KOSTENLOSE RESSOURCE

CHECKS



03

WAS WEISS DEINE KI EIGENTLICH ÜBER DICH?

Eine Bestandsaufnahme, was dein KI-Assistent speichert und annimmt, mit einer klaren Liste, was bleibt und was gelöscht wird.

CHECKS | 25 MINUTEN | EINSTEIGER

LUCAS RIECKEN

KI-Systeme für Unternehmer

@lucas_riecken

FÜR WEN

Für alle, die ihren KI-Assistenten regelmäßig mit Kundenthemen, Zahlen oder Strategie füttern, vor allem Selbstständige mit Kundendaten und Teams, die ein Konto teilen.

DAS PROBLEM

Dein Assistent merkt sich Dinge und zieht eigene Schlüsse aus deinen Gesprächen. Das kann nützlich sein. Es kann aber auch Details weiterverwenden, die du längst nicht mehr dort haben willst. Aufgeschrieben hast du nirgends, was bleiben darf.

DEIN ERGEBNIS

Du hast eine Liste, was der Assistent von dir sieht, welche Annahmen er trifft, was du behältst, korrigierst oder löschst, und eine Kontrollliste für die Einstellungen. Zum Schluss prüfst du in einem frischen Chat nach.

NUTZ DAS, WENN

- Du nutzt dasselbe KI-Konto seit Monaten für Arbeit oder Planung.
- Mehrere Personen teilen sich ein Konto oder Projekt.
- Du willst bald Kunden-, Mitarbeiter- oder Finanzthemen in die KI geben.

LASS ES, WENN

- Du willst damit beweisen, was der Anbieter auf seinen Servern speichert. Das kann ein Chat nicht.
- Du willst ein Persönlichkeitsprofil über dich. Darum geht es hier nicht.
- Du kommst nicht an die Einstellungen deines Kontos heran.

DAS BRAUCHST DU

- Zugang zum KI-Konto, das du prüfen willst
- Eine Liste von Dingen, die nie gespeichert werden sollen
- Einen Blick auf deine aktuellen Einstellungen zu Gedächtnis und Datennutzung
- Falls geteilt: die Regeln für Team oder gemeinsame Projekte
- Einen sicheren Ort für deine Notizen zur Entscheidung

SCHRITT FÜR SCHRITT

SO GEHST DU VOR

01 DEINE NIE-SPEICHERN-LISTE SCHREIBEN

Notiere vorab die Kategorien, die nicht bleiben sollen, zum Beispiel Zugangsdaten, Kundenakten oder Gesundheit. Schreib nur die Kategorie auf, nie den echten Wert.

02 SICHTBARES GEDÄCHTNIS ABFRAGEN

Gib dem Assistenten die erste Abfrage. Er listet auf, was er zu dir nutzen kann, und bewertet, wie heikel es ist. Er soll nichts Neues erraten.

03 ANNAHMEN AUFDECKEN

Mit der zweiten Abfrage findest du heraus, was er aus deinen Gesprächen schon unterstellt, ohne dass du es gesagt hast. Gibt es keinen Beleg, soll er "unbelegt" schreiben.

04 ENTSCHEIDEN UND IN DEN EINSTELLUNGEN UMSETZEN

Entscheide pro Eintrag: behalten, korrigieren oder löschen. Setz das dann in den echten Einstellungen deines Tools um. Der Assistent sagt nur, was er sieht, und löscht nichts verlässlich selbst.

05 IM FRISCHEN CHAT NACHTESTEN

Öffne einen neuen Chat und frag nach, was noch gespeichert ist. Taucht Gelöschtes wieder auf, prüfe die Einstellungen noch mal und wende dich an den Support des Anbieters.

