

Lokale KI: Daten zuordnen, Pilotprojekt planen

Ordne deine Unterlagen einer Datenklasse zu, kläre die Fragen vor dem Start und leg fest, woran du das Pilotprojekt misst. Die Übersicht ist ein Ausgangspunkt, keine Freigabe und keine Rechtsberatung.

1 · WELCHE DATEN IN WELCHE KI

Datenklasse	Gratis- oder Privatkonto	Cloud mit Firmenvertrag	Box im EU-Rechenzentrum	Lokal im eigenen Haus
Öffentliche Inhalte Website, Produkttexte	✓ passt	✓ passt	✓ passt	✓ passt
Interne Unterlagen Handbücher, Angebote	✗ eher nicht, kein Vertrag	✓ passt, Training aus	✓ passt, Vertrag mit dem Dienstleister	✓ passt, Zugriffsrechte regeln
Personenbezogene Daten Kunden, Mitarbeitende	✗ eher nicht, kein Vertrag	! mit Auflagen, Vertrag zur Auftragsverarbeitung und Datenstandort	✓ passt, Vertrag zur Auftragsverarbeitung	✓ passt, Zugriffsrechte regeln
Besonders geschützt Gesundheit, Mandate	✗ eher nicht, kein Vertrag	! mit Auflagen, Prüfung im Einzelfall	! mit Auflagen, Schweigepflicht nach § 203 StGB	✓ passt, Zugriffsrechte regeln

So liest du die Übersicht: ✓ passt in der Regel, ! nur mit Auflagen, ✗ eher nicht. Auch lokal brauchst du eine Rechtsgrundlage, Zugriffsrechte und Löschfristen, sobald personenbezogene Daten im Spiel sind. Wartet ein Dienstleister die Box im eigenen Haus, gelten die Auflagen der betreuten Box.

2 · VOR DEM PILOTPROJEKT KLÄREN

- ☐ Die Aufgabe steht in einem Satz fest.
 ☐ Die Ordner, die die KI lesen darf, sind festgelegt.
 ☐ Die Zahl gleichzeitiger Nutzer ist geschätzt.
 ☐ Löschfristen für Dokumente, Protokolle und Chatverläufe stehen fest.
 ☐ Wartet ein Dienstleister die KI, liegt ein Vertrag zur Auftragsverarbeitung vor.
- ☐ Die Unterlagen sind einer Datenklasse zugeordnet.
 ☐ Klar ist, wer welche Antworten sehen darf.
 ☐ Fachlich, technisch und für den Datenschutz ist je eine Person zuständig.
 ☐ Die Lizenz des Modells erlaubt deine gewerbliche Nutzung.
 ☐ Verzeichnis, Information der Betroffenen und bei Bedarf Datenschutz-Folgenabschätzung sind erledigt.

3 · PILOTPROJEKT AUSWERTEN

Kriterium	Ziel vor dem Start	Ergebnis danach
Antwortqualität · richtige Antworten von 20 Testfragen		
Quellenangabe · Antwort nennt das richtige Dokument		
Zugriffsrechte · keine Inhalte außerhalb der Freigabe		
Zeitgewinn · gesparte Stunden je Woche im Team		
Nutzung · wie viele im Team arbeiten regelmäßig damit		

Auswertung: Leg die Ziele fest, bevor das Pilotprojekt startet. Erreicht es sie, legst du die Betriebsform und die Zuständigen dauerhaft fest. Verfehlt es ein Ziel deutlich, prüfst du zuerst Quellen und Zugriffsrechte, dann die Modellgröße.

Du willst Firmenwissen mit einer lokalen KI nutzen?

Schreib mir, welche Unterlagen die KI beantworten soll. Ich sage dir, welche Betriebsform technisch und organisatorisch zu deinen Daten passt.

hallo@inventivo.de