KI-GEWERBE

KI-Wissen für kleine Unternehmen

KI IM KLEINEN UNTERNEHMEN

KI-Agenten im kleinen Unternehmen

Was darf die KI selbst erledigen?

PRAXISBUCH

Band 3 · 1. Ausgabe

Mit Praxisfällen, 5-Grenzen-Modell, Sicherheitscheck, Musterregeln und 30-Tage-Einführungsplan.

KI-Wissen für kleine Unternehmen
1. Ausgabe · Oktober 2026
Hersteller: AI-Ideenschmiede · Vertrieb: AILORIUM

Bevor es losgeht

KI-Agenten sind der Schritt von der reinen Antwortmaschine zur handelnden Software. Ein Chatbot formuliert einen Text, wenn Sie ihn darum bitten. Ein Agent kann dagegen einen Auftrag über längere Zeit verfolgen, Informationen aus mehreren Quellen zusammentragen, Regeln anwenden und - wenn Sie ihm die Berechtigung geben - Aktionen in anderen Systemen auslösen. Genau darin liegt der Nutzen, aber auch das Risiko.

Für kleine Unternehmen ist die entscheidende Frage deshalb nicht: Was kann die KI technisch? Sondern: Welche Handlung darf sie in unserem Betrieb selbst ausführen, welche muss ein Mensch freigeben und welche Entscheidung bleibt vollständig beim Menschen? Dieses Buch beantwortet diese Frage nicht abstrakt, sondern anhand typischer Abläufe aus Büro, Verkauf, Kundenservice, Buchhaltung, Marketing, Einkauf und Personal.

Das Ziel ist nicht maximale Automatisierung. Das Ziel ist kontrollierte Automatisierung: Routinearbeit soll verschwinden, ohne dass Kontrolle, Nachvollziehbarkeit und Verantwortung verschwinden.

> **Die Grundidee dieses Bandes**
> Ein guter KI-Agent besitzt einen klaren Auftrag, möglichst wenige Zugriffsrechte, feste Grenzen, definierte Freigabepunkte, eine Eskalationsregel und einen Not-Aus. Je größer die mögliche Auswirkung auf Menschen, Geld oder Verträge, desto enger müssen diese Grenzen sein.

So nutzen Sie dieses Buch

Lesen Sie zuerst die Kapitel 1 bis 4. Dort entsteht das Grundmodell. Danach können Sie direkt zu den Bereichen springen, die in Ihrem Betrieb wichtig sind. Die Praxisbeispiele sind bewusst so geschrieben, dass sie sich auf verschiedene Branchen übertragen lassen. Die Arbeitsblätter und Eintragungen gehören in das separate Arbeitsheft; dieses Praxisbuch bleibt deshalb inhaltlich dicht und vermeidet leere Schreibflächen.

Wichtiger Hinweis

Dieses Buch vermittelt allgemeine Informationen und praktische Orientierung. Es ersetzt keine Rechts-, Steuer-, Datenschutz- oder IT-Sicherheitsberatung. Bei Anwendungen mit erheblicher rechtlicher, finanzieller oder personenbezogener Wirkung sollte der konkrete Einzelfall fachlich geprüft werden.

ORIENTIERUNG

Inhalt & Lernweg

Schnell finden, passend vertiefen und direkt mit dem Arbeitsheft weiterarbeiten.

