

STARTERKIT

KI-Governance-Starterkit für KMU

Offenlegungsregeln, Freigabe-Workflows, Prompt- und Asset-Register sowie Datengrenzen, dimensioniert für ein Schweizer KMU unter DSG - Governance ohne Enterprise-Bürokratie.

Governance, die zu einem KMU passt

Enterprise-KI-Governance setzt eine Compliance-Abteilung voraus. Ein KMU hat dieselbe Exposition - Kundendaten in Prompts, ungeprüfte Ergebnisse beim Kunden, Mitarbeitende mit nicht freigegebenen Tools - ohne das Personal. Dieses Kit ist eine minimal tragfähige Policy: vier Dokumente und eine Gewohnheit, genug um 'was ist unsere KI-Policy?' vor Kunden oder Auditoren glaubwürdig zu beantworten.

Dokument eins: zulässige Nutzung

- Freigegebene Tool-Liste - welche KI-Dienste Mitarbeitende beruflich nutzen dürfen, und mit welchen Konten (firmenverwaltet, nicht privat)
- Datenklassen - was nie in einen Prompt darf: Personendaten von Kunden, Zugangsdaten, unveröffentlichte Finanzzahlen, Vertragstexte Dritter
- Output-Regeln - KI-Output ist Entwurf; extern verwendete Texte, Code und Analysen brauchen menschliche Prüfung vor Einsatz
- Offenlegung - wann Kunden informiert werden müssen, dass KI beigetragen hat (Support-Antworten, Gutachten, generierte Medien)

Dokument zwei: der Freigabe-Workflow

Eine benannte Person genehmigt: neue Tools, neue Anwendungsfälle für Personendaten und alles KI-Generierte, das unter Firmennamen das Haus verlässt. Der Workflow ist bewusst kurz - schriftliche Anfrage, Ja/Nein mit Bedingungen, eine Zeile im Register. Dauert die Freigabe mehr als einen Tag, wird sie umgangen.

Dokument drei: das Register

Eine einzige Tabelle mit drei Tabs beantwortet die meisten Auditfragen: eingesetzte Tools (Name, Zweck, Kontoinhaber, erlaubte Datenklassen), produktiv genutzte Prompts und Templates sowie an Kunden gelieferte KI-gestützte Arbeiten. Pflegeaufwand: zehn Minuten pro Woche - der Unterschied zwischen 'wir haben Governance' als Behauptung und als Fakt.

Dokument vier: Datengrenzen

- Nach dem DSG (dem Schweizer Datenschutzgesetz) ist das Einspeisen von Personendaten in einen externen KI-Dienst eine Bekanntgabe an Dritte - die Rechtsgrundlage dokumentieren oder nichts senden
- Für alles mit Kundendaten Tools mit vertraglicher No-Training-Zusage bevorzugen
- Selbst gehostete Inferenz ist eine Option für sensitive Workloads - sie erübrigt die Drittparteien-Frage, zum Preis korrekten Betriebs
- Aufbewahrung: festlegen, wie lange Prompts und Outputs aufbewahrt werden und wer sie einsehen kann

Die eine Gewohnheit

Vierteljährlich, dreissig Minuten: das Register durchgehen, prüfen ob die Tool-Liste noch zur Realität passt, und die Nutzungsseite an alle Mitarbeitenden neu verteilen. Governance, die nicht geübt wird, ist Dekoration.

- ☐ Nutzungsseite verfasst und verteilt
- ☐ Verantwortliche Person für die Freigabe neuer Werkzeuge und Datennutzungen benannt
- ☐ Register existiert: Tools, Prompts, gelieferte Arbeiten
- ☐ Datenklassen definiert; Kundendaten-Regeln explizit
- ☐ Vierteljährliche Prüfung terminiert

Dieses Dokument ist Teil der UHL-Ressourcen. Direkter Download und verwandte Arbeiten: <https://uhl-services.ch/de/resources/>

