EUDORACLE Technisches Dokument (einfach erklärt)

🔄Projektdauer & Rolle

- Laufzeit: 48 Monate
- Mimi Tech AI ist technischer Partner
- EU-Förderung: ca. 600.000 Euro (100% finanziert)

🈂️Architektur Übersicht

Das System besteht aus mehreren Schichten:

1. **Vor-Ort Ebene (z. B. im Krankenhaus):**
2. Patientendaten (Bilder, Berichte) bleiben lokal
3. Kliniken betreiben eigene Rechner (z. B. mit GPUs) zur Bildauswertung
4. **Föderiertes Lernen (TalTech):**
5. Trainingsdaten bleiben am Standort
6. Es werden nur verschlüsselte Lern-Ergebnisse übertragen
7. Datenschutz durch Techniken wie "Differential Privacy"
8. **Cloud-Ebene (nur für Softwarebereitstellung):**
9. Nutzung europäischer Cloud-Anbieter (z. B. OVH, IONOS)
10. Daten bleiben in der EU (kein Zugriff durch Drittländer)
11. Sicherheit durch "Confidential Computing" (SGX, SEV)
12. **Anwendungsschicht (Mimi Tech AI):**
13. Benutzeroberflächen für Klinikpersonal
14. Schnittstellen (API) zu anderen Partnern
15. KI-Erklärungen (XAI) direkt in der Benutzeroberfläche

Wichtig: Patientendaten verlassen niemals das Krankenhaus. Alles ist verschlüsselt (AES-256, TLS 1.3).

☪️Aufgaben von Mimi Tech AI

- **Benutzeroberflächen:** Moderne, leicht bedienbare Oberflächen für Ärzt:innen
- **Schnittstellen:** Verbindung zu Kliniksystemen (DICOM, FHIR)
- **Plattform-Zusammenbau:** Alle Module arbeiten als ein Gesamtsystem
- **XAI-Visualisierung:** Anzeigen, wie die KI zu ihrer Einschätzung kam (z. B. mit "Heatmaps")

Nicht Aufgabe von Mimi Tech AI: - Betrieb von GPUs oder Training von KI-Modellen - Regulatorische Verantwortung (CE, MDR) - Verwaltung medizinischer Daten

🛜 Technologiestack

- **Frontend:** React, TailwindCSS, TypeScript
- **Backend:** Python (FastAPI), Rust (für schnelle Module)
- **Betrieb:** Kubernetes, Docker, Helm, Pulumi
- **Monitoring:** OpenTelemetry, Grafana, eBPF
- **Security:** OAuth2, mTLS, Vault, Rollenrechte, Audit-Logs
- **Supply Chain Security:** Signierte Container, SBOM, Trivy, reproducible builds
- **Compliance:** Datenschutzberichte, Bias-Checks, Erklärbarkeit, Herkunftsnachweise

---

🆚 Technische Ergebnisse (Mimi Tech AI)

- 3 Benutzeroberflächen (z. B. für Bilddiagnostik, Dokumentation)
- Offizielle API-Dokumentation (FHIR, DICOMweb)
- Visuelle KI-Erklärungen (z. B. SHAP, LIME, Grad-CAM)
- Klinische Validierung mit dem **German Medical Institute (GMI)**
- Leistungskriterien: <3s Antwortzeit, >99% Erklärbarkeit, >99,5% Verfügbarkeit

---

📶 Datenschutz & Regularien

- EU AI Act: Als Hochrisiko-KI eingeordnet
- MDR: Verantwortung liegt beim Partner **GMI**, nicht bei Mimi Tech AI
- Daten bleiben in der EU und sind DSGVO-konform
- Datenschutzfolgeabschätzungen (DPIA) sind vorgesehen
- Alle Vorgänge werden protokolliert (Audit Trail, nicht löschbar)

⚠️ Risiken und Gegenmaßnahmen

Risiko	Lösung
Funktionsausweitung	Klare Abgrenzung der Zuständigkeiten
Schwankende Performance	Messwerte (z. B. Antwortzeit) und Monitoring
Klinische Akzeptanz	Frühzeitige Einbindung medizinischer Nutzer:innen
Regulatorische Änderung	Laufende Beobachtung von MDR & EU KI-Verordnung
Anbieter-Abhängigkeit	Nutzung mehrerer EU-Cloudanbieter

⚪ Zusammenfassung

Mimi Tech AI entwickelt die benutzerfreundlichen Teile der KI-Plattform: Oberflächen, Schnittstellen und KI-Erklärungen. Alle Daten bleiben sicher im Krankenhaus. Partner wie **GMI** oder **TalTech** liefern KI-Modelle und regulatorische Expertise.