GRUNDLAGEN

01 · Was ein KI-Agent wirklich ist S. 4
AH Ü1 · S. 4
02 · Die drei Stufen der Autonomie S. 5
AH Ü2 · S. 5
03 · Die KI-Ampel S. 6
AH Ü3 · S. 6
04 · Das 5-Grenzen-Modell S. 7
AH Ü4 · S. 7

EINSATZFELDER

05 · Kundenanfragen und E-Mail S. 7-8
AH Ü5 · S. 8
06 · Termine und Organisation S. 8-9
AH Ü6 · S. 9
07 · Angebote, Rechnungen und Mahnungen S. 9
AH Ü7 · S. 10
08 · Einkauf und Bestellungen S. 9-10
AH Ü8 · S. 11
09 · Marketing und Social Media S. 10
AH Ü9 · S. 12
10 · Kundendienst und Chatbots S. 10-11
AH Ü10 · S. 13

EINSATZFELDER

11 · Personal, Bewerbungen und Mitarbeiter S. 11
AH Ü11 · S. 14
12 · Verträge, Zusagen und Geld S. 12
AH Ü12 · S. 15
13 · Datenschutz und Zugriffsrechte S. 12-13
AH Ü13 · S. 16
14 · Sicherheit: Fehler, Manipulation und Not- S. 13
AH Ü14 · S. 17
15 · Protokolle und Verantwortung S. 13-14
AH Ü15 · S. 18

UMSETZUNG & ABSCHLUSS

16 · Agenten richtig anweisen S. 14-15
AH Agentenkarte · S. 19
17 · Vier vollständige Praxisabläufe S. 15
AH 10-Sek.-Check · S. 20
18 · Einführung in 30 Tagen S. 16
AH Pilotplan · S. 21
19 · Welche Aufgaben sich wirklich lohnen S. 16-17
AH Startprofil · S. 3
20 · Werkzeuge und Verbindungen S. 17-18
AH Rechte-Matrix · S. 16
21 · Qualitätskontrolle im Alltag S. 18-19
AH Testprotokoll · S. 22
22 · Zehn typische Fehlstarts S. 19-20
AH Abschluss-Check · S. 23
23 · Musterrollen für kleine Unternehmen S. 20-21
AH Agentenkarte · S. 19
24 · Rechtlicher Rahmen S. 21-22
AH Rechtliches · S. 25
25 · Schnellcheck und Schlussfolgerung S. 22
AH Abschluss-Check · S. 23
Quellen und weiterführende Hinweise S. 23
Aktuelle Grundlagen und Nachweise.

ARBEITSHEFT

Direkt weiterarbeiten:
Übungen 1-15 ab Seite 4 · Agentenkarte S. 19 · Pilot & Abschluss S. 21-23.

1. Was ein KI-Agent wirklich ist

Ein KI-Agent ist kein magischer digitaler Mitarbeiter, der "einfach alles erledigt". Praktisch betrachtet besteht er aus fünf Bausteinen: Auftrag, Informationen, Werkzeuge, Regeln und Rückmeldung. Erst wenn diese Bausteine zusammenkommen, wird aus einer einzelnen KI-Antwort ein Arbeitsablauf.

Vom Prompt zum Arbeitsauftrag

Bei einem normalen Chat schreiben Sie beispielsweise: „Formuliere eine freundliche Antwort auf diese Kundenmail.“ Danach endet die Aufgabe. Ein Agent könnte dagegen den Auftrag erhalten: „Prüfe werktags neue Serviceanfragen, ordne sie einem Thema zu, suche die passende Information in unserer Wissensbasis und erstelle einen Antwortentwurf. Beschwerden und Rabattwünsche legst du immer einem Menschen vor.“ Der Agent muss dafür nicht nur Text erzeugen, sondern mehrere Schritte in der richtigen Reihenfolge erledigen.

> **Baustein Frage im Unternehmen Beispiel**

Auftrag Was soll der Agent erreichen? Neue Kundenanfragen vorbereiten

Informationen Worauf darf er zugreifen? Postfach, FAQ, Kundenstammdaten

Werkzeuge Was darf er benutzen? E-Mail, Kalender, CRM

Regeln Welche Grenzen gelten? Keine Rabatte, keine Vertragszusagen

Rückmeldung Wann muss er stoppen? Beschwerde, Unsicherheit, fehlende Daten

Agent ist nicht gleich Agent

Der Begriff wird für sehr unterschiedliche Systeme verwendet. Manche Agenten können lediglich Informationen sammeln und Entwürfe erzeugen. Andere dürfen Kalender verändern, Nachrichten senden oder Daten in Anwendungen eintragen. Wieder andere können mehrere spezialisierte Unter-Agenten koordinieren. Für kleine Unternehmen ist weniger die Bezeichnung entscheidend als die konkrete Berechtigung: Was kann dieses System in meinem Namen tatsächlich verändern?

