenen CRM-/ERP-System des Auftraggebers, extrahiert relevante Daten und erstellt einen Lösungs- oder Antwortvorschlag. Je nach konfiguriertem Automatisierungsgrad wird das Anliegen vollautomatisch gelöst oder einem menschlichen Agenten zur Prüfung vorgelegt.

4.2 Systemarchitektur

Die Plattform besteht aus getrennten Microservices, die ausschließlich als Docker-Container in Kubernetes-Clustern auf Servern von Hetzner (Deutschland) betrieben werden. Jeder Mandant erhält eine dedizierte Instanz mit eigener Datenbank; die Instanz wird über eine eindeutige Mandantenkennung konfiguriert und greift ausschließlich auf die eigene Datenhaltung zu.

Dienst	Aufgabe	Personenbezug
Frontend (Ops)	Benutzeroberfläche für Service-Agenten: Ticketbearbeitung, Chat, Telefonie, KI-Kontrollzentrum	Anzeige von Kunden- und Vorgangsdaten
Mind	Fachliches Backend: Vorgangsverwaltung, Geschäftslogik, Datenmodelle, Schnittstellen zu CRM/ERP	Speicherung der Vorgangs- und Kundendaten (MySQL)
Cortex	KI-Pipeline: Anliegenerkennung, Kundenidentifikation, Datenextraktion, OCR, Wissensdatenbank, Entfernung personenbezogener Daten	Verarbeitung von Vorgangsinhalten zur Laufzeit
Auth	Authentifizierung der Nutzer: Login, SSO (Microsoft Azure, Google), Zwei-Faktor-Authentifizierung, Zugriffsprotokollierung	Mitarbeiterdaten der Agenten
IO-Proxy	Echtzeit-Kommunikation (WebSocket), E-Mail-Versand, Anbindung externer Systeme	Durchleitung von Kommunikationsdaten
ACD	Telefonie: SIP-Anbindung, Anrufverteilung, WebRTC, Voicebots, Gesprächsaufzeichnung	Sprachdaten, Gesprächstranskripte
Code-Executor	Abgeschottete Sandbox zur Ausführung kundenspezifischer Integrationslogik	Zur Laufzeit übergebene Vorgangsdaten

Unterstützende Infrastruktur: ein zentrales LLM-Gateway (LiteLLM-Proxy) bündelt und protokolliert alle KI-Aufrufe; Langfuse protokolliert jeden LLM-Aufruf für die Nachvollziehbarkeit; Signoz erfasst Logs und verteilte Traces (OpenTelemetry); Weaviate dient als Vektordatenbank für bereinigte Ticket-Beispiele und Wissensinhalte; Redis dient als Cache; MinIO/S3-kompatibler Objektspeicher hält Dateianhänge und Gesprächsaufzeichnungen.

4.3 Kategorien betroffener Personen und Datenarten

Die verarbeiteten Datenkategorien entsprechen Abschnitt 1.1 des AVV:

Betroffene Personen	Datenarten	Zweck
Mitarbeiter des Auftraggebers (Service-Agenten)	Identifikationsdaten (Name, E-Mail, SSO-Kennung), Rollen und Zugriffsrechte, Kompetenzen (bei Skill-Routing), Ticketbearbeitungsdaten, Protokolldaten, Sprachaufzeichnungen (bei Telefonie)	Identifikation und Authentifizierung, Bestimmung der Zugriffsrechte, Qualitätssicherung, Protokollierung
Kunden und Interessenten des Auftraggebers	Identifikationsdaten (Name, Anschrift, Geburtsdatum, Kontaktdaten, Zählernummer), Vertragsdaten (Kunden-/Vertragsnummer, Bankverbindung, SEPA-Mandat, Rechnungs- und Mahndaten, Ablese- und Verbrauchsdaten), Korrespondenz, Protokolldaten, Sprachaufzeichnungen	Automatisierte Erkennung und Lösung von Kundenanliegen, Erkennung der Kundenzufriedenheit, Statistiken, Qualitätssicherung
Externe Servicedienstleister, die das System nutzen	Identisch mit Mitarbeiterdaten	Identisch mit Mitarbeiterdaten

Kundendaten werden nur verarbeitet, soweit der Auftraggeber sie an Enneo überträgt bzw. sein Abrechnungs- oder CRM-System anbindet. Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sind nicht Gegenstand der bestimmungsgemäßen Verarbeitung; sie können jedoch in Freitext-Anliegen von Kunden enthalten sein und werden dann wie alle Kommunikationsinhalte nach den hier beschriebenen Schutzmaßnahmen behandelt.

4.4 Verarbeitungszwecke

- Automatisierte Erkennung, Klassifizierung und Beantwortung von Kundenanliegen durch KI-Agenten
- Kundenidentifikation anhand der im angebundenen CRM-/ERP-System hinterlegten Daten
- Unterstützung menschlicher Agenten durch KI-Vorschläge (Co-Pilot)
- Dokumentenerkennung (OCR) und strukturierte Datenextraktion, z. B. aus Briefen und Zählerfotos
- Beantwortung inhaltlicher Fragen über eine redaktionell gepflegte Wissensdatenbank (RAG)
- Telefonie einschließlich Anrufverteilung und optionaler Voicebots
- Speicherung und Protokollierung zur Qualitätssicherung
- Aggregierte Auswertungen und Statistiken zur Systemoptimierung

4.5 Ablauf der Verarbeitung

Ein eingehendes Kundenanliegen durchläuft automatisiert folgende Schritte:

- Erkennung: Das Anliegen wird analysiert und dem passenden KI-Agenten zugeordnet (z. B. Zählerstandsmeldung, Rechnungsanfrage)
- Kundenidentifikation: Der Kunde wird anhand der verfügbaren Daten im angebundenen CRM/ERP-System erkannt und legitimiert
- Extraktion: Relevante Informationen werden strukturiert extrahiert (z. B. Zählernummer, Betrag, Vertragsnummer)
- Validierung: Die extrahierten Daten werden gegen das Fachsystem auf Plausibilität geprüft
- Bearbeitung: Je nach Automatisierungsgrad wird das Anliegen vollautomatisch gelöst oder mit einem Antwortvorschlag an einen Mitarbeiter übergeben

4.6 Automatisierungsgrade und menschliche Aufsicht

Jeder Vorgang trägt einen Automatisierungsgrad von L0 (vollständig manuell) bis L5 (vollautomatisiert). Die vollautomatische Bearbeitung ohne menschliche Interaktion (Dunkelverarbeitung) ist an strenge, je Mandant konfigurierbare Voraussetzungen geknüpft:

