
KOSTENLOS VON WECANDO.AI

Die KI-Blacklist: 23 Dinge, die du ChatGPT NIEMALS sagen solltest

Herausgeber: wecando.ai • Stand: April 2026 • Version: 1.0

wecando.ai – Die KI-Plattform für Macher
Stand: April 2026 | Version 1.0

Die KI-Blacklist: 23 Dinge, die du ChatGPT NIEMALS sagen solltest

Herausgeber: wecando.ai | Stand: April 2026 | Version: 1.0

Diese Liste gilt nicht nur für ChatGPT, sondern für alle KI-Chatbots: Claude, Gemini, Copilot, Perplexity und Co. Die Fehler sind überall die gleichen. Die Konsequenzen auch.

Kategorie 1: Datenschutz-Fallen

Diese fünf Fehler können dich Geld, Job oder Kunden kosten. Kein Witz. Die DSGVO kennt Bußgelder bis 20 Millionen Euro oder 4% des Jahresumsatzes — je nachdem, was höher ist.

1. Kundendaten in den Prompt kopieren

Was du NICHT tun solltest:

✗ NICHT SO

```
"Analysiere diese Kundenliste und finde Muster: Max Müller, Tel 0172-9876543, max.mueller@firma.de, Umsatz 12.400€; Lisa Weber, Tel 0151-1234567..."
```

Warum das ein Problem ist:

Du überträgst personenbezogene Daten an einen US-Anbieter — ohne Rechtsgrundlage, ohne AVV, ohne Einwilligung der Betroffenen. Bei der kostenlosen ChatGPT-Version können diese Daten sogar im Modelltraining landen. Das ist kein theoretisches Risiko: Italienische und deutsche Datenschutzbehörden haben bereits Verfahren gegen KI-Anbieter eingeleitet.

Was du STATTDENnoch tun solltest:

✓ BESSER SO

```
"Ich habe eine Kundenliste mit 500 Einträgen. Die Spalten sind: anonyme ID, Branche, Umsatzklasse (A/B/C), Region (PLZ-Bereich). Welche Segmentierungsstrategien kannst du mir empfehlen? Hier sind 10 anonymisierte Beispielzeilen: ID-001, IT-Dienstleister, Klasse A, PLZ 7..."
```

Pseudonymisiere oder anonymisiere deine Daten **bevor** sie in den Prompt gehen. Keine Namen, keine Telefonnummern, keine E-Mail-Adressen.

2. Personalakten oder Bewerbungen einfügen

Was du NICHT tun solltest:

X NICHT SO

```
"Bewerte diesen Lebenslauf: Lisa Schmidt, geb. 15.03.1988, wohnhaft Hauptstraße 12, 70173 Stuttgart. Ausbildung: ..."
```

Warum das ein Problem ist:

Art. 22 DSGVO verbietet automatisierte Einzelentscheidungen, die rechtliche Wirkung entfalten — und eine Bewerbungsabsage ist genau das. Zusätzlich verarbeitest du besonders sensible Daten (Geburtsdatum, Adresse, ggf. Gesundheitsangaben) ohne Rechtsgrundlage. Falls der Bewerber je erfährt, dass seine Unterlagen durch ChatGPT gelaufen sind, hast du ein Problem, das kein Rechtsanwalt gerne sieht.

Was du STATTDESSEN tun solltest:

✓ BESSER SO

```
"Ich suche einen Senior-Entwickler mit Python-Erfahrung und Teamleitungskompetenz. Erstelle mir eine Bewertungsmatrix mit 10 Kriterien, die ich auf Lebensläufe anwenden kann. Gewichte die Kriterien nach Relevanz für ein 20-Personen-Startup."
```

Lass die KI die **Methode** bauen — nicht die **Entscheidung** treffen.

3. Interne Finanzdaten teilen

Was du NICHT tun solltest:

X NICHT SO

```
"Optimiere diesen Quartalsbericht: Unser Umsatz Q1 war 2,3 Mio €, EBITDA 340K, Personalkosten 1,1 Mio. Kunde Telekom macht 40% aus, Vertragsverlängerung unsicher..."
```

Warum das ein Problem ist:

Geschäftsgeheimnisse verlieren ihren Schutz nach dem GeschGehG, wenn du keine angemessenen Geheimhaltungsmaßnahmen triffst. Das Einfügen in ein KI-Tool ohne Enterprise-Vertrag kann als Verlust der Schutzwürdigkeit gewertet werden. Für börsennotierte Unternehmen kommt Insiderhandels-Problematik dazu. Für alle anderen: Dein Wettbewerber sagt danke.

