KI.SH

Leitfragen KI-Souveränität

Datensouveränität

- **Wo** werden meine **Unternehmensdaten** bei KI-Nutzung **gespeichert und verarbeitet**?
- **Wer hat** in meinem Unternehmen aktuell **Zugriff** auf welche **KI-Systeme und Daten**?
- Habe ich die **Zustimmung meiner Kund:innen und Mitarbeiter:innen**, deren Daten in KI-Systemen zu verarbeiten?
- Unter welchem **Rechtssystem** erfolgt diese Speicherung (EU-DSGVO oder US Cloud Act)?
- Kann ich die **Löschung** meiner Daten beim Anbieter **nachweislich erzwingen**?
- Werden meine Daten für das **Training des Anbieters** genutzt?
- Werden auch **Metadaten** (z.B. Nutzungsverhalten, Zeitstempel, Eingabelängen) beim Anbieter gespeichert?

Modellsouveränität

- **Welche KI-Modelle und Anbieter werden** aktuell in meinem Unternehmen **genutzt**?
- Bin ich **an einen einzigen Anbieter gebunden**? Was würde ein **Wechsel** kosten?
- Wie **transparent ist die Qualitätsentwicklung** des Modells?
- Werde ich **informiert**, wenn sich das Modellverhalten durch **Updates** verändert?
- Kann ich bei Bedarf auf **ältere Versionen** zugreifen?
- Kann ich das Modell für **meine spezifischen Anforderungen anpassen**?
- Verstehe ich, **nach welchen Regeln** das Modell **antwortet**? Kann ich diese **Regeln** bei Bedarf **beeinflussen**?
- Welche **Inhalte** lehnt das Modell ab, und **wer legt diese Grenzen fest**?

Infrastruktursouveränität

- Auf **wessen Infrastruktur** läuft meine KI?
- Was passiert bei einem **Ausfall** des Anbieters?
- **Welche Infrastruktur** wäre **nötig**, um meinen KI-Anwendungsfall **lokal zu betreiben**?
- Ist meine KI-Infrastruktur in meine bestehende **IT-Sicherheitsstrategie** eingebunden?
- Gibt es eine **Notfallstrategie**?

Governance

- Gibt es **interne Richtlinien**, welche Daten in welche KI-Systeme eingegeben werden dürfen?
- Wer im Unternehmen ist **verantwortlich** für KI-Entscheidungen und deren Konsequenzen?
- Gibt es einen **definierten Prozess**, neue KI-Tools vor der **Einführung** zu prüfen und freizugeben?
- Wie werden die Anforderungen des **EU AI Act und der DSGVO** berücksichtigt?
- Können meine KI-Entscheidungen **auditiert und erklärt** werden?

Kompetenz

- Werden Mitarbeiter:innen **regelmäßig** über **neue KI-Risiken und Möglichkeiten informiert**?
- Gibt es **interne Ansprechpersonen** oder **Power-User**, die KI-Wissen aktiv im Unternehmen weitergeben?
- Hat mein Team genug **Wissen**, um KI-Systeme und -Anbieter **kritisch zu beurteilen**?
- Welche **Kompetenz** für die **eigenständige Inbetriebnahme und Wartung** von KI-Systemen sind vorhanden oder müssten erworben werden?
- Wofür wird **externe Unterstützung** benötigt?

KI.SH, bestehend aus dem KI-Anwendungszentrum und dem KI-Transfer-Hub, wird gefördert aus dem Landesprogramm Wirtschaft 2021-2027 mit Mitteln des Europäischen Fonds für regionale Entwicklung.

Kofinanziert von der Europäischen Union

SH Schleswig-Holstein Landesregierung