- Eindeutige Kundenerkennung: Der Absender muss einem Kunden im Fachsystem eindeutig zuzuordnen sein
- Legitimation: Dunkelverarbeitung erfolgt nur für legitimierte Kunden (übereinstimmende Vertrags- und Identifikationsdaten); erkannte, aber nicht legitimierte Kunden werden stets an einen Menschen geleitet
- Regelbasierter Abschluss: Standardmäßig führen nur regelbasierte KI-Agenten Vorgänge automatisch aus, nicht rein promptbasierte
- Konfidenzlevel: Die Automatisierung greift nur oberhalb eines konfigurierbaren Konfidenz-Schwellwerts (maximal / sehr hoch / hoch / mittel); unklare Fälle gehen an einen Menschen
- Freigabeart: Je Agent konfigurierbar mit Freigabe (Bearbeitung erst nach manueller Prüfung) oder ohne Freigabe (sofortige Automatisierung), optional mit Zeitversatz
- Transparenz: Vollautomatisierte Antworten tragen einen standardisierten KI-Transparenzhinweis als aktivierte Voreinstellung (siehe Abschnitt 6.5); der Absendername des Bots ist konfigurierbar

4.7 Speicherorte und Datenhaltung

- Produktivdaten: MySQL-Datenbank je Mandant auf dedizierten Servern bei Hetzner (Deutschland)
- Dateianhänge und Gesprächsaufzeichnungen: S3-kompatibler Objektspeicher (MinIO) in derselben Infrastruktur
- Vektordatenbank: ausschließlich bereinigte Ticket-Beispiele (ohne direkte Identifikatoren) und Wissensinhalte
- Backups: verschlüsselt, in einem separaten Rechenzentrum in Deutschland oder Finnland (Aixit bzw. Hetzner)
- KI-Verarbeitung: ausschließlich flüchtig zur Laufzeit über REST-APIs der in Abschnitt 5 genannten Anbieter; keine Speicherung beim Modellanbieter

4.8 Löschkonzept

Enneo setzt automatisierte Löschfristen um; der Verantwortliche kann die Aufbewahrung von Vorgängen je Mandant konfigurieren. Vertraglich gilt eine Standardlöschfrist von 4 Jahren ab dem letzten Aktivitätsdatum (AVV Ziffer 1.2).

Datenart	Löschfrist	Anmerkung
Vorgänge (Tickets) inkl. Konversation, Anhängen, Auswertungen	Standard 4 Jahre; je Mandant konfigurierbar (nie / täglich / 90 / 365 / 1095 Tage nach Abschluss)	Täglicher Löschlauf; transaktionale Löschung über alle Tabellen inkl. Objektspeicher
Zugriffsprotokolle und Netzwerkdaten (inkl. IP-Adressen)	30 Tage	Fest vorgegeben (AVV Ziffer 1.2)
Technische Ereignisprotokolle inkl. Details der KI-Aufrufe	30 Tage	Wöchentlicher Bereinigungslauf

Datenart	Löschfrist	Anmerkung
Bereinigte Ticket-Beispiele	90 Tage rollierend	Obergrenze 10.000 Beispiele je Mandant; direkte Identifikatoren entfernt, Restidentifizierbarkeit im Einzelfall nicht vollständig ausgeschlossen (siehe R5)
Inaktive Chat-Sitzungen	30 Tage	Einschließlich zugehöriger Anhänge
Temporäre Dateien und Caches	1 Stunde	Automatische Bereinigung
Backups	30 Tage (monatliche Sicherung 1 Jahr)	Verschlüsselt, separates Rechenzentrum (Deutschland oder Finnland); identisch in SLA Abschnitt 3.1 vereinbart
Löschung auf Anfrage / Betroffenenrecht	Unverzüglich, spätestens innerhalb von 30 Tagen	Einzelvorgangslöschung über API und Oberfläche

5. Einsatz künstlicher Intelligenz

5.1 Multi-Modell-Architektur und LLM-Gateway

Enneo trainiert keine eigenen KI-Grundmodelle, sondern nutzt Sprachmodelle etablierter Anbieter über gesicherte REST-APIs. Für jede Teilaufgabe (z. B. Anliegenerkennung, Zusammenfassung, OCR) ist ein Verwendungszweck definiert, dem ein Primär- und ein Ausweichmodell zugeordnet sind. Die Zuordnung ist zentral konfiguriert und kann je Mandant überschrieben werden. Alle KI-Aufrufe laufen über ein zentrales LLM-Gateway (LiteLLM-Proxy), das Aufrufe protokolliert, Wiederholversuche und automatische Modell-Ausweichrouten steuert sowie Budget- und Zugriffskontrolle je Mandant durchsetzt. Fällt ein Anbieter aus, wird ohne Betriebsunterbrechung auf das Ausweichmodell umgeschaltet.

5.2 Modellinventar nach Verwendungszweck

Die folgende Tabelle zeigt die Standardzuordnung der Modelle je Verwendungszweck (Produktiv-Preset, Stand Juli 2026). Sämtliche Standardmodelle werden in EU-Rechenzentren betrieben:

Verwendungszweck	Primärmodell	Anbieter (Region)	Ausweichmodell
Anliegen-/Tag-Erkennung	GPT-5-4 Nano	Microsoft Azure (Schweden)	Gemini 3.1 Flash Lite (Google, Belgien)
Entfernung personenbezogener Daten (Ticket-Beispiele)	Gemini 3.1 Flash Lite	Google (Belgien)	GPT-5-4 Nano (Azure, Schweden)
Kundenidentifikation	Claude Sonnet 4.5	AWS Bedrock (Frankfurt)	GPT-5-4 Nano (Azure, Schweden)
Zusammenfassung	GPT-5-4 Nano	Microsoft Azure (Schweden)	–
Dokumenten-OCR (Briefe, Zählerfotos)	GPT-5-4, Amazon Nova 2 Lite, Gemini 3.1 Flash Lite	Azure / AWS / Google (EU)	wechselseitig
Chat-Verarbeitung	Claude Sonnet 4.5	AWS Bedrock (Frankfurt)	GPT-5-4 (Azure, Schweden)

Verwendungszweck	Primärmodell	Anbieter (Region)	Ausweichmodell
Intelligente Agenten (Antwortvorschlag)	GPT-5	Microsoft Azure (Schweden)	Claude Sonnet 4.5 (AWS, Frankfurt)
Embeddings (Vektorisierung)	Gemini Embedding 001	Google (Belgien)	–
Schnellklassifizierung (Telefonie)	Gemini 3.1 Flash Lite	Google (Belgien)	Cosmos3 Super Reasoner (Nebius, Finnland)
Standard (übrige Zwecke)	Claude Sonnet 4.5	AWS Bedrock (Frankfurt)	GPT-5-4 (Azure, Schweden)

Die Modellauswahl wird laufend optimiert; Änderungen werden über die wöchentlichen Release Notes kommuniziert (Abonnement auf Anfrage). Modelle der rein europäischen Anbieter Mistral AI (u. a. Mistral Medium, Devstral), Nebius (u. a. Qwen-Modelle, EU-Rechenzentrum Finnland) und Media Trooper (offene Sprachmodelle auf eigener GPU-Infrastruktur, Rechenzentren in Deutschland und den Niederlanden) sind in der Plattform integriert und können je Mandant und Verwendungszweck als Primär- oder Ausweichmodell konfiguriert werden.