Was du STATTDESSEN tun solltest:

✓ BESSER SO

"Ein SaaS-Unternehmen mit 30 Mitarbeitern hat folgende Kennzahlen: Umsatz X, EBITDA-Marge 15%, Personalkosten 48% vom Umsatz, Klumpenrisiko bei einem Kunden (40%). Welche Hebel gibt es, um die Profitabilität in Q2 zu steigern?"

Verändere die Zahlen oder nutze Prozentwerte und Verhältnisse. Die KI braucht keine echten Beträge, um dir gute Strategien zu liefern.

4. Passwörter oder API-Keys eingeben

Was du NICHT tun solltest:

✗ NICHT SO

```
"Mein Script funktioniert nicht. Hier ist der Code: import openai; openai.api_key = 'sk-proj-4f7g8h9j2k3l5m6n7p8q..' – Was ist falsch?"
```

Warum das ein Problem ist:

Dein API-Key ist jetzt potenziell Teil der Trainingsdaten. Automatisierte Scraper durchsuchen geleakte Credentials systematisch. Ein offener OpenAI-Key kann innerhalb von Stunden Kosten im vierstelligen Bereich verursachen. Das gilt genauso für AWS-Keys, Datenbank-Passwörter, SSH-Keys und Tokens jeder Art.

Was du STATTDENEN tun solltest:

✓ BESSER SO

```
"Mein Python-Script wirft einen AuthenticationError bei der OpenAI API. Der Key ist als Umgebungsvariable gesetzt: os.environ.get('OPENAI_API_KEY'). Der Fehler tritt nur in der Produktionsumgebung auf, lokal funktioniert es. Was könnte die Ursache sein?"
```

Beschreibe das Problem. Zeig die Fehlermeldung. Zeig die Code-Struktur. Aber **niemals** den Schlüssel selbst.

5. Patientendaten oder Gesundheitsinfos

Was du NICHT tun solltest:

X NICHT SO

"Ich habe einen Patienten, männlich, 52, Diabetiker Typ 2, BMI 34, aktuelle Medikation: Metformin 1000mg, Ramipril 5mg. Letzte Blutwerte: HbA1c 8,2%, Kreatinin 1,4. Was empfehlst du?"

Warum das ein Problem ist:

Gesundheitsdaten gehören zu den "besonderen Kategorien personenbezogener Daten" nach Art. 9 DSGVO. Ihre Verarbeitung ist grundsätzlich **verboten** — mit eng definierten Ausnahmen, zu denen "mal schnell ChatGPT fragen" definitiv nicht gehört. Für Ärzte kommen berufsrechtliche Schweigepflicht und strafrechtliche Konsequenzen (§ 203 StGB) dazu.

Was du STATTDESSEN tun solltest:**✓ BESSER SO**

"Welche aktuellen Leitlinien gibt es für die Behandlung von Diabetes Typ 2 bei Patienten mit eingeschränkter Nierenfunktion? Konkret: Welche Alternativen zu Metformin werden bei einer GFR unter 45 empfohlen? Bitte mit Quellenangaben."

Frag nach **Wissen**, nicht nach **Diagnosen**. Und prüfe jede medizinische Antwort gegen aktuelle Leitlinien — KI-Modelle haben einen Wissensstand, der Monate hinter der aktuellen Forschung liegt.

Kategorie 2: Halluzinations-Trigger

KI-Modelle halluzinieren. Das bedeutet: Sie erfinden Fakten, Zahlen, Quellen und Paragraphen — mit der gleichen Überzeugung, mit der sie korrekte Informationen liefern. Diese fünf Prompts triggern das besonders zuverlässig.

6. Nach aktuellen Fakten fragen (ohne Quellen-Check)

Was du NICHT tun solltest:**X NICHT SO**

"Was war der DAX-Stand gestern bei Börsenschluss? Und wie hat sich der Bitcoin-Kurs diese Woche entwickelt?"