ZUM KOPIEREN

DIE PROMPTS FÜR DEN GEDÄCHTNIS-CHECK

VORLAGE_03.TXT

```
TEIL 1: DEINE NIE-SPEICHERN-LISTE

Hake ab, was bei dir nicht gespeichert bleiben soll. Schreib nur die Kategorie auf,
niemals den echten Inhalt:
[ ] Passwörter, Zugangscodes, Wiederherstellungsschlüssel
[ ] Kartendaten und Bankdaten
[ ] Ausweis- oder Steuernummern
[ ] Gesundheitsdaten
[ ] Infos über Mitarbeiter, etwa Leistung oder Abmahnungen
[ ] Kundendaten, die für die aktuelle Aufgabe nicht nötig sind
[ ] Verträge und Rechtsfragen
[ ] Daten von Kindern
[ ] Genauer Wohnort oder Reisepläne
[ ] Unveröffentlichte Zahlen, Preise, Vorhaben
[ ] [WEITERE KATEGORIE AUS DEINEN REGELN]

TEIL 2: ABFRAGE 1, WAS DU SICHTBAR SPEICHERST

Kopiere das in den Assistenten, den du prüfen willst:

"Ich prüfe gerade, was du über mich speicherst und nutzt. Liste nur auf, was du aus
gespeichertem Gedächtnis, Profil, Projekten oder diesem Gespräch jetzt tatsächlich
abrufen kannst.

Gib mir eine Tabelle mit diesen Spalten:
- Eintrag
- Quelle (Gedächtnis, Profil, Projekt, aktuelles Gespräch oder unbekannt)
- Habe ich das selbst gesagt, ja oder nein
- Wie beeinflusst es deine Antworten
- Wie heikel: niedrig, mittel oder hoch
- Brauche ich das noch: ja, nein oder unsicher
- Empfehlung: behalten, korrigieren, löschen oder in den Einstellungen prüfen

Rate nichts Neues. Schließe keine Dinge wie Alter, Gesundheit, Einkommen, Herkunft,
Religion, Politik, Familienstand oder Charakter. Wenn du einen Speicher nicht einsehen
kannst, sag das. Deine Antwort zeigt nur, was du sehen kannst, und ist kein Beweis
dafür, was der Anbieter speichert."

TEIL 3: ABFRAGE 2, WAS DER ASSISTENT ANNIMMT

"Schau dir dieses Gespräch und deine Tabelle an. Welche Annahmen über mich oder mein
Geschäft nutzt du schon, die ich nicht als Tatsache genannt habe?

Pro Annahme: der Satz oder das Verhalten, woraus du sie abgeleitet hast, wie sicher du
dir bist, wie sie deine Antwort verändert, ob du sie brauchst und was stattdessen eine
bessere Rückfrage an mich wäre. Wenn es keinen Beleg gibt, schreib 'unbelegt'. Stelle
keine neuen Vermutungen an und analysiere nicht meine Person."
```

TEIL 4: DEINE ENTSCHEIDUNGSTABELLE

Lege sie selbst an, mit diesen Spalten:
Eintrag | Behalten | Korrigieren | Löschen | Warum | Genutzte Einstellung | Datum

Regeln:
- Behalte nur, was dir wiederholte Arbeit spart und wenig Risiko birgt.
- Korrigiere Veraltetes oder zu Grobes.
- Lösche Heikles, das du nicht brauchst, und Vermutungen, die als Tatsache behandelt werden.
- Prüfe alles Unbekannte in den echten Einstellungen.
- Bei geteilten Projekten: Wer sieht mit?

TEIL 5: EINSTELLUNGEN ABHAKEN

[ ] Gedächtnis angesehen
[ ] Unerwünschtes gelöscht
[ ] Falsches korrigiert
[ ] Personalisierung bewusst gewählt
[ ] Datennutzung zum Training bewusst gewählt
[ ] Verbundene Apps geprüft
[ ] Geteilte Projekte geprüft
[ ] Alte Chats und Dateien nach deinen Regeln behandelt
[ ] Weg für Auskunfts- und Löschwunsch gespeichert

TEIL 6: NACHTEST IM NEUEN CHAT

"Ohne mich nach neuen persönlichen Angaben zu fragen: Welche gespeicherten Fakten oder Profildaten kannst du jetzt nutzen? Trenne Gespeichertes von dem, was nur in diesem Chat steht. Wenn du das Gedächtnis nicht einsehen kannst, sag es."

Dann für eine gelöschte Kategorie: "Hast du gespeicherte Angaben zur Kategorie [KATEGORIE]? Antworte nur mit ja, nein oder kann ich nicht prüfen. Rate keinen Inhalt."

Wiederhole den Check alle drei Monate und immer dann, wenn jemand dein Team verlässt oder du eine neue App verbindest.



MEIN TIPP

Ich mache diesen Check, bevor ich mit einem neuen Kunden im selben Konto arbeite. Ehrlich gesagt hat mich das Aufräumen mehr gebracht als jede neue Funktion, weil ich dem Assistenten danach wieder bewusst sage, was er wissen darf.

HIER PRÜFST DU SELBST

- Jede Löschung und Korrektur erledigst du selbst in den Einstellungen und kontrollierst sie.
- Du liest nach, was der Anbieter zu Speicherung und Training schreibt.
- Bei Kundendaten, Mitarbeiterdaten oder Rechtsfragen fragst du eine Fachperson, etwa deine Datenschutzberatung.

DATENSCHUTZ UND GRENZEN

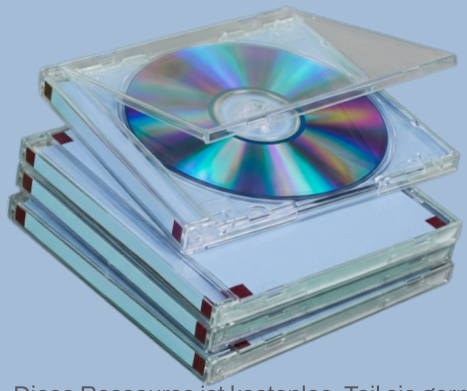
- Gib keine zusätzlichen heiklen Daten ein, nur um zu testen, ob sie gemerkt werden.
- Lass die KI nichts über sensible Eigenschaften von dir oder anderen vermuten.
- Die Antwort des Assistenten ist kein Beweis für das, was der Anbieter wirklich speichert oder gelöscht hat.

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.