5.3 Anbieter und Datenresidenz

Anbieter	Rolle	Region der Verarbeitung	Einsatz
Microsoft Ireland Operations Ltd. (Azure)	OpenAI-Modelle unter EU-Datenschutz	Schweden (EU)	Standard
Google Cloud EMEA Limited (Vertex AI)	Gemini-Modelle	Belgien (EU)	Standard
Amazon Web Services EMEA SARL (Bedrock)	Claude- und Nova-Modelle	Frankfurt (EU)	Standard
Mistral AI SAS	Mistral-Modelle	Frankreich (EU)	Standard / konfigurierbar
Nebius B.V.	Offene Modelle (u. a. Qwen)	Finnland (EU)	Standard / konfigurierbar
Media Trooper GmbH	Offene Sprachmodelle (eigene GPU-Infrastruktur)	Deutschland/ Niederlande (EU)	Standard / konfigurierbar
OpenAI, L.L.C.	GPT-Modelle (Direktzugriff), Realtime-Sprachmodelle	USA	Nur nach vorheriger schriftlicher Freigabe
Cohere Inc.	Sprachmodelle	Kanada/USA	Nur nach vorheriger schriftlicher Freigabe
Groq Inc.	Inferenz-Beschleunigung	USA	Nur nach vorheriger schriftlicher Freigabe
ElevenLabs (Eleven Labs Poland sp. z o.o.)	Sprachsynthese	Polen/USA	Nur nach vorheriger schriftlicher Freigabe
Deepgram, Inc.	Sprachtranskription (Flux)	USA	Nur nach vorheriger schriftlicher Freigabe

Im Standardbetrieb findet die gesamte KI-Verarbeitung ausschließlich in EU-Rechenzentren statt. US-basierte Anbieter mit Verarbeitung außerhalb der EU werden nur eingesetzt, wenn der Auftraggeber dies zuvor schriftlich freigegeben hat (AVV Ziffer 7.1).

5.4 Ausschluss der Trainingsnutzung

Mit allen KI-Anbietern ist vertraglich ausgeschlossen, dass übermittelte Daten gespeichert oder für das Training von Modellen verwendet werden (AVV Ziffer 7.1). Die Verarbeitung erfolgt ausschließlich flüchtig zur Laufzeit. Enneo selbst nutzt Kundendaten ebenfalls nicht zum Training von Grundmodellen. Der Umsetzungsstand je Anbieter (Zero Data Retention bzw. Abuse-Monitoring-Opt-out) wird in folgender Nachweismatrix gepflegt und mindestens halbjährlich aktualisiert:

Anbieter	Vertragsklausel	ZDR- / Abuse-Monitoring-Opt-out-Status	Stand
Microsoft Ireland (Azure OpenAI, Azure Document Intelligence)	AVV Ziffer 7.1	Zero Data Retention vereinbart	August 2026
Google Cloud EMEA (Vertex AI / Gemini)	AVV Ziffer 7.1	Zero Data Retention vereinbart	August 2026
AWS EMEA (Bedrock: Claude, Nova)	AVV Ziffer 7.1	Zero Data Retention vereinbart	August 2026
Mistral AI	AVV Ziffer 7.1	Zero Data Retention vereinbart	August 2026
Nebius B.V.	AVV Ziffer 7.1	Zero Data Retention vereinbart (selbst gehostete Open-Weights-Modelle)	August 2026
Media Trooper GmbH	AVV Ziffer 7.1	Zero Data Retention vereinbart (selbst gehostete Open-Weights-Modelle)	August 2026
OpenAI, L.L.C. (Direktzugriff, nur nach Freigabe)	AVV Ziffer 7.1	Kein Training auf API-Daten (API-Standardvertrag); Zero Data Retention / Modified Abuse Monitoring erfordert gesonderte Gewährung durch OpenAI — Status wird vor jeder Kundenfreigabe verifiziert	August 2026
Cohere, Groq (nur nach Freigabe)	AVV Ziffer 7.1	Zero Data Retention vereinbart	August 2026
ElevenLabs (nur nach Freigabe)	AVV Ziffer 7.1	Zero Data Retention vereinbart	August 2026
Deepgram (Transkription, nur nach Freigabe)	AVV Ziffer 7.1	Zero Data Retention vereinbart	August 2026

Die Einträge werden gegen die jeweils geschlossenen Anbieterverträge verifiziert; ohne verifizierten Zero-Data-Retention-Status wird für den betroffenen Anbieter keine Kundenfreigabe erteilt. Diese Matrix ist Anlage zu dieser DSFA. Die Prozessbox im Datenflussdiagramm heißt entsprechend „Ablage bereinigter Ticket-Beispiele (kein Modelltraining)“ (siehe das unter docs.enneo.ai/de/legal veröffentlichte Datenflussdiagramm).

5.5 Wissensdatenbank (RAG)

Für inhaltliche Auskünfte (z. B. Tarife, Produktinformationen) greift das System auf eine strukturierte Wissensdatenbank zurück, die von autorisierten Nutzern des Auftraggebers redaktionell gepflegt wird (Rolle Wissensmanager). Die Wissensinhalte sind

Unternehmensinformationen des Auftraggebers und enthalten bestimmungsgemäß keine personenbezogenen Daten von Endkunden. Antworten werden per Retrieval-Augmented-Generation aus diesen redaktionellen Inhalten erzeugt, was Halluzinationen reduziert und die inhaltliche Kontrolle beim Auftraggeber belässt.

5.6 Sprachverarbeitung (Telefonie und Voicebot)

Bei angebundener Telefonie verarbeitet der ACD-Dienst Audiodaten der Anrufer. Für Voicebots wird der Audiostrom in Echtzeit an ein Sprachmodell mit Realtime-Schnittstelle übergeben (wahlweise über Microsoft Azure in der EU oder – nur nach schriftlicher Freigabe – OpenAI direkt); für die Transkription kann – ebenfalls nur nach vorheriger schriftlicher Freigabe – Deepgram eingesetzt werden. Dabei entstehen Transkripte, die wie übrige Vorgangsinhalte behandelt werden. Gesprächsaufzeichnungen sind je Mandant und sogar je Gespräch steuerbar; sofern aktiviert, werden Aufnahmen zunächst in einem temporären, nach Gesprächsende bereinigten Verzeichnis erstellt, zu einer Datei zusammengeführt und in den Objektspeicher des Mandanten übertragen, wo sie dem Löschkonzept des jeweiligen Vorgangs unterliegen.