Warum das ein Problem ist:

Die KI wird dir eine Zahl nennen. Mit Dezimalstellen. Voller Überzeugung. Und sie wird falsch sein. Sprachmodelle sind keine Datenbanken — sie haben keinen Echtzeit-Zugriff auf Börsendaten,

Wetterbericht oder Sportergebnisse (es sei denn, sie nutzen explizit eine Suchfunktion). Das Heimtückische: Die Antwort klingt perfekt plausibel.

Was du **STATTDESEN** tun solltest:

✓ **BESSER SO**

"Erkläre mir, welche Faktoren den DAX typischerweise beeinflussen. Welche makroökonomischen Indikatoren sollte ich für eine Wochenanalyse des deutschen Aktienmarkts beobachten?"

Für aktuelle Daten: Nutze die offizielle Quelle direkt. Für Kontext und Einordnung: Da ist die KI stark. Diese Trennung rettet dich vor peinlichen Fehlern.

7. Rechtsberatung verlangen

Was du **NICHT** tun solltest:

✗ **NICHT SO**

"Mein Vermieter will die Miete um 15% erhöhen. Darf er das? Was sagt das BGB? Soll ich Widerspruch einlegen?"

Warum das ein Problem ist:

Die KI wird Paragraphen zitieren — manchmal existieren sie, manchmal nicht. Sie wird Fristen nennen — manchmal stimmen sie, manchmal verwechselt sie Bundes- und Landesrecht. Sie wird dir eine Einschätzung geben, die sich anhört wie von einem Anwalt — aber keiner haftet dafür. Ein falscher Rat zur Mieterhöhung kann dich deine Wohnung kosten.

Was du **STATTDESEN** tun solltest:

✓ **BESSER SO**

"Erkläre mir die Grundlagen des Mieterhöhungsrechts in Deutschland. Welche Formen der Mieterhöhung gibt es, welche Fristen gelten grundsätzlich, und welche Mieterrechte existieren? Ich nutze das als Vorbereitung für ein Gespräch mit meinem Mieterverein."

Nutze die KI als Briefing-Tool, nicht als Rechtsberater. Und geh danach zum Profi.

8. Medizinische Diagnosen stellen lassen

Was du **NICHT** tun solltest:

X NICHT SO

"Ich habe seit drei Tagen Kopfschmerzen links, Schwindel beim Aufstehen und mein linkes Auge zuckt. Was habe ich?"

Warum das ein Problem ist:

Die KI wird differentialdiagnostisch antworten und dabei klingen wie ein Chefarzt in der Visite. Nur: Sie kann dich nicht untersuchen, hat keine Bildung, kein Labor, keine Anamnese. In einem Fall sagt sie "Spannungskopfschmerz, trink mehr Wasser", im anderen übersieht sie einen Schlaganfall. Beides ist gleich wahrscheinlich. Beides ist gleich gefährlich.

Was du STATTDENNEN tun solltest:

✓ BESSER SO

"Ich gehe morgen zum Arzt wegen anhaltender Kopfschmerzen mit Schwindel. Welche Fragen sollte ich dem Arzt stellen? Welche Untersuchungen sind bei dieser Symptomkombination üblich? Worauf sollte ich achten?"

Lass die KI dir helfen, das **Gespräch mit dem Arzt** vorzubereiten — nicht den Arzt zu ersetzen.

9. Wissenschaftliche Quellen zitieren lassen

Was du NICHT tun solltest:

X NICHT SO

"Nenne mir 5 peer-reviewte Studien, die belegen, dass Remote Work die Produktivität steigert. Mit Autoren, Journal, Jahrgang und DOI."

Warum das ein Problem ist:

Das ist der Halluzinations-Klassiker. Die KI erfindet Autorennamen, Journaltitel, Jahrgänge und DOIs, die täuschend echt aussehen. "Smith et al. (2023), Journal of Organizational Psychology, DOI: 10.1037/ocp0000..." — klingt perfekt, existiert aber nicht. Wer das in eine Hausarbeit, Bachelorarbeit oder Unternehmenspräsentation übernimmt, fliegt auf.

Was du STATTDENNEN tun solltest:

✓ BESSER SO

"Welche Argumente und Gegenargumente gibt es in der Forschung zum Thema Remote Work und Produktivität? Welche Forschungsrichtungen und bekannten Forscher sollte ich in Google Scholar oder PubMed suchen?"

