

Maximal geschützt

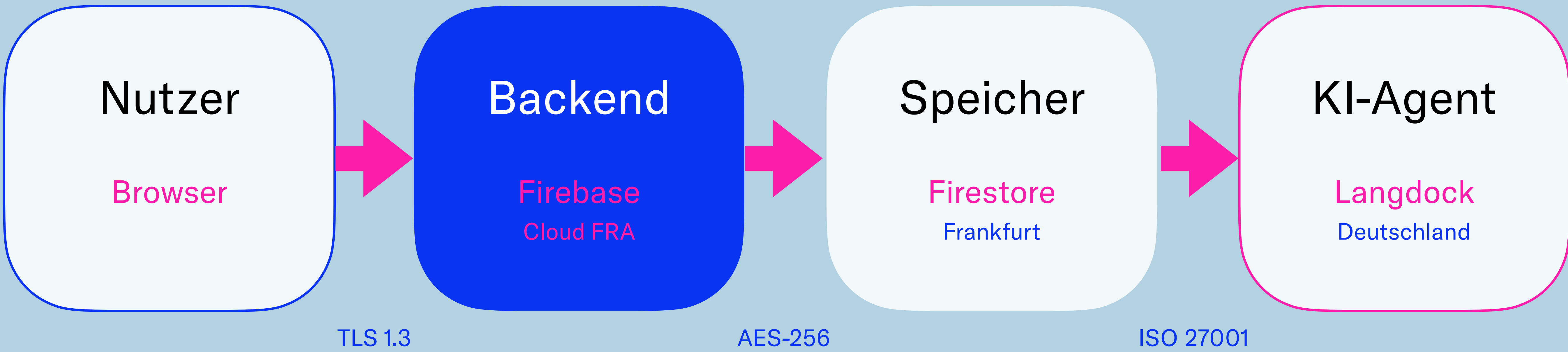
Unsere Sicherheitsarchitektur

Datenschutz hat bei uns Priorität. Wenn Sie in Ihrem Browser eine Anfrage eingeben, wird diese nicht ungeschützt ins Internet gesendet. Zunächst erreicht sie das findig-Backend in zertifizierten Rechenzentren von Google in Frankfurt. Dort wird Ihre Identität geprüft und die Anfrage verschlüsselt – nach Sicherheitsstandards, wie sie auch im Bankwesen üblich sind.

Anschließend wird die Anfrage an die deutsche Plattform Langdock weitergeleitet. Langdock fungiert als Vermittler und überträgt die Daten an die europäischen Server der eingesetzten Sprachmodelle. Ein wesentlicher Vorteil dabei: Die Verarbeitung erfolgt innerhalb der EU. Damit gelten die strengen Anforderungen der DSGVO sowie die regulatorischen Vorgaben des EU AI Act.

Die Verarbeitung erfolgt ausschließlich temporär. Die Daten werden weder gespeichert noch für das Training der KI verwendet. In Kombination mit der europäischen Datenverarbeitung schafft dies eine hohe regulatorische Sicherheit und Transparenz.

Der gesamte Datenfluss bleibt innerhalb eines geschlossenen europäischen Systems.



Kein Browser kommuniziert direkt mit der KI — jede Anfrage wird serverseitig authentifiziert.

Vier Sicherheitssäulen

Zugriff	Verschlüsselung	Datenschutz	Compliance
• Rollenbasiertes Berechtigungsmodell • MFA für alle Admins • Kein Bypass möglich • Admins sehen keine Chat-Inhalte	• TLS 1.3 bei Übertragung • AES-256 bei Speicherung • API-Keys im Secret Manager • HTTPS erzwungen (HSTS)	• 100% EU: Frankfurt (DE) • Kein Training auf Ihren Daten • Keine Weitergabe an Dritte • Löschung: max. 12 Monate	• DSGVO Art. 28 AVV • ISO 27001 (Langdock zertifiziert) • Datenpanne: Meldung < 48h • Google Multi-Zone Redundanz