Shadow-AI-Bestandsaufnahme

in 5 Schritten

Arbeitsvorlage für den Mittelstand

Pragmatisch. Sofort einsetzbar. Ohne Großprojekt.

Martin Müller – KI-Beratung für den Mittelstand | Weniger Show, mehr Wirkung.
martin@martin-mueller-ki.de

Warum diese Vorlage?

Laut Bitkom nutzen 42 % der deutschen Unternehmen bereits KI-Tools am Arbeitsplatz – aber nur 29 % sind sicher, dass keine privaten Tools im Einsatz sind. Die restlichen 71 % haben einen blinden Fleck.

Diese Vorlage hilft Ihnen, in 5 strukturierten Schritten Sichtbarkeit über die KI-Nutzung in Ihrem Unternehmen zu bekommen – ohne Verbote, ohne Tool-Theater, ohne Großprojekt.

Zeitaufwand: ca. 2–3 Stunden für die Ersterhebung, verteilt auf 2 Wochen.

Schritt 1: Inventarisieren

Ziel: Einen Überblick bekommen, welche KI-Tools in welchen Teams für welche Zwecke genutzt werden.

So gehen Sie vor:

- Senden Sie eine kurze 5-Fragen-Umfrage an alle Teamleiter (dauert 10 Min pro Person).
- Fragen Sie: Welche Tools? In welchen Teams? Für welche Use Cases? Welche Daten fließen rein? Wie häufig?
- Tragen Sie die Ergebnisse in die folgende Tabelle ein:

KI-Tool / Anwendung	Team / Abteilung	Use Case	Datentypen	Quelle / Hinweis
z.B. ChatGPT (privat)	Vertrieb	Angebotstexte	Kundendaten, Preise	Teamleiter-Umfrage
z.B. DeepL Pro	Marketing	Übersetzungen	Produkttexte	IT-Audit
z.B. Copilot (privat)	HR	Stellenanzeigen	Anforderungen	Selbstauskunft

Schritt 2: Daten klassifizieren

Ziel: Für jeden Use Case bewerten, welche Art von Daten in KI-Tools fließt – und ob das in Ordnung ist.

Nutzen Sie die Ampel-Logik:

Datentyp	Beispiele	Ampel	Regel
Öffentliche Daten	Produktinfos, FAQs, Blog-Texte	**GRÜN – frei nutzbar**	Darf in jedes KI-Tool
Interne Daten	Umsatzzahlen, Prozesse, Strategiepapiere	**GELB – nur freigegebene Tools**	Nur in genehmigten Tools mit DPA
Personenbez. / sensible Daten	Kundendaten, Verträge, Gehälter, Patente	**ROT – nicht in KI-Tools**	Nie in externe KI-Tools eingeben

Tragen Sie die Ampelfarbe in Schritt 3 für jeden Use Case ein.

Schritt 3: Risiko bewerten (light)

Ziel: Die wichtigsten Use Cases nach Risiko einordnen – Fokus auf die Top 10, nicht auf Vollständigkeit.

Bewertungskriterien:

- Daten-Ampel (aus Schritt 2)
- Nutzungshäufigkeit (täglich / wöchentlich / selten)
- Anzahl betroffener Personen / Kunden

Use Case	Daten-Ampel	Häufigkeit	Personenanzahl	Risiko gesamt	Maßnahme
Angebotstexte formulieren	ROT	Täglich	5+	**HOCH**	Leitplanken + erlaubtes Tool
Blog-Texte erstellen	GRÜN	Wöchentlich	2	**NIEDRIG**	Freigabe, keine Einschränkung
Bewerbungen vorfiltern	ROT	Wöchentlich	3	**HOCH**	DPA prüfen, Prozess definieren

Faustregel: Rote Daten + tägliche Nutzung + viele Personen = HOCH. Grüne Daten + selten = NIEDRIG.

Schritt 4: Leitplanken definieren

Ziel: Klare Regeln schaffen, mit denen Mitarbeitende KI sicher nutzen können – statt Verbote auszusprechen.

Füllen Sie die folgenden Felder aus:

Kategorie	Definition	Ihr Eintrag
Erlaubte Tools (Allowlist)	Welche KI-Tools dürfen genutzt werden?	
No-Go-Daten	Welche Daten dürfen nie in KI-Tools?	
Prompt-Regeln	Was muss beim Prompten beachtet werden?	
Freigabeprozess	Wer entscheidet über neue Tools / Use Cases?	

Verantwortliche Person	Wer ist Ansprechpartner für KI-Fragen?	

Tipp: Starten Sie mit 2–3 erlaubten Tools und einer klaren No-Go-Liste. Der Rest kann iterativ wachsen.

Schritt 5: Freigabe & Monitoring

Ziel: Einen einfachen Review-Rhythmus etablieren, damit die Bestandsaufnahme nicht einmalig bleibt.

Empfehlung: Review alle 2 Monate mit folgender Checkliste:

Aufgabe	Status / Datum
Inventar aktualisieren (neue Tools?)	
Datenklassifikation prüfen (neue Datentypen?)	
Risikobewertung der Top-10-Use-Cases aktualisieren	
Allowlist anpassen (neue Tools freigeben/sperren?)	
Prompt-Regeln aktualisieren	
Mitarbeitende informieren / kurzes Update	

Tipp: Definieren Sie den Freigabeprozess in einem Satz, z.B.: „Neue KI-Tools werden durch [Name/Rolle] nach Rücksprache mit IT und Datenschutz freigegeben.“

Nächste Schritte

- ☐ Woche 1: Schritt 1–2 durchführen (Inventar + Datenklassifikation)
- ☐ Woche 2: Schritt 3–4 durchführen (Risikobewertung + Leitplanken)
- ☐ Woche 2: Schritt 5 einrichten (Freigabe + ersten Review-Termin setzen)
- ☐ Ergebnisse mit GF / IT / Datenschutzbeauftragtem teilen

Unterstützung gewünscht?

Sie möchten die Bestandsaufnahme nicht allein durchgehen?

Ich biete einen kostenlosen 15-Minuten Reality-Check an: 3 Fragen, 1 Ampel-Einschätzung, klare nächste Schritte.

Einfach antworten auf diese Nachricht oder schreiben Sie mir:
martin@martin-mueller-ki.de

Viele Grüße
Martin Müller