Lass dir Suchbegriffe und Forschungsrichtungen geben — und suche die echten Quellen dann selbst in Fachdatenbanken.

10. Nach Personen-Details fragen

Was du NICHT tun solltest:

X NICHT SO

"Was ist die E-Mail-Adresse von Tim Cook? Und wie erreiche ich die Pressestelle von Apple direkt?"

Warum das ein Problem ist:

Die KI wird entweder eine plausibel klingende, aber falsche Adresse generieren — oder tatsächlich existierende Kontaktdaten zusammenwürfeln, die veraltet oder falsch zugeordnet sind. Im besten Fall schreibst du ins Leere. Im schlimmsten Fall kontaktierst du die falsche Person mit vertraulichen Inhalten.

Was du STATTDENEN tun solltest:

✓ BESSER SO

"Wie ist die offizielle Kontaktstruktur bei Apple für Presseanfragen? Über welche Kanäle nimmt Apple typischerweise Anfragen von Geschäftspartnern entgegen?"

Für echte Kontaktdaten: Offizielle Website, LinkedIn, Impressum. Die KI kann dir zeigen, **wo** du suchen sollst — aber nicht die Daten selbst liefern.

Kategorie 3: Kompetenz-Grenzen

KI ist kein Universalgenie. In diesen fünf Bereichen überschätzen die meisten Nutzer die Fähigkeiten dramatisch — und treffen dann Entscheidungen auf Basis von selbstbewusstem Unsinn.

11. Komplexe Mathematik blind vertrauen

Was du NICHT tun solltest:

X NICHT SO

"Berechne den internen Zinsfuß für folgende Cashflows: -500.000, +120.000, +150.000, +180.000, +200.000, +250.000. Und mach gleich die Sensitivitätsanalyse dazu."

Warum das ein Problem ist:

Sprachmodelle sind keine Taschenrechner. Sie "berechnen" nicht — sie prognostizieren das wahrscheinlichste nächste Token. Bei einfacher Arithmetik funktioniert das oft, bei komplexen Berechnungen nicht zuverlässig. Ein falscher IRR kann eine Investitionsentscheidung im sechsstelligen Bereich kippen.

Was du STATTDENNEN tun solltest:**✓ BESSER SO**

"Erstelle mir eine Excel-Formel für den internen Zinsfuß (IKV/IRR). Die Cashflows stehen in B2:B7 mit Initialinvestition in B1. Erkläre mir außerdem, wie ich eine Sensitivitätsanalyse mit Datentabellen in Excel aufbaue."

Lass die KI dir das **Werkzeug** bauen, nicht die Rechnung machen. Excel, Python, R — dort gehören Berechnungen hin.

12. Steuererklärung machen lassen

Was du NICHT tun solltest:**X NICHT SO**

"Ich habe 2025 eine vermietete Wohnung in Stuttgart, Mieteinnahmen 14.400€, Zinsen 8.200€, AfA 2%. Füll mir die Anlage V aus."

Warum das ein Problem ist:

Die KI kennt die groben Regeln — aber nicht die aktuellen BMF-Schreiben, nicht die neueste BFH-Rechtsprechung, nicht die Besonderheiten deines Finanzamts. Ein falscher Werbungskosten-Ansatz ist kein Kavaliersdelikt. Das Finanzamt nennt das "leichtfertige Steuerverkürzung" — und die ist strafbar.

Was du STATTDENNEN tun solltest:**✓ BESSER SO**

"Ich vermiete eine Wohnung und mache meine Steuererklärung selbst. Welche Werbungskosten kann ich bei einer vermieteten Eigentumswohnung grundsätzlich absetzen? Welche Belege brauche ich? Was sind typische Fehler bei der Anlage V?"

Nutze die KI als Checkliste und Lernhilfe. Die Steuererklärung selbst gehört in ELSTER, WISO oder zum Steuerberater.

13. Verträge ohne Anwalt erstellen

Was du NICHT tun solltest:

X NICHT SO

"Schreib mir einen Kaufvertrag für eine Eigentumswohnung in München, Kaufpreis 450.000€, Übergabe 01.07.2026."

