1 KI & Datensouveränität – Management Summary

1.1 Einleitung

Die zunehmenden geopolitischen Spannungen verändern die globale Technologielandschaft grundlegend. Für europäische Unternehmen stellt sich zunehmend die Frage, wie sie ihre digitale Souveränität sichern und Abhängigkeiten von außereuropäischen Anbietern reduzieren können. Als Lector haben wir uns frühzeitig strategisch positioniert: Wir setzen konsequent auf europäische Infrastruktur, transparente Partnerschaften und höchste Sicherheitsstandards.

1.2 Unsere Position: Europäische Datensouveränität

- **Europäische Cloud-Infrastruktur:** Wir setzen auf europäische Cloud-Anbieter – allen voran OVH als unser Haupt-Cloudpartner mit Rechenzentren in Deutschland und Frankreich. Auch bei der Nutzung internationaler Anbieter wie Microsoft Azure oder Google Cloud erfolgt die Datenverarbeitung ausschließlich in EU-Rechenzentren (Germany West Central bzw. Frankfurt).
- **Europäisches KI-Hosting:** Wir nutzen ausschließlich KI-Modelle, die in Europa gehostet werden. Wo sinnvoll, bevorzugen wir europäische KI-Lösungen wie Mistral sowie Open-Source-Modelle.
- **Maximale Kontrolle:** Wir unterstützen vollständig On-Premises-Installationen. Dabei verbleiben sämtliche Daten in der kundeneigenen Infrastruktur – ohne Datenübermittlung an externe Dienste.
- **Subunternehmer-Transparenz:** Alle eingesetzten Subunternehmer sind vertraglich gebunden und verarbeiten Daten ausschließlich an EU-Standorten.

1.3 Regulatorische Compliance

- **EU-AI Act:** Lector fällt nach eingehender Prüfung in die Kategorie **„minimales Risiko”** gemäß EU-AI Act. Unsere Lösung beschränkt sich auf Dokumentenklassifikation und Informationsextraktion – ohne autonome Entscheidungsfindung. Menschliche Kontrolle und Korrektur sind ausdrücklich vorgesehen.
- **DSGVO:** Wir erfüllen alle Anforderungen der DSGVO. Datenschutz-Folgenabschätzungen (DSFA) werden bei Bedarf durchgeführt. Eine Datenschutzbeauftragte ist benannt.
- **Kontinuierliche Compliance-Überwachung:** Zukünftige Entwicklungen und regulatorische Änderungen werden aktiv beobachtet und bewertet.

1.4 Nach außen: Partnerschaften & Ökosystem

Akademische Zusammenarbeit

- Unsere Wurzeln liegen in der europäischen akademischen Forschung, mit der wir bis heute eng verbunden sind.
- Wir unterstützen aktiv Studierende, indem wir ihnen praktischen Zugang zu KI ermöglichen – beispielsweise durch die Übertragung konkreter Aufgaben als praxisnahe Lernmöglichkeiten.

Open-Source-Engagement

- Wir engagieren uns im Open-Source-KI-Ökosystem: Wir tragen zur Entwicklung von Open-Source-LLMs bei und bieten Open-Source-Lösungen im Bereich Machine Learning an.

Branchenallianzen und Partnerschaften

- **ARIC Hamburg:** Wir sind Mitglied im Artificial Intelligence Center Hamburg (ARIC), dem offiziellen KI-Netzwerk für Norddeutschland. ARIC verbindet Wirtschaft, Wissenschaft und Gesellschaft, um verantwortungsvolle, menschenzentrierte KI-Innovationen zu fördern und praktisch anzuwenden.
- **OVH Open Trusted Cloud:** Als Partner des OVH Open Trusted Cloud Programms setzen wir auf ein offenes, vertrauenswürdiges Cloud-Ökosystem, das europäische Standards für Datensouveränität und Datenschutz (GDPR) erfüllt. Die Infrastruktur ist unabhängig vom US CLOUD Act und unterliegt ausschließlich europäischer Rechtsprechung.
- Wir beteiligen uns aktiv in weiteren Branchenallianzen und Interessengruppen, die sich dem Aufbau von KI-Expertise in Deutschland und Europa widmen.

1.5 Nach innen: Sicherheit & Prozesse

Technische Maßnahmen

- Konsequentes Rechtemanagement nach dem Least-Privilege-Prinzip
- Multi-Faktor-Authentifizierung (MFA) für alle Zugänge
- Verschlüsselung aller Daten – im Ruhezustand (AES-256) und während der Übertragung (TLS)
- Detaillierte Protokollierung aller Systemaktivitäten
- Automatisierte Systemüberwachung mit Alarmierung
- Intrusion Detection und Prevention Systeme (IDS/IPS)
- Firewall, Spamfilter und Virenscanner mit regelmäßiger Aktualisierung

Organisatorische Maßnahmen

- Regelmäßige Schulungen zu Datenschutz und Informationssicherheit für alle Mitarbeitenden
- Dokumentiertes Incident-Response-Management mit klarem Prozess zur Erkennung, Meldung und Nachbearbeitung von Sicherheitsvorfällen
- Mehrstufiges Backup- und Recovery-Konzept mit regelmäßigen Wiederherstellungstests
- Notfallplan für alle eingesetzten Systeme
- Jährliche Überprüfung aller technischen und organisatorischen Maßnahmen

Softwareentwicklung

- Moderne Entwicklungsprozesse nach aktuellem Stand der Technik
- Verpflichtende Code-Reviews für alle Änderungen
- Automatisierte Tests und Continuous Integration
- Kontrolliertes Release-Management mit Versionierung
- Dokumentierte Best Practices und Qualitätsstandards

1.6 Umgang mit Hochrisikodaten

- Wir verarbeiten hochsensible Daten aus kritischen Sektoren: Gesundheitswesen, Krankenversicherungen, Rechtswesen und Logistik.
- Bis heute wurden alle Cyberangriffe erfolgreich abgewehrt – es wurden keine Daten gestohlen, und unsere Systeme wurden nie kompromittiert.
- An kritischen Stellen unserer Infrastruktur orientieren wir uns an den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI).
- **ISO 27001 Zertifizierung:** Wir befinden uns aktuell im Zertifizierungsprozess mit geplantem Audit im Sommer 2026.
- **Penetration Tests:** Im Herbst 2026 sind umfassende Penetration Tests geplant, um die Sicherheit unserer Systeme zusätzlich zu validieren.

1.7 Ausblick: Nächste Schritte

Maßnahme	Zeitrahmen
ISO 27001 Zertifizierung	Sommer 2026
Penetration Tests	Herbst 2026

Stand: 01.02.2026

© 2026 lector.ai GmbH - Alle Rechte vorbehalten