KI-Compliance-Checkliste

Welche Fragen musst du stellen, bevor du KI-Infrastruktur aufbaust?

Du jagst Dokumente durch ein KI-Modell, analysierst Kundendaten oder trainierst eigene Modelle – das sind sensible Informationen, Geschäftsgeheimnisse und proprietäre Inhalte. Wer diese Daten auf US-Hyperscalern betreibt, riskiert ungewollten Datenzugriff durch US-Behörden (CLOUD Act), Compliance-Verstösse und Haftungsrisiken. Diese Checkliste hilft dir, die richtigen Fragen zu stellen.

1 Datensouveränität & Jurisdiktion

- [ ] Wo werden meine Trainings- und Inferenzdaten physisch gespeichert?
- [ ] Können US-Behörden Zugriff auf meine Daten verlangen, ohne mich zu informieren?
- [ ] Unterliegt mein Anbieter einer US-Jurisdiktion, auch wenn die Server in Europa stehen?
- [ ] Ist der Gerichtsstand vertraglich in der Schweiz geregelt?
- [ ] Habe ich eine Datenverarbeitungsvereinbarung (DVV) abgeschlossen?

2 Regulatorische Anforderungen & Aufsicht

- [ ] Welche regulatorischen Vorgaben gelten für meine Branche bei Datenhaltung und Auslagerung (FINMA 2008/7, HMG, kantonales DSG)?
- [ ] Sind KI-Auslagerungen in meiner Outsourcing-Richtlinie erfasst?
- [ ] Habe ich Exit-Strategien und Notfallpläne dokumentiert?
- [ ] Können Prüf- und Aufsichtsbehörden im Bedarfsfall Zugang zu Systemen und Logs erhalten?
- [ ] Sind Verantwortlichkeiten bei KI-Entscheidungen klar geregelt?

3 Datenschutz (DSG / DSGVO)

- [ ] Welche Personendaten fliessen in meine KI-Modelle ein?
- [ ] Habe ich eine Datenschutz-Folgeabschätzung (DSFA) durchgeführt?
- [ ] Sind Trainings- und Inferenzdaten pseudonymisiert oder anonymisiert?
- [ ] Wie lange werden Daten aufbewahrt und wer hat Zugriff?
- [ ] Sind Betroffenenrechte (Auskunft, Löschung) sichergestellt?

4 Sicherheit & Zertifizierungen

- [ ] Ist mein Infrastrukturanbieter ISO 27001 zertifiziert?
- [ ] Gibt es regelmässige Sicherheitsaudits und Penetrationstests?
- [ ] Sind Backup- und Disaster-Recovery-Prozesse definiert und getestet?
- [ ] Welche SLAs gelten für Verfügbarkeit und Reaktionszeiten?
- [ ] Sind Zugriffsrechte und Netzwerkisolation klar definiert?

5 Technische Anforderungen

- [ ] Welche GPU-Spezifikationen benötige ich (Training vs. Inferenz)?
- [ ] Brauche ich dedizierte Hardware oder reicht geteilte Infrastruktur?
- [ ] Wie skaliere ich bei wachsenden Anforderungen?
- [ ] Habe ich einen direkten technischen Ansprechpartner?
- [ ] Sind Netzwerklatenz und Bandbreite für meine Workloads ausreichend?

6 Anbieterauswahl & Verträge

- [ ] Wo hat mein Anbieter seinen Firmensitz und Rechenzentren?
- [ ] Setzt mein Anbieter selbst US-Subprozessoren ein, und falls ja, für welche Dienste?
- [ ] Welche Zertifizierungen weist der Anbieter vor (ISO 27001, ISO 9001)?
- [ ] Gibt es einen persönlichen Ansprechpartner statt anonymem Support?
- [ ] Wie ist der Anbieter in einer Krisensituation erreichbar (24/7)?