5.7 Nachvollziehbarkeit der KI (Observability)

- Langfuse protokolliert jeden einzelnen LLM-Aufruf mit Eingabe, Antwort, Modell, Tokenverbrauch und Latenz — je Vorgang als vollständiger Entscheidungsbaum abrufbar
- Interne Ereignisprotokolle (Event Traces) dokumentieren jeden Verarbeitungsschritt einschließlich der KI-Aufrufe je Vorgang in der Benutzeroberfläche und per API; sie werden nach 30 Tagen gelöscht
- OpenTelemetry erfasst alle dienstübergreifenden Anfragen als verteilte Traces
- Zusammen ermöglichen diese Ebenen eine lückenlose Nachvollziehbarkeit von der eingehenden Nachricht bis zur ausgehenden Antwort

6. Notwendigkeit und Verhältnismäßigkeit

6.1 Rechtmäßigkeit der Verarbeitung

Die Rechtsgrundlagen der Verarbeitung bestimmt der Verantwortliche. Typischerweise stützt sich die Bearbeitung von Kundenanliegen auf Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung, z. B. Zählerstandsmeldung, Rechnungsfragen) sowie lit. f DSGVO (berechtigtes Interesse an effizientem Kundenservice und Qualitätssicherung). Enneo verarbeitet ausschließlich im Auftrag und nach dokumentierter Weisung (Art. 28 DSGVO).

6.2 Zweckbindung und Datenminimierung

- Es werden nur die Daten verarbeitet, die der Auftraggeber überträgt oder deren Quelle er anbindet
- KI-Modelle erhalten je Aufruf nur die für die konkrete Teilaufgabe erforderlichen Vorgangsinhalte
- Aus Lernbeispielen werden vor der Speicherung die direkten Identifikatoren entfernt; die Vektordatenbank enthält keine direkten Identifikatoren
- Netzwerk- und Zugriffsprotokolle unterliegen strenger Zweckbindung (Datenschutzkontrolle) und werden nicht zur anlasslosen Verhaltens- oder Leistungskontrolle von Mitarbeitern ausgewertet
- Aggregierte Statistiken enthalten keine Einzelpersonenbezüge

6.3 Speicherbegrenzung

Alle Datenarten unterliegen dem in Abschnitt 4.8 dokumentierten Löschkonzept mit automatisierten Fristen. Der Verantwortliche steuert die Aufbewahrungsdauer der Vorgänge selbst; kurze Fristen (Löschung am Abschlusstag) sind ebenso konfigurierbar wie längere gesetzliche Aufbewahrungszeiträume. Protokoll- und Netzwerkdaten werden unabhängig davon stets nach 30 Tagen gelöscht.

6.4 Richtigkeit und Ergebnisqualität

Extrahierte Daten werden vor jeder automatisierten Aktion gegen das Fachsystem des Auftraggebers validiert. Antworten aus der Wissensdatenbank basieren auf redaktionell verantworteten Inhalten. Das KI-Kontrollzentrum macht Kennzahlen wie Klassifizierungsgenauigkeit, Kundenidentifikationsquote und Antwortqualität laufend sichtbar; hinterlegte Testfälle je Agent werden regelmäßig automatisch ausgeführt und Abweichungen angezeigt.

6.5 Transparenz gegenüber betroffenen Personen

- Chat und Telefonie: ein Begrüßungstext weist als aktivierte Voreinstellung darauf hin, dass mit einem KI-System kommuniziert wird; Sprachausgaben synthetischer Stimmen (z. B. Realtime-Voicebot, TTS-Ansagen) werden zusätzlich maschinenlesbar als KI-generiert gekennzeichnet (Art. 50 Abs. 2 AI Act)
- Teilautomatisierte E-Mail (L2/L3): der Mitarbeiter prüft und verantwortet die Antwort; ein KI-Hinweis kann zusätzlich in die Vorlage integriert werden
- Vollautomatisierte E-Mail (L4/L5): die Plattform liefert einen standardisierten Transparenzhinweis als aktivierte Voreinstellung aus; der Auftraggeber kann den Absendernamen des Bots konfigurieren
- Eine Deaktivierung der vorgenannten Transparenzhinweise ist nur durch ausdrückliche Konfigurationsentscheidung des Auftraggebers möglich; in diesem Fall übernimmt der Auftraggeber insoweit die Verantwortung für die Erfüllung der Transparenzpflichten nach Art. 50 AI Act (Leistungsbeschreibung, Abschnitt „KI-Einsatz“)
- Die Informationspflichten nach Art. 13/14 DSGVO erfüllt der Verantwortliche; Enneo stellt die dafür nötigen Informationen (dieses Dokument, AVV, TOM, Datenflussdiagramm) bereit

6.6 Geprüfte Alternativen

- Eigenes Modelltraining mit Kundendaten wurde verworfen: höhere Datenschutzrisiken (dauerhafte Einbettung personenbezogener Daten in Modellgewichte) bei geringerer Qualität gegenüber aktuellen Grundmodellen
- Ausschließlich US-basierte Modellnutzung wurde verworfen: Drittlandrisiken; stattdessen EU-Rechenzentren als Standard und rein europäische Anbieter als zusätzliche Absicherung
- Vollständiger Verzicht auf KI wurde als Standardbetrieb verworfen (Kernnutzen der Plattform), bleibt aber als konfigurierbarer Notbetrieb erhalten (siehe Risiko R7)
- Speicherung von Klardaten-Beispielen für das Anlernen wurde verworfen; stattdessen fünfstufige Entfernung personenbezogener Angaben vor jeder Speicherung

7. Betroffenenrechte

Enneo unterstützt den Verantwortlichen bei der Erfüllung der Betroffenenrechte nach Kapitel III DSGVO. Wendet sich eine betroffene Person direkt an Enneo, wird sie an den Verantwortlichen verwiesen und der Antrag unverzüglich weitergeleitet (AVV Ziffer 6.4):