Warum das ein Problem ist:

Ein KI-generierter Kaufvertrag wird professionell aussehen. Er wird Paragraphen haben, Klauseln, Unterschriftenzeilen. Und er wird lückenhaft sein. Fehlende Gewährleistungsregelungen, unklare Haftungsklauseln, vergessene Rücktrittsrechte — all das merkst du erst, wenn es zu spät ist. Bei Immobilien ist der Vertrag ohnehin notarpflichtig. Bei allem anderen: Ein Anwalt kostet 300 Euro. Ein fehlerhafter Vertrag kostet 30.000.

Was du STATTDESSEN tun solltest:

✓ BESSER SO

"Ich kaufe eine Eigentumswohnung. Welche Klauseln muss ein Kaufvertrag enthalten? Worauf sollte ich besonders achten? Welche Punkte sollte ich mit meinem Notar besprechen?"

Lass dir eine **Checkliste** erstellen, nicht den Vertrag. Und nimm die Checkliste mit zum Notar.

14. Investmentberatung holen

Was du NICHT tun solltest:

X NICHT SO

"Soll ich jetzt Bitcoin kaufen oder lieber in ETFs investieren? Ich habe 50.000€ und will in 10 Jahren eine Wohnung kaufen."

Warum das ein Problem ist:

Die KI hat keine Lizenz als Finanzberater, haftet für nichts und kennt weder deine steuerliche Situation noch deine Risikotoleranz noch deine Gesamtvermögenslage. Sie wird trotzdem antworten — mit Sätzen wie "historisch gesehen haben ETFs..." Die gleiche KI hätte 2021 wahrscheinlich den Kauf von Luna-Token empfohlen. Weil die Trainingsdaten zu dem Zeitpunkt

bullish waren.

Was du STATTDESSEN tun solltest:

✓ BESSER SO

"Erkläre mir die Unterschiede zwischen Bitcoin und breit gestreuten ETFs als Anlageklassen. Welche Faktoren (Volatilität, Besteuerung, Liquidität, historische Renditen) sollte ich bei einem 10-Jahres-Anlagehorizont berücksichtigen? Welche Fragen sollte ich meinem Finanzberater stellen?"

Lass die KI dir **Wissen** liefern, damit du die richtigen Fragen stellen kannst. Die Entscheidung trifftst du selbst — oder mit einem zugelassenen Berater.

15. Code ohne Review deployen

Was du NICHT tun solltest:

✗ NICHT SO

"Generiere mir die komplette Backend-API für einen Online-Shop: User-Authentifizierung, Zahlungsabwicklung, Warenkorblogik, Datenbankschema. In Python mit FastAPI. Ich deploy das direkt auf meinen Server."

Warum das ein Problem ist:

KI-generierter Code funktioniert oft — und ist trotzdem unsicher. Typische Probleme: SQL Injection, fehlende Input-Validierung, hartcodierte Secrets, unsichere Kryptografie, fehlende Rate Limits. Besonders bei sicherheitskritischem Code (Auth, Payment, User-Daten) ist "funktioniert" nicht genug. Es muss **sicher** funktionieren.

Was du STATTDESSEN tun solltest:

✓ BESSER SO

"Ich baue eine FastAPI-Backend-API für einen Online-Shop. Generiere mir die User-Authentifizierung mit JWT. Markiere jeden Punkt, an dem Security-Maßnahmen nötig sind, mit einem TODO-Kommentar. Welche OWASP Top 10 Risiken sind für diese Architektur relevant?"

Lass die KI Code generieren — aber mit eingebauten Warnhinweisen. Und mach ein Code Review, bevor irgendwas live geht. Immer.

Kategorie 4: Prompt-Fehler

Kein Datenschutz-Problem, kein Halluzinations-Risiko — aber trotzdem Geld und Zeit verschwendet. Diese vier Fehler sind der Unterschied zwischen "KI bringt mir nichts" und "KI spart mir 10 Stunden pro Woche."

16. Zu vage prompten

Was du NICHT tun solltest:

x NICHT SO

"Mach mir was Schönes zum Thema Marketing."

Warum das ein Problem ist:

Vager Input = generischer Output. Die KI wird dir einen 08/15-Text liefern, der überall und nirgends passt. Du bekommst den kleinsten gemeinsamen Nenner aus Millionen von Marketing-Texten im Internet. Das ist, als würdest du im Restaurant bestellen: "Bringen Sie mir was zu essen."

