Zive - AI Transparency Sheet

Stand: August 2025

Dieses Dokument stellt zentrale Informationen zur Nutzung von General Purpose AI (GPAI) innerhalb der Zive-Plattform bereit und dient zur Unterstützung bei der Einhaltung von Transparenzanforderungen im Kontext des EU AI Act.

Verwendete KI-Modelle

Übersicht über die aktuell verfügbaren LLMs in der Zive Plattform.

Provider	Hosting-Region
OpenAI	EU via Zive (Azure)
Mistral	EU via Mistral
Anthropic	EU via Zive (Amazon AWS)
Google	Global via Zive (Google Cloud)

Hinweis: Modellverfügbarkeit kann je nach Kundeneinstellung und Systemintegration variieren.

Trainingsnutzung

Zive verwendet ausschließlich Modelle über APIs mit **deaktivierter Trainingsnutzung**.

Keine Kundendaten werden an die Modellanbieter zurückgeführt oder für die Weiterentwicklung der LLMs verwendet.

Trainingsverzicht durch:

- Nutzung von KI-Modellen mit immer aktivierten “data logging off” Option
- Auswahl von API-Partnern mit No-Training-Zusage
- Kein direkter Modellzugriff durch Endnutzer

Hosting & Infrastruktur

Komponente	Infrastruktur	Standort
Zive-Plattform	Microsoft Azure	EU
Knowledge Graph	Microsoft Azure	EU

LLM API-Zugriffe	Je nach Anbieter	EU/Global für Google-Modelle
Backup & Logging	Microsoft Azure	EU

Zive ist ISO 27001 zertifiziert. Daten werden ausschließlich in der EU verarbeitet für alle Kernfunktionen der Plattform. Kunden können optional weitere Dienste aktivieren, die zu einer Verarbeitung außerhalb der EU führen können.

Schutzmaßnahmen (LLM-bezogene Risiken)

Risiko	**Zive-Schutzmechanismus**
Prompt Injection / Jailbreak	Prompt Sanitization, Output-Filter
Halluzination / Unverlässliche Antwort	Quellenverweise, Verified Content Flag
Unautorisierter Zugriff	SSO, rollenbasiertes Zugriffskonzept
Datenweitergabe an falsche Nutzer	Rechtevererbung aus Quellsystem, Mandantentrennung
Unklare Nutzeraktionen	Session Logs, Audit Trails
Modellwahl durch User ohne Kontrolle	Modellzugriff steuerbar durch Admins

Rollen & Zugriffsmodell

Rolle	**Berechtigungen**
Admin	Plattformkonfiguration, Nutzer- & Modellverwaltung, Analytics
Moderator	Content-Kuration, Agent-Management, Feedback-Auswertung
User	Abfrage, Suche, keine Verwaltung

- SSO via Entra ID oder SAML
- De-/Provisionierung automatisiert

Weitere Transparenz-Features

- Sichtbare Modell-Auswahl im Chat-Interface
- Konfigurierbare API-Nutzung (z. B. Claude aktiv/inaktiv)

Kontaktstelle für Datenschutz & Compliance

Datenschutzbeauftragter:

Kertos GmbH
Briennerstraße 41
80333 München
dsb@kertos.io

Produkt- & Compliance-Fragen:

privacy@zive.com