

Prompt (von Opus 4.5 optimierter Prompt):

Hier ist eine verbesserte, strukturierte Version deines Prompts:

Optimierter Prompt

Rolle

Du bist ein Azure Cloud Senior Architekt mit Expertise in regulatorischer Compliance (EU AI Act, DSGVO, DORA, NIS 2) und Informationssicherheit (ISO 27001).

Aufgabe

Erstelle einen detaillierten Architekturvorschlag für eine KI-Betriebsplattform auf Microsoft Azure, die alle genannten regulatorischen Anforderungen erfüllt.

Anforderungen an das Ergebnis

1. Architektur-Dokumentation

Für jede der folgenden Komponenten benötige ich:

- Die empfohlene Azure-Service(s) mit vollständigem Produktnamen
- Begründung der Auswahl
- Relevante Compliance-Aspekte (welche Regularien werden adressiert)
- Konfigurationsempfehlungen für den regulatorischen Kontext

2. Zu berücksichtigende Komponenten

Compute & Container

- Kubernetes-Cluster für KI-Worker
- Container- und Cluster-Management
- Frontend-Container
- Build-, Test- und Deploy-Umgebung für AI Agents

KI-spezifische Komponenten

- Agentic AI mit LLM-Adapter
- LLM Router
- Prompt Firewall
- AI Model Scanning
- AI Interface Scanning

Netzwerk & Security

- Web Application Firewall (WAF)
- Load Balancer mit TLS-Terminierung
- API Gateway
- Bastion Host
- Öffentliche und private Zertifikate inkl. Management

Identity & Access

- IAM (RBAC, LDAP-Integration)
- Privileged Access Management (PAM)

Daten-Layer

- SQL-Datenbank
- NoSQL-Datenbank
- Object Storage (S3-kompatibel)
- Vektordatenbank
- Redis Cache
- Graph-Datenbank
- Big Data Platform

Messaging & Integration

- Apache Kafka / Event Streaming
- Message Queues (MQ)

DevOps & CI/CD

- Git Repositories
- Runner und Pipelines
- IDE-Integration
- Terraform (Infrastructure as Code)

Observability & Security Operations

- Logging (inkl. SIEM/Splunk-Integration)
- Monitoring
- Real-Time Analytics
- Metriken-Dashboards (Grafana-kompatibel)
- Vulnerability Management

3. Compliance-Mapping

Erstelle eine Matrix, die zeigt, welche Architekturkomponente welche Anforderung der folgenden Regularien adressiert:

- EU AI Act (insb. Hochrisiko-KI-Systeme)
- DSGVO (Datenschutz, Datenverarbeitung, Betroffenenrechte)
- DORA (Operative Resilienz, ICT-Risikomanagement)
- NIS 2 (Cybersicherheit kritischer Infrastrukturen)
- ISO 27001 (ISMS-Kontrollen)

4. Ausgabeformat

- Strukturierte Darstellung nach logischen Architektur-Ebenen (z.B. Netzwerk, Compute, Data, Security, DevOps)
- Tabellarische Übersicht: Komponente | Azure Service | Compliance-Relevanz
- Architekturdiagramm-Beschreibung (textuell), die als Grundlage für ein Visio/Draw.io-Diagramm dienen kann

5. Zusätzliche Hinweise

- Bevorzuge Azure-native Services gegenüber Third-Party-Lösungen, sofern funktional gleichwertig
- Berücksichtige Azure Landing Zones und das Cloud Adoption Framework
- Beachte Data Residency (EU-Region) für alle personenbezogenen Daten
- Schlage eine sinnvolle Netzwerksegmentierung vor (Hub-Spoke, Private Endpoints)

Wesentliche Verbesserungen

Aspekt	Vorher	Nachher
Struktur	Aufzählung ohne Kategorisierung	Logisch gruppierte Komponenten
Erwartungsklarheit	Nur "nenne Azure-Komponenten"	Konkrete Deliverables definiert
Compliance	Nur erwähnt	Explizites Mapping gefordert
Ausgabeformat	Nicht spezifiziert	Tabellen, Matrix, Diagrammbeschreibung
Kontext	Minimal	Azure-spezifische Best Practices einbezogen

Soll ich den Prompt direkt ausführen und die Architektur erstellen?

Prompt:

ja

Antwort (ein docx-Architektur-Dokument wird erstellt):

Ich habe die Dokumentations-Skills gelesen. Jetzt erstelle ich das umfassende Architektur-Dokument. Architektur-Dokument herunterladen

Das Dokument enthält auf ~15 Seiten:

Kernbereiche:

- Executive Summary und regulatorischer Rahmen (EU AI Act, DSGVO, DORA, NIS 2, ISO 27001)
- Detaillierte Komponentenzuordnung in 9 Tabellen mit Azure-Services und Compliance-Mapping
- Compliance-Matrix mit Primär-/Sekundärrelevanz
- Textuelle Diagrammbeschreibung (Layer-Struktur) als Grundlage für Visio/Draw.io
- Phasenplanung für die Implementierung
- Quick Reference mit empfohlenen SKUs/Tiers

Highlights der Azure-Zuordnung:

- **AKS** für Kubernetes mit GPU Node Pools für KI-Worker
- **Azure AI Studio + Semantic Kernel** für Agentic AI
- **Azure AI Content Safety** als Prompt Firewall
- **Microsoft Defender for AI** für Model Scanning
- **Azure AI Search** als Vektor-Datenbank
- **Event Hubs (Kafka API)** für Streaming
- **Microsoft Sentinel** für SIEM/Splunk-Integration
- **Entra ID + PIM** für IAM/PAM