Was du STATTDESSEN tun solltest:

✓ BESSER SO

"Schreibe einen LinkedIn-Post (max. 200 Wörter) für ein B2B-SaaS-Startup im HR-Bereich. Zielgruppe: Personalleiter in Unternehmen mit 200-500 Mitarbeitern. Thema: Warum manuelle Onboarding-Prozesse Geld kosten. Ton: professionell aber nicht steif. Endet mit einer Frage an die Leser."

Je spezifischer dein Prompt, desto besser das Ergebnis. Definiere: Format, Zielgruppe, Thema, Tonalität, Länge, Ziel.

17. Alles in einen einzigen Prompt packen

Was du NICHT tun solltest:

x NICHT SO

"Schreib mir einen 2.000-Wörter-Blogartikel, erstelle daraus 5 LinkedIn-Posts, 3 Instagram-Captions, einen Newsletter-Text, optimiere alles für SEO und mach mir noch einen Content-Kalender für den nächsten Monat."

Warum das ein Problem ist:

Die Qualität sinkt mit jeder zusätzlichen Aufgabe im selben Prompt. Sprachmodelle haben ein begrenztes Aufmerksamkeitsbudget. Wenn du sechs Aufgaben gleichzeitig stellst, bekommt keine davon die volle Qualität. Der Blogartikel wird oberflächlich, die Social Posts generisch, der

Newsletter lieblos.

Was du STATTDESSEN tun solltest:

✓ BESSER SO

Prompt 1: "Schreib mir einen 2.000-Wörter-Blogartikel zum Thema X. [Detaillierter Brief]"
Prompt 2: "Hier ist mein Blogartikel [einfügen]. Erstelle daraus 5 LinkedIn-Posts. Jeder Post soll einen anderen Aspekt hervorheben."
Prompt 3: "Basierend auf diesem Artikel: Erstelle einen Newsletter-Teaser (max. 100 Wörter) mit einer starken Betreffzeile."

Ein Prompt = eine Aufgabe. Ergebnisse aus Prompt 1 werden Input für Prompt 2. So baust du eine Qualitätskette statt einen Kompromiss-Stapel.

18. Keine Rolle zuweisen

Was du NICHT tun solltest:

✗ NICHT SO

"Schreib mir eine E-Mail an einen potenziellen Kunden."

Warum das ein Problem ist:

Ohne Rollenzuweisung antwortet die KI als generischer Assistent. Mit Rolle aktiviert sie spezialisiertes Wissen und einen passenden Tonfall. Der Unterschied ist messbar: Rolle = spezifischerer Wortschatz, bessere Struktur, relevantere Inhalte. Es ist der einfachste Hebel für bessere Ergebnisse — und die meisten Nutzer lassen ihn liegen.

Was du STATTDESSEN tun solltest:

✓ BESSER SO

"Du bist ein erfahrener B2B-Sales-Texter mit 15 Jahren Erfahrung in der SaaS-Branche. Schreibe eine kalte Akquise-E-Mail an den CTO eines mittelständischen Logistikunternehmens. Produkt: Predictive-Maintenance-Software. Ziel: Termin für eine 15-minütige Demo. Ton: direkt, kein Geschwafel, Mehrwert in der ersten Zeile."

Eine Rolle, eine Zielgruppe, ein Ziel, ein Ton. Vier Angaben, die den Output verdoppeln.

19. Keine Constraints setzen

Was du NICHT tun solltest:

X NICHT SO

"Erkläre mir Künstliche Intelligenz."

Warum das ein Problem ist:

Du bekommst eine 1.500-Wörter-Vorlesung, die bei Alan Turing anfängt und bei AGI aufhört. Vielleicht wolltest du drei Sätze für einen Elevator Pitch. Vielleicht eine technische Erklärung für Entwickler. Vielleicht eine kinderfreundliche Version für eine Schulpräsentation. Ohne Constraints rät die KI — und rät meistens falsch.