Recht	Umsetzung in der Plattform	Frist
Auskunft (Art. 15)	Vollständiger Export der zu einer Person gespeicherten Vorgänge über Oberfläche und API	Unverzüglich, spätestens 1 Monat
Berichtigung (Art. 16)	Korrektur über Oberfläche/API; Stammdaten werden im führenden System des Auftraggebers berichtigt und synchronisiert	Unverzüglich
Löschung (Art. 17)	Transaktionale Einzelvorgangslöschung inkl. aller Anhänge, Auswertungen und Protokolle; revisionssicherer Löschnachweis ohne Personenbezug. Backups werden nicht selektiv verändert; gelöschte Daten werden bei einer Wiederherstellung erneut gelöscht, spätestens mit Ablauf der Backup-Aufbewahrung (AVV Ziffer 4.3)	Unverzüglich, spätestens 30 Tage
Einschränkung (Art. 18)	Sperrung einzelner Vorgänge für die weitere Verarbeitung	Unverzüglich
Datenübertragbarkeit (Art. 20)	Export in strukturierten, maschinenlesbaren Formaten über API	Unverzüglich, spätestens 1 Monat
Widerspruch (Art. 21)	Umsetzung durch den Verantwortlichen; Enneo setzt Weisungen (z. B. Ausschluss von der KI-Verarbeitung) technisch um	Unverzüglich

Automatisierte Einzelentscheidungen im Sinne des Art. 22 DSGVO mit rechtlicher Wirkung trifft die Plattform nicht; die Dunkelverarbeitung beschränkt sich auf die Erledigung des vom Kunden selbst angestoßenen Anliegens, ist an die in Abschnitt 4.6 beschriebenen Schwellen gebunden und kann vom Verantwortlichen jederzeit deaktiviert oder auf Freigabe durch Mitarbeiter umgestellt werden.

8. Risikobewertung und Abhilfemaßnahmen

8.1 Vorgehen

Nachfolgend werden die identifizierten Risiken für die Rechte und Freiheiten betroffener Personen einzeln beschrieben und bewertet. Je Risiko werden Schwere und Eintrittswahrscheinlichkeit vor dem Hintergrund der getroffenen Maßnahmen eingeschätzt und das Restrisiko bewertet. Eine Gesamtübersicht enthält die Risikomatrix am Ende dieses Abschnitts.

8.2 R1 – Unbefugte Offenlegung durch externe Angriffe

Ein erfolgreicher Angriff auf die Plattform könnte zur Offenlegung von Kunden- und Vertragsdaten führen. Schwere: hoch. Maßnahmen: Zero-Trust-Architektur, TLS 1.3 für alle externen Verbindungen, Verschlüsselung gespeicherter Daten nach BSI-Empfehlungen, Netzwerksegmentierung mit getrennten Firewall-Zonen (Dev, Prod, Admin) und DMZ, dauerhaft aktiver DDoS-Schutz, regelmäßige externe Penetrationstests, Schwachstellen-Scans auf Quellcode- und Container-Ebene in der CI/CD-Pipeline, 24/7-Monitoring mit automatisierter Vorfallreaktion. Eintrittswahrscheinlichkeit: niedrig. Restrisiko: akzeptabel.

8.3 R2 – Missbrauch interner Zugriffsrechte

Mitarbeiter von Enneo oder des Auftraggebers könnten Zugriffsrechte zweckwidrig nutzen. Schwere: hoch. Maßnahmen: rollenbasiertes Berechtigungskonzept mit dokumentierter Vergabe und revisionssicherer Änderungshistorie, ausschließlich persönliche Named Accounts, verpflichtende Zwei-Faktor-Authentifizierung für jeden Zugriff auf personenbezogene Daten,

Freigabe zusätzlicher Berechtigungen nur durch die Geschäftsführung, Sperrung von Zugängen ausscheidender Mitarbeiter spätestens nach fünf Werktagen, Protokollierung aller Zugriffe mit strenger Zweckbindung, Verpflichtung aller Mitarbeiter auf das Datengeheimnis und regelmäßige Datenschutzschulungen. Eintrittswahrscheinlichkeit: sehr niedrig. Restrisiko: akzeptabel.

8.4 R3 – Fehlerhafte automatisierte Antworten (KI-Halluzination)

Ein Sprachmodell könnte inhaltlich falsche Antworten erzeugen oder Daten falsch extrahieren, was zu fehlerhaften Auskünften oder Buchungen führen könnte. Schwere: mittel. Maßnahmen: Validierung aller extrahierten Daten gegen das Fachsystem vor jeder Aktion, Dunkelverarbeitung nur durch regelbasierte Agenten oberhalb konfigurierbarer Konfidenzschwellen, unklare Fälle gehen stets an einen Menschen, inhaltliche Antworten ausschließlich aus der redaktionell gepflegten Wissensdatenbank (RAG), automatisch ausgeführte Testfälle je Agent, Qualitätskennzahlen im KI-Kontrollzentrum, vollständige Nachvollziehbarkeit jedes KI-Aufrufs. Eintrittswahrscheinlichkeit: niedrig. Restrisiko: akzeptabel.

8.5 R4 – Diskriminierung durch KI (Bias)

Modelle könnten Anliegen bestimmter Personengruppen systematisch schlechter behandeln. Schwere: mittel. Maßnahmen: keine Verarbeitung von Merkmalen nach Art. 9 DSGVO als Entscheidungskriterium, Klassifizierung ausschließlich anhand des Anliegen-Inhalts (Transkript-only), objektive regelbasierte Ausführungslogik, quartalsweise Bias-Überprüfung, menschliche Kontrolle unterhalb der Konfidenzschwellen, Beschwerdeweg über den Kundenservice des Auftraggebers. Eintrittswahrscheinlichkeit: niedrig. Restrisiko: akzeptabel.

8.6 R5 – Re-Identifikation bereinigter Ticket-Beispiele

Unvollständig bereinigte Beispiele könnten Rückschlüsse auf Personen erlauben; eine erfolgreiche Re-Identifizierung würde der Nutzung dieser Beispiele für RAG-Lernen die Rechtsgrundlage entziehen. Schwere: mittel. Maßnahmen: zweistufige Bereinigung (deterministische Vorverarbeitung ersetzt alle Ziffern und E-Mail-Adressen, anschließend KI-gestützte Ersetzung aller erkannten personenbezogenen Angaben durch Platzhalter), Entfernung von Signaturen und zitierten Verläufen, manuelle Stichprobenkontrollen über eine eigene Oberfläche, rollierende 90-Tage-Aufbewahrung mit Obergrenze, strikte Mandantentrennung der Beispiele. Eintrittswahrscheinlichkeit: niedrig. Restrisiko: akzeptabel.

