KOSTENLOSE RESSOURCE

CHECKS




# 08

# DATENSCHUTZ-CHECK FÜR DEIN KI-GEDÄCHTNIS

Du siehst, was ChatGPT oder Claude über dich und dein Business gespeichert hat, und räumst es auf.

CHECKS | 25 MINUTEN | EINSTEIGER

**LUCAS RIECKEN**

KI-Systeme für Unternehmer

@lucas_riecken

## FÜR WEN

Für alle, die ChatGPT, Claude oder einen anderen Assistenten seit Monaten nutzen und wissen wollen, welche Infos über sie und ihre Kunden dort hängen geblieben sind.

## DAS PROBLEM

KI-Assistenten merken sich Dinge, ohne dass du daran denkst. Alte Angaben, Details über Kunden oder falsche Vermutungen beeinflussen später die Antworten. Du siehst es nicht, solange du nicht nachschaust.

## DEIN ERGEBNIS

Du hast eine Liste von allem, was der Assistent über dich zu wissen glaubt. Jeder Punkt ist als behalten, korrigieren oder löschen markiert und in den Einstellungen umgesetzt. Dazu hast du eine einfache Regel, was du künftig gar nicht mehr in Chats schreibst.

### NUTZ DAS, WENN

- Du nutzt denselben Account seit mehreren Monaten.
- Du willst der KI mehr über dein Business geben und willst vorher aufräumen.
- Antworten klingen, als wüsste die KI Dinge, die du in diesem Chat gar nicht erwähnt hast.

### LASS ES, WENN

- Du willst einen rechtlich gültigen Nachweis, was der Anbieter über dich speichert. Dafür gibt es die offizielle Auskunftsanfrage beim Anbieter.
- Du teilst dir den Account mit jemandem und es ist unklar, wessen Daten dort liegen.
- Du erwartest, dass der Chat dir wirklich alles verrät. Er kennt nicht jeden Eintrag im Hintergrund.

### DAS BRAUCHST DU

- Zugang zu deinem KI-Account und den Einstellungen für Gedächtnis oder Personalisierung
- Eine leere Tabelle oder Notiz für deine Liste
- Eine Liste mit Themen, die nie gespeichert werden sollen, zum Beispiel Kundendaten oder Gesundheit
- Zwanzig ungestörte Minuten

SCHRITT FÜR SCHRITT

# SO GEHST DU VOR

## 01 LISTE ANLEGEN

Mach eine Tabelle mit den Spalten Eintrag, Art, Entscheidung und erledigt am. Schreib keine sensiblen Details hinein, nur Kategorien.

## 02 DEN ASSISTENTEN FRAGEN

Starte einen neuen Chat und füge den Prompt unten ein. Der Assistent zeigt dir, was er über dich nutzt, und trennt Gesagtes von Vermutetem.

## 03 JEDEN EINTRAG ENTSCHEIDEN

Geh Zeile für Zeile durch. Stimmt es noch? Ist es nötig? Ist es zu privat? Dann behalten, korrigieren oder löschen.

## 04 IN DEN EINSTELLUNGEN UMSETZEN

Öffne die Gedächtnis-Verwaltung des Tools und lösche oder ändere dort selbst. Der Chat allein löscht nichts zuverlässig.

## 05 GEGENPROBE MACHEN

Öffne einen frischen Chat, stell die Kontrollfrage aus dem Prompt und vergleich das Ergebnis mit deiner Liste. Speicher die Liste mit Datum.

