

Sicherer, europäisch ausgerichteter KI-Betrieb mit ÉLAN

Technische und organisatorische Stellungnahme für Unternehmen mit hohen Anforderungen an Datenschutz, Nachvollziehbarkeit und verantwortungsvollen KI-Einsatz.

Geltungsbereich: ÉLAN-Portal und KI-gestützte Fachprozesse **Ausgestellt durch:** BSV / ÉLAN-Team

Unser Grundsatz: sichere Betriebsbasis, klar getrennte Datenflüsse und menschliche Verantwortung.

ÉLAN verbindet eine deutsche Hosting-Umgebung mit einer kontrollierten KI-Anbindung. Fachsysteme bleiben führend; KI unterstützt Anwenderinnen und Anwender, ersetzt jedoch keine fachliche Prüfung oder Verantwortung.

Was Kundinnen und Kunden von ÉLAN erwarten können

ÉLAN ist für einen nachvollziehbaren Einsatz in europäischen Unternehmensprozessen konzipiert. Die Betriebsarchitektur trennt Portal, Integrationen, Fachsysteme und KI-Verarbeitung. Damit lassen sich Rollen, Datenflüsse und Verantwortlichkeiten sauber beschreiben und je Kundenprojekt kontrolliert konfigurieren.

Deutsche Betriebsbasis. Die ÉLAN-Anwendung wird auf deutscher STRATO-Infrastruktur betrieben. Das betrifft Portal, Anwendungsdienste und die zugehörige Betriebsumgebung.

Flüchtige Laufzeit, kontrollierte Persistenz. Container werden aus versionierten Images bereitgestellt und können reproduzierbar ersetzt werden. Dauerhafte Daten werden nicht in der flüchtigen Laufzeitschicht versteckt, sondern ausschließlich in dafür vorgesehenen Speichern geführt.

Keine Modellverbesserung aus API-Inhalten standardmäßig. Bei der OpenAI API werden übermittelte Inhalte standardmäßig nicht zum Trainieren oder Verbessern der Modelle verwendet. Die KI-Anbindung wird als externer Verarbeitungsschritt transparent behandelt.

Menschliche Kontrolle. KI-Ausgaben sind fachliche Unterstützung. Operative Entscheidungen und Geschäftsvorgänge verbleiben in der Verantwortung der berechtigten Mitarbeitenden und der führenden Fachsysteme.

Wichtig für die Einordnung: Deutsches Hosting der ÉLAN-Anwendung und der Ort einer externen KI-Verarbeitung sind getrennte Sachverhalte. Diese Stellungnahme benennt beide bewusst getrennt.

Technische Architektur und Datenbehandlung

Die Architektur folgt dem Prinzip der funktionalen Trennung: Die Anwendungsoberfläche, die Schnittstellenlogik, die führenden Fachsysteme und die KI-Verarbeitung haben unterschiedliche Aufgaben und werden entsprechend getrennt betrachtet.

Baustein	Betriebsmodell	Datenbehandlung
ÉLAN Portal und BFF	Container auf deutscher STRATO-Infrastruktur; versioniert und reproduzierbar ausgerollt.	Die Laufzeitschicht ist ersetzbar. Dauerhafte Anwendungsdaten liegen nur in ausdrücklich vorgesehenen Volumes bzw. Datenbanken.
MCP-Gateway	Getrennter Integrationscontainer für kontrollierte Schnittstellenaufrufe.	Für den Gateway-Container ist kein Anwendungsdaten-Volume eingebunden; Betriebsprotokolle sind hiervon getrennt zu betrachten.
ERP und Identität	Fach- und Identitätssysteme bleiben die führenden Stellen für die jeweiligen Geschäftsprozesse.	Nur die für einen angeforderten Prozess erforderlichen Angaben werden über Schnittstellen verarbeitet.
KI-Service	OpenAI API als externer, kontrolliert angebundener KI-Verarbeiter.	Für die Bearbeitung erforderliche Ein- und Ausgaben; keine Modellverbesserung aus API-Inhalten standardmäßig. Residenz wird projektbezogen festgelegt.