8.7 R6 – Zugriff durch Drittlandbehörden

Behörden aus Drittländern (insb. USA, CLOUD Act) könnten Herausgabeverlangen an Anbieter mit US-Konzernbezug richten. Schwere: hoch. Maßnahmen: Hosting und Datenspeicherung ausschließlich bei europäischen Anbietern (Betrieb: Hetzner, Deutschland; Backup: Aixit bzw. Hetzner, Deutschland und Finnland); KI-Verarbeitung im Standard ausschließlich in EU-Rechenzentren über europäische Vertragsgesellschaften (Microsoft Ireland, Google Cloud EMEA, AWS EMEA) ohne Speicherung beim Anbieter (flüchtige Laufzeitverarbeitung); rein europäische Anbieter (Mistral, Nebius) als konfigurierbare Alternative ohne US-Konzernbezug; Drittlandübermittlungen nur unter den Voraussetzungen der Art. 44 ff. DSGVO nach vorheriger schriftlicher Freigabe des Auftraggebers. Eintrittswahrscheinlichkeit: sehr niedrig. Restrisiko: akzeptabel.

8.8 R7 – Geopolitische Zugriffsbeschränkung auf US-Anbieter

Enneo nutzt für die LLM-Verarbeitung unter anderem EU-Rechenzentren der US-Anbieter Microsoft (Azure), Google (Google Cloud) und Amazon (AWS Bedrock). Es besteht das Risiko, dass die USA den Zugang zu Diensten US-basierter Anbieter einschränken (z. B. durch Exportkontrollen oder Sanktionen) und diese Dienste dadurch kurzfristig nicht mehr für die LLM-Verarbeitung zur Verfügung stehen. Schwere: hoch (Ausfall der KI-Funktionen), wobei keine Vertraulichkeitsverletzung droht, sondern eine Verfügbarkeitseinschränkung. Maßnahmen: Zur Minderung hat Enneo mit Mistral AI SAS (Paris, Frankreich), Nebius B.V. (Schiphol, Niederlande;

Rechenzentrum in Finnland) und Media Trooper GmbH (Idstein, Deutschland; Rechenzentren in Deutschland und den Niederlanden) drei rein europäische KI-Anbieter als Unterauftragsverarbeiter in den AVV aufgenommen (Mistral und Nebius im Februar 2026, Media Trooper im August 2026). Die Multi-Modell-Architektur erlaubt es, jeden Verwendungszweck ohne Betriebsunterbrechung auf diese Anbieter umzustellen; Nebius-Modelle sind bereits im Standard-Preset als Ausweichmodelle hinterlegt. Für den Extremfall, dass vorübergehend weder US-basierte noch europäische KI-Anbieter verfügbar sind, besteht eine weitere Rückfallebene: Enneo kann so konfiguriert werden, dass es vollständig ohne KI-Funktionen als reines Vorgangsbearbeitungs- und Telefoniesystem betrieben wird; die Kernfunktionen (Ticketbearbeitung, Kundenkommunikation, Telefonie) bleiben dabei uneingeschränkt nutzbar. Eintrittswahrscheinlichkeit: niedrig. Restrisiko: akzeptabel.

8.9 R8 – Ausfall der Plattform oder Datenverlust

Hardwaredefekte, Rechenzentrumsausfälle oder fehlerhafte Änderungen könnten zu Nichtverfügbarkeit oder Datenverlust führen. Schwere: mittel. Maßnahmen: tägliche verschlüsselte Backups mit Lagerung in einem separaten Rechenzentrum, 30 Tage Aufbewahrung (monatliche Sicherung ein Jahr), tägliche automatisierte Backup-Validierung, Wiederherstellungsziele (RTO/RPO) je Service Level gemäß SLA Abschnitt 3.1, Festplattenspiegelung, unterbrechungsfreie Stromversorgung mit Netzersatzanlage im Rechenzentrum, vollständige Infrastructure-as-Code-Spezifikation für schnellen Wiederanlauf, 24/7-Monitoring, wöchentlicher Release-Zyklus mit Staging-Umgebungen. Eintrittswahrscheinlichkeit: niedrig. Restrisiko: akzeptabel.

8.10 R9 – Mandantenübergreifende Datenvermischung

Daten eines Mandanten könnten für einen anderen sichtbar werden. Schwere: hoch. Maßnahmen: dedizierte Instanz je Mandant mit eigener Datenbank und eindeutiger Mandantenkennung in jedem Dienst, getrennte Zugangsdaten und KI-Gateway-Schlüssel je Mandant, getrennte Protokollierungs-Mandanten in der LLM-Observability, mandantengetrennte Lernbeispiele und Wissensdatenbank, Trennungskontrolle gemäß TOM Ziffer 8. Eintrittswahrscheinlichkeit: sehr niedrig. Restrisiko: akzeptabel.

8.11 R10 – Manipulation der KI durch präparierte Eingaben (Prompt Injection)

Kunden könnten versuchen, durch präparierte Nachrichten die KI zu unbeabsichtigten Aktionen oder zur Preisgabe fremder Daten zu bewegen. Schwere: mittel. Maßnahmen: KI-Agenten können ausschließlich vordefinierte, je Agent freigegebene Aktionen mit validierten Parametern ausführen; jede Aktion wird gegen das Fachsystem und die Legitimation des Absenders geprüft; Dunkelverarbeitung nur für eindeutig legitimierte Kunden; Auskünfte nur zu dem Vertrag, dem der Absender zugeordnet ist; kundenspezifische Integrationslogik läuft in einer abgeschotteten Sandbox; vollständige Protokollierung aller KI-Aufrufe ermöglicht die Erkennung von Missbrauchsmustern. Eintrittswahrscheinlichkeit: niedrig. Restrisiko: akzeptabel.

8.12 R11 – Sprachaufzeichnungen in der Telefonie

Gesprächsaufzeichnungen sind besonders sensibel, da Stimme und Gesprächsinhalt zusammen anfallen. Schwere: mittel. Maßnahmen: Aufzeichnung nur bei entsprechender Konfiguration durch den Verantwortlichen (der die Einwilligungs- bzw. Hinweispflichten steuert), Steuerbarkeit bis auf Einzelgesprächsebene, temporäre Verarbeitungsdateien werden nach Gesprächsende automatisch bereinigt, dauerhafte Ablage nur im mandantenspezifischen Objektspeicher unter dem Löschkonzept des Vorgangs, Echtzeit-Sprachmodelle im Standard über EU-Rechenzentren. Eintrittswahrscheinlichkeit: niedrig. Restrisiko: akzeptabel.

