Zive – AI Transparency Sheet

Version: August 2025

This document provides key information on the use of General Purpose AI (GPAI) within the Zive platform and is intended to support compliance with transparency requirements in the context of the EU AI Act.

AI models used

Overview of currently available LLMs in the Zive platform.

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

Note: Model availability may vary depending on customer preferences and system integration.

Training use

Zive only uses models via APIs with **training usage disabled**.

No customer data is passed back to the model providers or used for the further development of the LLMs.

No training is ensured due to:

- Using AI models with “data logging off” option always enabled
- Selection of API partners with no-training commitment
- No direct model access by end users

Hosting & Infrastructure

Components	Infrastructure	Location
Zive platform	Microsoft Azure	EU
Knowledge Graph	Microsoft Azure	EU

LLM API access	Depending on the provider	EU/Global for Google models
Backup & Logging	Microsoft Azure	EU

Zive is ISO 27001 certified. Data is processed exclusively in the EU for all core services. Customers may optionally activate functionality that may require data processing outside the EU.

Protective measures (LLM-related risks)

Risk	**Zive protection mechanism**
Prompt Injection / Jailbreak	Prompt Sanitization, Output-Filter
Hallucination / Unreliable answer	Source references, Verified Content Flag
Unauthorized access	SSO, role-based access concept
Data transfer to incorrect users	Rights inheritance from source system, client separation
Unclear user actions	Session Logs, Audit Trails
Model selection by users without control	Model access controllable by admins

Roles & access model

Role	**Permissions**
Admin	Platform configuration, user & model management, analytics
Moderator	Content curation, agent management, feedback evaluation
User	Query, search, no administration

- SSO via Login ID or SAML
- De-/provisioning automated

Additional transparency features

- Visible model selection in the chat interface
- Configurable API usage (e.g. Claude active/inactive)

Contact point for Data Protection & Compliance

Data Protection Officer:

Kertos GmbH
Briennerstraße 41
80333 Munich
Germany
dsb@kertos.io

Product & Compliance Questions:

privacy@zive.com