

PRAKTISCHES WERKZEUG · VERANTWORTUNGSVOLLER KI-EINSATZ

Shadow-KI-Workshop

Eine Zeile = ein konkreter KI-Einsatz. · Keine vage Richtlinie. · Keine Grauzone.

Dieses Werkzeug macht die in einem KMU bereits vorhandenen oder geplanten KI-Einsätze sichtbar. Das Ziel ist einfach: Einsatz für Einsatz entscheiden, was erlaubt, unter Auflagen erlaubt oder verboten ist.

Anleitung

1

Reale Einsätze auflisten
Eine Zeile pro Einsatz. Formel: «Ich nutze [Tool + Konto] für [Aufgabe] mit [Daten]». Bsp.: ChatGPT (privates Konto), um eine Kunden-E-Mail umzuformulieren.

2

Daten einordnen
Den in der Zeile verwendeten Datentyp ankreuzen – siehe Legende der Typen unten.

3

Zweck der KI-Ausgabe angeben
Verwendung der Ausgabe angeben: Idee, internes Dokument, externe Nachricht, Empfehlung... – siehe Legende.

4

Entscheiden
Ja (erlaubt) · Ja unter Auflagen (wenn schriftliche Auflagen erfüllt) · Nein (verboten). Wenn das Team nicht entscheiden kann: «Vorerst Nein» + offene Frage.

Register der KI-Einsätze

DATENTYPEN

Öffentlich

Intern nicht sensibel

Kunden / Interessenten / Lieferanten

HR / Personen

Verträge / Finanzen

Geschäftsgeheimnisse

Sensibel

Zugänge / Sicherheit

AUSGABE VERWENDET FÜR

Idee

Internes Dokument

Externe Nachricht

Empfehlung

Sensible Entscheidung

Automatische Aktion

Registerverantwortliche/r

Nächste Überprüfung

KI-EINSATZ	TOOL + KONTO	VERWENDETE DATEN	KI-AUSGABE VERWENDET FÜR	ENTSCHEIDUNG (AUFLAGEN / VERANTWORTLICH)
Kunden-E-Mail umformulieren	ChatGPT (privates Konto)	Kunde / E-Mail	Externe Nachricht, geprüft	Ja unter Auflagen – Anonymisieren + vor Versand prüfen
Kundendatenbank importieren, um Segmente zu erstellen	Kostenloses Marketing-KI-Tool	Kunden / Interessenten	Kundensegmentierung	Nein – Kein Import der Kundendatenbank in ein nicht freigegebenes Tool
Ideen für LinkedIn-Posts vorbereiten	Notion AI	Öffentlich / nicht sensibel	Idee / Entwurf	Ja – Richtigkeit und Ton prüfen

QUELLEN

Silic, M., Silic, D., & Kind-Trüller, K. (2025). From Shadow IT to Shadow AI – Threats, Risks and Opportunities for Organizations. DOI: <https://doi.org/10.1002/jsc.2682>
NIST (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). DOI: <https://doi.org/10.6028/NIST.AI.100-1>