8.13 R12 – Verstöße bei Unterauftragsverarbeitern

Ein Subunternehmer könnte vertragliche oder gesetzliche Pflichten verletzen. Schwere: hoch. Maßnahmen: sorgfältige dokumentierte Auswahl vor Beauftragung, Auftragsverarbeitungsverträge

mit allen Subunternehmern mit Weitergabe sämtlicher Pflichten (Art. 28 Abs. 4 DSGVO), Vorabinformation (30 Tage) und Widerspruchsrecht aus wichtigem Grund bei Änderungen (AVV Ziffer 7.2), Audit- und Kontrollrechte gemäß AVV, regelmäßige Überprüfung anhand von Zertifikaten und Testaten, unverzügliche Meldung von Sicherheitsvorfällen entlang der Kette. Eintrittswahrscheinlichkeit: sehr niedrig. Restrisiko: akzeptabel.

8.14 Risikomatrix (Übersicht)

Risiko	Schwere	Wahrscheinlichkeit	Wesentliche Maßnahmen	Restrisiko
R1 Unbefugte Offenlegung (extern)	Hoch	Niedrig	Verschlüsselung, Zero Trust, Pen-Tests, Monitoring	Akzeptabel
R2 Missbrauch interner Rechte	Hoch	Sehr niedrig	RBAC, 2FA, Named Accounts, Protokollierung	Akzeptabel
R3 Fehlerhafte KI-Antworten	Mittel	Niedrig	Validierung, Konfidenzschwellen, menschliche Prüfung, RAG	Akzeptabel
R4 KI-Bias	Mittel	Niedrig	Transkript-only, Bias-Reviews, menschliche Kontrolle	Akzeptabel
R5 Re-Identifikation von Beispielen	Mittel	Niedrig	Zweistufige Bereinigung, Stichproben, 90-Tage-Rotation	Akzeptabel
R6 Zugriff durch Drittlandbehörden	Hoch	Sehr niedrig	EU-Hosting, EU-Rechenzentren, EU-Anbieter, Art. 44 ff.	Akzeptabel
R7 Geopolitische Beschränkung US-Anbieter	Hoch	Niedrig	EU-LLM-Anbieter (Mistral, Nebius, Media Trooper), Modell-Routing, Notbetrieb ohne KI	Akzeptabel
R8 Ausfall / Datenverlust	Mittel	Niedrig	Backups, IaC, Monitoring, RTO/RPO gemäß SLA	Akzeptabel
R9 Mandantenvermischung	Hoch	Sehr niedrig	Dedizierte Instanz und DB je Mandant	Akzeptabel
R10 Prompt Injection	Mittel	Niedrig	Vordefinierte Aktionen, Legitimationsprüfung, Sandbox	Akzeptabel
R11 Sprachaufzeichnungen	Mittel	Niedrig	Konfigurierbare Aufzeichnung, Löschkonzept, EU-Verarbeitung	Akzeptabel
R12 Subunternehmer-Verstoß	Hoch	Sehr niedrig	Sub-AVVs, Auditrechte, Zertifikate	Akzeptabel

9. Technische und organisatorische Maßnahmen

Die vollständigen Maßnahmen sind im separaten TOM-Dokument nach den acht Kontrollbereichen dokumentiert; nachfolgend die für diese DSFA wesentlichen Inhalte:

9.1 Zutrittskontrolle

Enneo ist ein vollständig virtuelles Unternehmen ohne eigene Büroräume. Die physische Sicherheit der Server gewährleistet der Rechenzentrumsbetreiber Hetzner: elektronisches Zutrittskontrollsystem mit Protokollierung, Hochsicherheitszaun, 24/7-Besetzung, Videoüberwachung, Zutritt nur in Begleitung von Rechenzentrumspersonal.

9.2 Zugangskontrolle

Zero-Trust-Sicherheitsarchitektur: jede Anfrage wird geprüft, als käme sie aus einem offenen Netzwerk. Zugang zu personenbezogenen Daten erfordert zwei Faktoren (z. B. Login/Passwort plus Einmalpasswort oder Zertifikat plus Passphrase). Passwort-Mindestanforderungen nach Stand der Technik, zentrale Zugangsdokumentation, externe Zugänge nur über gesicherte Verbindungen, mehrstufige Architektur mit DMZ, physische Schnittstellen (USB, Datenträger) grundsätzlich untersagt.

9.3 Zugriffskontrolle

Dokumentiertes Berechtigungskonzept mit revisionssicherer Änderungshistorie; jederzeit ist bekannt, welcher Mitarbeiter auf welche geschützten Daten zugreifen kann. Datenklassifikation C0–C4 mit abgestuften Freigaben; Verschlüsselung gespeicherter Daten auf Dateisystem- oder Datenbankebene gemäß BSI-Empfehlungen (Encryption at Rest); Sperrung der Zugänge ausscheidender Mitarbeiter spätestens nach fünf Werktagen; Grundsatz des aufgeräumten Schreibtischs und gesperrten Bildschirms.

9.4 Weitergabekontrolle

Alle Mitarbeiter sind auf das Datengeheimnis verpflichtet und werden regelmäßig geschult. Datenübermittlungen erfolgen ausschließlich verschlüsselt (TLS 1.3) und werden revisionssicher protokolliert (Verfahren, Empfänger, Daten, Zeitpunkt). Physische Datenträger sind nicht im Einsatz. Bei Weitergaben wird von Anonymisierung und Pseudonymisierung Gebrauch gemacht.

9.5 Eingabekontrolle

Ein Protokollierungskonzept regelt Art, Inhalt und Umfang der Protokollierung. Protokolle zeigen auf Benutzerebene, welche Anwendungen ein Benutzer in einem Zeitraum genutzt hat; sie sind gegen unbefugte Einsicht und Manipulation geschützt, unterliegen festen Löschfristen (30 Tage) und strenger Zweckbindung. Eine anlasslose Verhaltens- oder Leistungskontrolle findet nicht statt.

9.6 Auftragskontrolle

Alle Unterauftragsverarbeiter sind vertraglich nach Art. 28 Abs. 3 DSGVO gebunden; Auswahl und Begründung sind dokumentiert. Weisungen erfolgen schriftlich durch benannte weisungsberechtigte Personen. Ein unternehmensweites Datenschutz- und Risikomanagementsystem ist etabliert; datenschutzfreundliche Voreinstellungen werden bei der Softwareentwicklung berücksichtigt (Art. 25 DSGVO).

9.7 Verfügbarkeitskontrolle

Monitoring aller relevanten Server, dauerhaft aktiver DDoS-Schutz, unterbrechungsfreie Stromversorgung mit Netzersatzanlage, Festplattenspiegelung, mindestens tägliche verschlüsselte Backups mit regelmäßigem Restore-Test, Wiederanlauf nach Katastrophenfall in kurzer Zeit dank Infrastructure-as-Code.

