

KI in der Entwicklung nutzen – auch für sensible Daten und regulierte Umgebungen.

Souveräne Softwareentwicklung mit KI

KI-Unterstützung für sensiblen Code ermöglichen, einseitige Abhängigkeiten reduzieren und eigene Souveränität stärken

Ein Großteil der leistungsfähigsten KI-Modelle und Entwicklungs-Frameworks stammt heute von einer Handvoll außereuropäischer Unternehmen. Diese Konzentration schafft Abhängigkeiten hinsichtlich Zugang und Konditionen. Zudem können einige Projektklassen, bei denen der Code bzw. die verarbeiteten Daten besonders sensibel sind, nicht mit außer-

europäischen Lösungen verarbeitet werden. Mit einem unabhängigen KI-Stack adressieren wir beide Herausforderungen mit dem Ziel einer zukunftssicheren Infrastruktur, die technologische Unabhängigkeit, Datenschutz und Compliance bei vollständiger Datenkontrolle vereint.

Herausforderungen

- **Abhängigkeit:** Änderungen bei Datenschutzklauseln, regionalen Verfügbarkeiten oder kurzfristige Abschaltungen werden einseitig durch KI-Anbieter vorgenommen. Diese Abhängigkeiten stellen ein unkalkulierbares Betriebsrisiko dar.
- **Verarbeitungsverbot:** Nicht jeder Code darf mit Cloud-basierten KI-Entwicklungs-Frameworks verarbeitet werden. Ohne souveräne Alternative bleibt die KI-Produktivität für einen Teil der Projekte unerreichbar.
- **Unkalkulierbare Kosten:** Variable Token-Preise und Tier-Modelle der Anbieter erschweren die Budgetplanung. Ein flächendeckender Rollout wird zum finanziellen Risiko.
- **Risiken beim Parallelbetrieb:** Wenn proprietäre und souveräne Umgebungen parallel betrieben werden, besteht das Risiko eines Datenabflusses durch Fehlbedienung.

Ganzheitliche Lösung

- **Souveräne Ergänzung:** Souveräne Entwicklungs-Frameworks (z. B. OpenCode oder Pi) kombiniert mit offenen Modellen reduzieren Abhängigkeiten von Modell- und Tool-Anbietern und ermöglichen gleichzeitig die Erweiterung um proprietäre Lösungen wie Claude Code oder GitHub Copilot.
- **Hybride Architektur:** Souveräne und proprietäre Modelle sowie Tools werden über geeignete Architekturen integriert – für On-Premises-, Cloud- oder Hybridbetrieb. Confidential-AI-Lösungen verbinden dabei Cloud-Skalierbarkeit mit kryptografischer Isolation sensibler Daten.
- **Governance-Framework:** Klare Richtlinien für die daten- und projektbezogene Nutzung schaffen einen sicheren, governance-konformen Parallelbetrieb.
- **Integration:** Die Einbindung souveräner Frameworks und Modelle in bestehende Prozess- und Tool-Landschaften ermöglicht einen reibungslosen Betrieb. Semantisches Routing setzt dabei Governance-Vorgaben automatisiert durch.

Business Value

- ✓ **Unabhängigkeit:** Kein Vendor Lock-in bei KI-Harness und KI-Modellen, sodass jederzeit Anpassungen entsprechend den eigenen Anforderungen vorgenommen werden können.
- ✓ **KI-Einsatz für sensiblen Code:** Auch regulierte, vertrauliche und sensible Projekte profitieren von KI-Unterstützung – ohne Kompromisse bei der Datensicherheit.
- ✓ **Datenschutz und Compliance:** Kein Quellcode und keine schützenswerten Informationen verlassen die Infrastruktur. DSGVO, NIS2 und interne Richtlinien werden vollständig eingehalten.
- ✓ **Transparenz & Audit-Fähigkeit:** Die vollständige Kontrolle über Modelle, Datenflüsse und Inferenzprozesse schafft eine belastbare Grundlage für Qualitätssicherung und regulatorische Prüfungen.

Warum S&N?

Leistungen & Expertise

Know-how

- **Fundierte Kenntnisse** im Einsatz souveräner Entwicklungs-Frameworks und offener Modelle in sensiblen Umgebungen.
- **Bewährte Lösungen** für den Einsatz von Confidential Computing zur Verschlüsselung der Daten während der Modellausführung.
- **Mehrjährige Praxiserfahrung** in der Anwendung unterschiedlichster Coding-Harnesses und Best Practices (u. a. Coding-Assistants wie Claude Code, Pi, Codex oder Cursor).
- **Praxiserprobte Referenzarchitekturen** für souveräne KI-Plattformen sowie innovative Lösungen, z. B. für semantisches Routing.
- **Langjährige Erfahrung** in der Implementierung von Governance-Regeln für Unternehmen in regulierten Branchen.

Unser Angebot

- **Beratung:** Evaluierung der bestehenden Toolchain und Definition des technologischen Zielbilds auf Basis souveräner Frameworks und geeigneter Modelle.
- **AI-Coding-Plattform:** Konzeption einer resilienten KI-Architektur als On-Premises- oder Hybridlösung mit flexibler Integration offener und proprietärer Modelle sowie Entwicklungswerkzeuge.
- **Plattform & Integration:** Aufbau einer zentralen KI-Coding-Infrastruktur mit intelligentem Gateway für automatisiertes semantisches Routing und Integration in bestehende Prozesse.
- **Coding-Harness & Enablement:** Bereitstellung und Konfiguration eines geschützten und eigenverantworteten Coding-Harness. Zudem Enablement entlang der Identpendedn-AI-Chin sowie Unterstützung bei Finetuning, Betrieb und Agent-/Skill-Engineering.

Ansprechpartner



Maximilian Blume

Maximilian.Blume@sn-invent.de