Containerprinzip und Speicherkonzept

Containerisierung bedeutet bei ÉLAN: Anwendungskomponenten laufen isoliert und können anhand einer definierten Version neu erstellt werden. Dies verbessert die Wiederholbarkeit von Updates und die Abgrenzung der Komponenten.

Gleichzeitig wird nicht verschleiert, dass Betriebsdaten, Protokolle oder fachliche Daten dauerhaft sein können. Solche Daten gehören in explizit definierte Datenbanken, Volumes oder Systeme und sind Gegenstand eines kundenbezogenen Lös- und Berechtigungskonzepts. Ein flüchtiger Container ersetzt keine Datenklassifizierung.

KI-Verarbeitung und europäische Datenresidenz

ÉLAN übermittelt an den KI-Service nur Inhalte, die für die angeforderte Unterstützung erforderlich sind. Der KI-Service wird über die OpenAI API angebunden; API-Inhalte werden standardmäßig nicht für das Training der Modelle genutzt.

Für Kunden mit einer europäischen Residenzvorgabe wird die KI-Projektkonfiguration gesondert eingerichtet und nachgewiesen. Dazu gehört die ausgewählte Region, die zulässigen Aufbewahrungs- und Missbrauchsschutz-Einstellungen sowie die vertragliche Grundlage. Eine europäische Region ist nicht automatisch eine Zusage für eine ausschließlich deutsche KI-Verarbeitung; dies wird projektbezogen präzise dokumentiert.

Vor der produktiven Nutzung kann die gewünschte Datenresidenz gemeinsam gegen Projektkonfiguration, Auftragsverarbeitung und Nachweise abgeglichen. So wird aus einer Anforderung eine nachvollziehbare Betriebsvereinbarung.

Projektbezogene Absicherung und Transparenz

Für einen Kundenbetrieb mit erhöhtem Schutzbedarf konkretisieren wir die folgenden Punkte pro Projekt schriftlich:

- 1. Datenfluss und Zweck.** Welche Datenarten an welcher Stelle verarbeitet werden und welche Fachsysteme führend bleiben.
- 2. Region und Verarbeitung.** Welche Hosting- und KI-Region gewählt ist, welche Dienste beteiligt sind und welcher Nachweis hierzu vorliegt.
- 3. Aufbewahrung und Löschung.** Welche fachlichen Daten, Anwendungsdaten und Betriebsprotokolle wie lange benötigt werden und wie Löschvorgaben umgesetzt werden.
- 4. Berechtigung und Freigabe.** Wer Funktionen nutzen darf, welche Schnittstellenzugriffe erforderlich sind und wo eine fachliche Bestätigung erforderlich bleibt.
- 5. Vertragliche Grundlage.** Auftragsverarbeitungs- und Datenschutzunterlagen der beteiligten Anbieter sowie projektspezifische technische und organisatorische Maßnahmen.

Verantwortungsvoller KI-Einsatz in Europa

ÉLAN ist als unterstützendes System ausgelegt. Anwenderinnen und Anwender sollen KI-Ausgaben prüfen, bevor sie daraus geschäftliche Handlungen ableiten. Je nach Einsatzgebiet können darüber hinaus Informations-, Risiko- oder Governancepflichten gelten. Diese werden gemeinsam mit dem Kunden in die konkrete Nutzung überführt.

Technische Grundlagen und Nachweise

Die folgenden öffentlich verfügbaren Grundlagen werden bei der Projektprüfung herangezogen:

STRATO — Serverstandort und Sicherheit: <https://www.strato.de/server/server-place/>

OpenAI API — Data controls: <https://developers.openai.com/api/docs/guides/your-data>

EU-Kommission — Transparenzpflichten nach Artikel 50 AI Act: <https://digital-strategy.ec.europa.eu/en/library/guidelines-transparency-obligations-providers-and-deployers-ai-systems>

Hinweis zur Verbindlichkeit: Diese technische Stellungnahme beschreibt den vorgesehenen Betriebsrahmen und ersetzt keine individuelle Rechtsberatung oder Zertifizierung. Verbindlich werden regionale Verarbeitung, Aufbewahrung und Maßnahmen erst durch die kundenspezifische Konfiguration und die zugehörigen Vertragsunterlagen.

BSV / ÉLAN-Team

Für Fragen zur projektspezifischen Datenschutz- und Betriebsdokumentation.