ZUM KOPIEREN

# DER PROMPT ZUM KOPIEREN

VORLAGE_08.TXT

```
Ich möchte aufräumen, was du über mich weißt. Es geht um Kontrolle, nicht um Neugier.
Bitte antworte sachlich und ohne Ausschmückung.

TEIL 1: Was nutzt du gerade über mich?
Liste alles auf, was du verwendest, um deine Antworten auf mich zuzuschneiden. Teile es
in vier Gruppen:
a) Dinge, die ich dir ausdrücklich gesagt habe
b) Vorlieben, die ich dir genannt habe
c) Anweisungen, die ich dir gegeben habe
d) Sonstiges, was du über mich zu wissen glaubst
Schreib zu jedem Punkt dazu, ob es gespeichertes Gedächtnis ist, nur aus dem aktuellen
Chat stammt oder ob du dir nicht sicher bist. Fass nichts zusammen, jeder Punkt bekommt
eine eigene Zeile. Erfinde nichts Neues. Wenn du etwas nicht einsehen kannst, sag das
klar.

TEIL 2: Vermutungen
Nenne nur Schlüsse, die du schon vor dieser Nachricht über mich gezogen hast und die
deine Antworten beeinflussen. Gib zu jedem Schluss an, woraus er entstanden ist, und wie
sicher du dir bist (niedrig, mittel, hoch). Rate nicht zu Gesundheit, Einkommen,
Aufenthaltsstatus, Herkunft, Religion oder privaten Verhältnissen. Wenn es keine solchen
Schlüsse gibt, schreib "keine".

TEIL 3: Veraltetes und Heikles
Markiere aus Teil 1 und 2 alles, was veraltet sein könnte, was Kunden oder Dritte
betrifft oder was ich nicht länger gespeichert haben sollte. Begründe jeweils in einem
Satz.

TEIL 4: Meine Entscheidungen
Ich schreibe dir gleich pro Eintrag "behalten", "korrigieren: [NEUER WERT]" oder
"löschen". Sag mir dann Schritt für Schritt, wo ich das in meinen Einstellungen selbst
ändere. Behaupte nicht, dass du etwas gelöscht hast. Ich prüfe das selbst.

TEIL 5: Meine Regel für die Zukunft
Schlag mir auf Basis meiner Antworten eine kurze Regel mit fünf Punkten vor, was ich in
Chats künftig nicht mehr schreibe. Mein Business: [WAS DU ANBIETEST]. Meine sensiblen
Themen: [Z. B. KUNDENNAMEN, FINANZEN, GESUNDHEIT].

KONTROLLFRAGE für einen neuen Chat, nachdem ich aufgeräumt habe:
```

Was weißt du über mich, ohne dass ich es in diesem Chat gesagt habe? Nenne nur, was du tatsächlich gespeichert hast, und sag es, falls du nichts findest.



## MEIN TIPP

Ich war überrascht, wie viel sich über Monate ansammelt, was ich längst vergessen hatte. Seitdem schaue ich regelmäßig nach, statt einfach darauf zu vertrauen, dass schon alles passt.

### HIER PRÜFST DU SELBST

- Du vergleichst jeden gespeicherten Punkt mit dem, was wirklich stimmt. Vermutungen der KI behandelst du als unbewiesen.
- Du prüfst in der Gedächtnis-Verwaltung selbst, ob gelöschte Einträge wirklich weg sind.
- Du wiederholst die Gegenprobe in einem neuen Chat und hältst das Ergebnis fest.

### DATENSCHUTZ UND GRENZEN

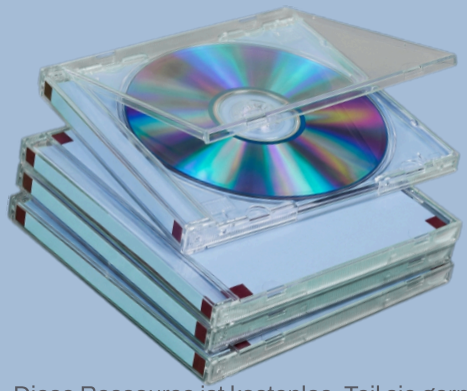
- Schreib keine Passwörter, Zugangsdaten, Zahlungsangaben, Kundenakten, Gesundheitsdaten oder Ausweisnummern in den Prüfchat.
- Bitte die KI nicht, neue Vermutungen über sensible Eigenschaften anzustellen.
- Ein Chat ist kein vollständiger Datenauszug. Wenn es ernst wird, nutzt du die offizielle Auskunfts- oder Löschanfrage des Anbieters.

KEINE ZEIT, DAS SELBST ZU BAUEN?

# WIR BAUEN DAS FÜR DICH.

Ich schaue mir dein Business an und zeige dir im kostenlosen Erstgespräch, wo KI dir am meisten Zeit spart.

**Kostenloses Erstgespräch buchen**



Diese Ressource ist kostenlos. Teil sie gern, aber bitte mit Hinweis auf Lucas Riecken.