Was du STATTDESSEN tun solltest:

✓ BESSER SO

"Erkläre Künstliche Intelligenz in exakt 3 Sätzen. Zielgruppe: Ein Geschäftsführer, der wissen will, ob KI für sein Unternehmen relevant ist. Kein Fachjargon. Fokus auf den geschäftlichen Nutzen, nicht auf die Technologie."

Definiere: Länge, Zielgruppe, Detailtiefe, Fokus. Was du weglässt, ist genauso wichtig wie was du einschließt.

Kategorie 5: Workflow-Fallen

Du nutzt KI schon regelmäßig? Gut. Dann sind das die Fehler, die dich trotzdem ausbremsen — nicht weil du die KI falsch bedienst, sondern weil du den Workflow falsch aufgebaut hast.

20. Die erste Antwort akzeptieren

Was du NICHT tun solltest:

X NICHT SO

Die KI liefert einen Text. Du liest ihn. "Passt schon." Copy. Paste. Fertig.

Warum das ein Problem ist:

Die erste Antwort ist der Rohdiamant, nicht der geschliffene Ring. KI-Output ist immer ein Startpunkt. Wer die erste Version nimmt, bekommt durchschnittliche Qualität. Das Potenzial liegt in der Iteration: Feedback geben, nachschärfen, Richtung korrigieren. Drei Runden Iteration schlagen einen perfekten Prompt — jedes Mal.

Was du STATTDENSEN tun solltest:

✓ BESSER SO

Runde 1: "Schreib mir einen Blogartikel zu Thema X." Runde 2: "Guter Ansatz. Mach die Einleitung provokanter. Der dritte Abschnitt ist zu generisch – füge ein konkretes Zahlenbeispiel ein." Runde 3: "Fast perfekt. Kürze den Schluss um 50%. Ersetze das letzte Beispiel durch eines aus dem B2B-Bereich."

Iterieren ist keine Schwäche — es ist die Methode. Profis iterieren. Anfänger akzeptieren.

21. KI als Ersatz statt als Werkzeug behandeln

Was du NICHT tun solltest:

✗ NICHT SO

"Schreib meine komplette Bachelorarbeit zum Thema X. 60 Seiten, mit Quellenverzeichnis, Methodik und Ergebnissen."

Warum das ein Problem ist:

Erstens: Plagiatserkennung wird besser, nicht schlechter. Tools wie Turnitin erkennen KI-generierte Texte zunehmend zuverlässig. Zweitens: Eine Bachelorarbeit ohne eigene Stimme, ohne eigenes Denken, ohne echte Auseinandersetzung ist wertlos — auch wenn sie eine 1,7 bekommt. Drittens: Du lernst nichts. Und das war eigentlich der Punkt.

Was du STATTDENSEN tun solltest:

✓ BESSER SO

"Ich schreibe meine Bachelorarbeit zum Thema X. Ich habe folgende These: [These]. Hilf mir, meine Gliederung zu prüfen. Wo sind logische Lücken? Welche Gegenargumente muss ich berücksichtigen? Welche Methodik passt zu meiner Fragestellung?"

KI als Sparringspartner, nicht als Ghostwriter. Du schreibst. Die KI denkt mit.

22. Den Chat-Verlauf als Wahrheit behandeln

Was du NICHT tun solltest:

X NICHT SO

"Du hast mir vorhin gesagt, dass die Kündigungsfrist 4 Wochen beträgt. Stimmt das auch für Verträge, die vor 2020 geschlossen wurden?"

Warum das ein Problem ist:

KI-Chatbots haben kein verlässliches Gedächtnis. Was die KI drei Prompts vorher "gesagt" hat, ist nicht in Stein gemeißelt. In langen Chats geht Kontext verloren. In neuen Chats ist der alte Kontext komplett weg. Und: Die vorherige Antwort war vielleicht schon falsch. Darauf aufzubauen macht den Fehler nicht richtiger — nur tiefer.

Was du STATTDENNEN tun solltest:

✓ BESSER SO

"Ich möchte die Kündigungsfrist eines Dienstvertrags klären, der 2018 geschlossen wurde. Welche allgemeinen Regelungen gelten nach BGB für Dienstverträge? Gibt es Unterschiede je nach Vertragsdatum?"

Behandle jeden Prompt wie den ersten. Gib den relevanten Kontext mit. Baue nicht auf vorherige KI-Antworten als Faktenbasis.