9.8 Trennungskontrolle

Ausreichende Mandantentrennung: Daten verschiedener Auftraggeber sind wechselseitig weder einsehbar noch veränderbar (dedizierte Instanz und Datenbank je Mandant). Office-, Entwicklungs-/Test- und Produktivsysteme laufen in logisch getrennten Netzsegmenten; zu Test-

und Entwicklungszwecken kommen ausschließlich Testdaten zum Einsatz, auf Echtdaten basierende Testdaten werden anonymisiert.

10. Subunternehmer und Drittlandbezug

Die vollständige, vertraglich verbindliche Liste der Unterauftragsverarbeiter — einschließlich Anschriften, Verarbeitungszwecken und Einsatzbedingungen (Standardbetrieb, nur nach vorheriger schriftlicher Freigabe, nur wenn beauftragt) — enthält Ziffer 7.1 des AVV (docs.enneo.ai/de/legal/avv). Sie wird ausschließlich dort gepflegt und in diesem Dokument nicht dupliziert; für die KI-Anbieter dokumentiert Abschnitt 5.3 ergänzend die Datenresidenz.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in Mitgliedstaaten der EU bzw. des EWR statt oder unter den besonderen Voraussetzungen der Art. 44 ff. DSGVO (AVV Ziffer 8). Jede Abweichung bedarf der vorherigen schriftlichen Freigabe des Auftraggebers. Die Speicherung übermittelter Daten oder deren Überlassung für Trainingszwecke ist mit allen KI-Anbietern explizit ausgeschlossen. Neue oder geänderte Subunternehmer werden dem Auftraggeber mindestens 30 Tage vorab in Textform mitgeteilt; dem Auftraggeber steht ein Widerspruchsrecht aus wichtigem Grund zu (AVV Ziffer 7.2).

11. Überwachung, Audits und kontinuierliche Verbesserung

- Monatliche Überprüfung der Sicherheitsverfahren
- Quartalsweise Überprüfung des KI-Bias
- Jährliche sowie anlassbezogene Überprüfung dieser DSFA
- Monitoring: 24/7, automatisierte Vorfallreaktion; Meldung von Datenschutzverletzungen an den Auftraggeber unverzüglich, zur Wahrung der 72-Stunden-Frist des Art. 33 DSGVO
- Lückenlose Nachvollziehbarkeit: Protokollierung aller KI-Aufrufe (LLM-Observability) und aller Verarbeitungsschritte (Ereignisprotokolle, verteilte Traces)
- Audits: regelmäßige interne und externe Prüfungen; Penetrationstests durch externe Anbieter; eine SOC 2- oder ISO-27001-Zertifizierung durch eine unabhängige Instanz wird evaluiert, ist derzeit aber nicht abgeschlossen (aktueller Nachweis erfolgt über Selbstaudit gemäß AVV Ziffer 9.3)
- Backup: tägliche verschlüsselte Backups, 30 Tage Aufbewahrung, tägliche Backup-Validierung
- Vulnerability Management: Scans auf Quellcode- und Container-Ebene in der CI/CD-Pipeline
- Wöchentlicher Release-Zyklus mit dokumentierten Release Notes; KI-Modell-Updates ohne Betriebsunterbrechung

Änderungen an Architektur, Subunternehmern oder Verarbeitungszwecken durchlaufen das dokumentierte Change-Management einschließlich Risiko- und Datenschutzbewertung unter Einbeziehung des Datenschutzverantwortlichen, bevor sie produktiv gehen.

12. Konsultation und Fortschreibung

Der Datenschutzverantwortliche von Enneo war in die Erstellung dieser DSFA eingebunden und wird bei der Planung neuer sowie der Änderung bestehender Verfahren rechtzeitig beteiligt. Da nach Umsetzung der beschriebenen Maßnahmen kein hohes Restrisiko verbleibt, ist eine vorherige Konsultation der Aufsichtsbehörde nach Art. 36 DSGVO nicht erforderlich. Auftraggeber erhalten dieses Dokument als Grundlage für ihre eigenen datenschutzrechtlichen Prüfungen und etwaige eigene Folgenabschätzungen; ihre Rückmeldungen fließen in die Fortschreibung ein. Die nächste turnusmäßige Überprüfung ist für Juli 2027 vorgesehen.

13. Fazit

Enneo GmbH erfüllt die Anforderungen der DSGVO und des EU KI Acts durch eine datenschutzfreundliche Architektur, strenge Zugriffskontrollen und transparente Prozesse. Die Standardverarbeitung erfolgt ausschließlich in EU-Rechenzentren; durch die Aufnahme rein europäischer KI-Anbieter (Mistral AI, Nebius, Media Trooper) und den konfigurierbaren Notbetrieb ohne KI bleibt die Plattform auch bei geopolitischen Zugriffsbeschränkungen auf US-Anbieter funktionsfähig. Lernvorgänge finden ausschließlich auf bereinigten Beispielen ohne direkte Identifikatoren statt, automatisierte Bearbeitung ist an Legitimation, Konfidenzschwellen und konfigurierbare menschliche Freigaben gebunden, und sämtliche Datenarten unterliegen automatisierten Löschfristen. Die Risikobewertung zeigt, dass alle identifizierten Risiken durch die getroffenen technischen und organisatorischen Maßnahmen auf ein akzeptables Maß reduziert sind; ein hohes Restrisiko im Sinne des Art. 35 DSGVO verbleibt nicht.

14. Versionshistorie

Version	Datum	Änderungen
1.0	November 2025	Erstfassung
2.0	Juli 2026	Neues Risiko: geopolitische Zugriffsbeschränkung auf US-Anbieter; rein europäische KI-Anbieter (Mistral AI, Nebius) als Mitigation; Notbetrieb ohne KI
2.1	Juli 2026	Vollständig überarbeitete und erweiterte Fassung: Beschreibung der Verarbeitung, Modellinventar, Löschkonzept, Notwendigkeit und Verhältnismäßigkeit, erweiterter Risikokatalog (R1–R12), TOM-Zusammenfassung
2.2	August 2026	Überarbeitung nach externem Review: Ticket-Beispiel-Verfahren neutral beschrieben (bereinigte Ticket-Beispiele, Restrisiken in R5), präzisierte AI-Act-Einordnung, ZDR-Nachweismatrix, Deepgram ergänzt, Backup-Standorte vereinheitlicht, AVV-Verweise auf Aug-2026-Nummerierung, explizite Abschnittsnummerierung; Media Trooper als dritter rein europäischer KI-Anbieter ergänzt; Subunternehmer-Übersicht in §10 durch Verweis auf AVV Ziffer 7.1 ersetzt; Erforderlichkeits-Framing neutralisiert — die Schwellwertprüfung nach Art. 35 DSGVO obliegt dem Verantwortlichen, dieses Dokument nimmt sie nicht vorweg (§1, §2.1, §12)