23. Ohne Faktencheck veröffentlichen

Was du NICHT tun solltest:

X NICHT SO

KI generiert Blogartikel. Du liest drüber. "Klingt gut." Veröffentlichen.

Warum das ein Problem ist:

Dein Name steht drunter. Nicht "ChatGPT" — deiner. Wenn der Artikel eine falsche Statistik enthält, ein erfundenes Zitat oder eine sachlich falsche Behauptung, haftest du. Deine Glaubwürdigkeit. Deine Marke. Deine Reputation. Ein einziger faktisch falscher Artikel kann das Vertrauen zerstören, das du in einem Jahr Contentarbeit aufgebaut hast.

Was du STATTDENNEN tun solltest:

✓ BESSER SO

"Markiere in diesem Text alle Faktenbehauptungen, Statistiken und Zitate. Liste sie separat auf, damit ich sie einzeln gegen Originalquellen prüfen kann."

Lass die KI dir beim Faktencheck **helfen** — indem sie dir zeigt, was geprüft werden muss. Die eigentliche Prüfung machst du selbst. Jedes Mal. Ohne Ausnahme.

Fazit: KI ist ein Werkzeug — kein Orakel

Diese 23 Punkte lassen sich auf drei Grundregeln eindampfen:

- 1. Keine sensiblen Daten eingeben.** Nie. Egal wie bequem es wäre. Pseudonymisieren, anonymisieren, abstrahieren.
- 2. Nichts ungeprüft übernehmen.** Keine Zahl, kein Paragraph, keine Quelle, kein Medikament. Die KI klingt immer überzeugend — auch wenn sie falsch liegt.
- 3. KI verstärkt dich — sie ersetzt dich nicht.** Sie ist der beste Sparringspartner, den du je hattest. Aber du bleibst der Entscheider, der Prüfer, der Verantwortliche.

Wer diese drei Regeln verinnerlicht, wird mit KI mehr schaffen als 90% der Leute, die "Mach mir was Schönes" eintippen und hoffen, dass es schon passt.

Mehr KI-Praxiswissen?

Auf wecando.ai findest du:

- Tagesaktuelle KI-News und Tool-Reviews
- DSGVO-konforme KI-Strategien für Unternehmen
- Praxis-Guides für ChatGPT, Claude, Gemini und Co.
- Den kostenlosen **KI-ROI-Rechner** — finde in 2 Minuten heraus, wo KI dir am meisten Zeit spart

Erstellt von wecando.ai — Die KI-Plattform fuer Macher. Stand: April 2026. Datenschutz-Hinweise in diesem Dokument sind allgemeiner Natur und ersetzen keine Rechtsberatung.

Naechste Schritte

1 Lies die Liste und markiere die 3 Fehler die DU am haeufigsten machst

2 Wende die 'Richtig'-Alternative beim naechsten Prompt sofort an

Mehr kostenlose Ressourcen

Alle Lead Magnets sind kostenlos. Keine Anmeldung noetig.

DSGVO-KI-Compliance-Paket

- 4 Vorlagen: Checkliste, BV, Datenschutzhinweis, DSFA
wecando.ai/ki-business/dsgvo-ki-compliance-paket/

30 Prompt-SYSTEME

- Copy-Paste Workflows fuer ChatGPT, Claude & Co.
wecando.ai/ki-wissen/prompt-systeme-workflows/

KI-Blacklist: 23 Fehler

- Die haeufigsten KI-Fehler und wie du sie vermeidest
wecando.ai/ki-wissen/ki-blacklist/

150 Prompts Swipe-File

- Sofort einsetzbare Prompts fuer jede Situation
wecando.ai/ki-wissen/ki-prompt-swipe-file/

KI-Toolstack (7 Branchen)

- Branchenspezifische Tool-Empfehlungen mit Preisen
wecando.ai/ki-business/ki-toolstack-branchen/

KI in 7 Tagen (Kurs)

- Vom Anfaenger zum KI-Anwender in einer Woche
wecando.ai/ki-wissen/ki-in-7-tagen-kurs/

KI-ROI-Rechner

- Berechne deine KI-Ersparnis in 2 Minuten
wecando.ai/ki-tools/ki-roi-rechner/

wecando.ai – Die groesste deutschsprachige KI-Informationssammlung