> **Praxisregel**
> Beurteilen Sie einen KI-Agenten nicht nach seiner Oberfläche oder seinem Namen. Schreiben Sie stattdessen auf: Welche Daten kann er lesen? Welche Systeme kann er verändern? Welche Aktionen kann er ohne Rückfrage auslösen? Genau daraus ergibt sich sein tatsächliches Risiko.

Warum Agenten für kleine Unternehmen interessant sind

Kleine Betriebe haben häufig keine eigene Abteilung für Terminplanung, Kundenservice, Marketing oder Controlling. Wiederkehrende Aufgaben landen beim Inhaber oder bei wenigen Mitarbeitern. Genau dort können Agenten Zeit gewinnen: Sie suchen Informationen, tragen Daten zusammen, überwachen Fristen, erstellen Entwürfe oder führen klar definierte Standardvorgänge aus. Der größte Nutzen entsteht nicht bei seltenen Sonderfällen, sondern bei Tätigkeiten, die häufig, regelbasiert und gut überprüfbar sind.

- tägliche oder wöchentliche Routinen
- wiederkehrende Kundenfragen
- Übertragung von Daten zwischen Systemen

• Vorbereitung standardisierter Dokumente

• Fristen, Wiedervorlagen und Erinnerungen

• Zusammenfassungen und Statusberichte

2. Die drei Stufen der Autonomie

Nicht jede Automatisierung ist gleich riskant. Ein einfacher und sehr praxistauglicher Ansatz ist die Trennung in drei Stufen: vorbereiten, ausführen, entscheiden. Diese Einteilung hilft, eine Aufgabe so weit zu automatisieren, wie es sinnvoll ist, ohne gleich die komplette Kontrolle abzugeben.

Stufe 1 - Vorbereiten

Die KI sammelt, sortiert, prüft oder formuliert. Sie verändert noch nichts nach außen. Das ist für den Einstieg meist die beste Stufe. Beispiele: Antwortentwurf erstellen, freie Termine heraussuchen, offene Rechnungen auflisten, Bestellvorschlag vorbereiten oder einen Social-Media-Text formulieren.

Stufe 2 - Ausführen

Die KI führt eine bereits festgelegte Handlung aus. Dazu gehören etwa das Versenden einer freigegebenen Nachricht, das Eintragen eines Termins in einem erlaubten Zeitraum oder das Übertragen geprüfter Daten. In dieser Stufe muss klar sein, welche Bedingungen erfüllt sein müssen, bevor die Aktion startet.

Stufe 3 - Entscheiden

Die KI entscheidet selbst, ob und wie etwas geschehen soll. Hier entstehen die größten Auswirkungen. Beispiele wären ein eigener Rabattentscheid, die Ablehnung eines Bewerbers oder das Sperren eines Kundenkontos. Solche Entscheidungen sind nicht nur fehleranfälliger, sondern können rechtliche, wirtschaftliche oder menschliche Folgen haben.

GRÜN	GELB	ROT
Vorbereiten, zusammenfassen, suchen, Entwürfe erstellen.	Aktion nach klaren Regeln oder menschlicher Freigabe ausführen.	Rechtswirksame, finanzielle oder personelle Entscheidung nicht ungeprüft delegieren.

Die Rückwärtsfrage

Wenn Sie unsicher sind, beginnen Sie nicht mit der Frage „Wie viel kann ich automatisieren?“. Fragen Sie: Was wäre der schlimmste realistische Fehler? Wenn ein falscher Entwurf lediglich korrigiert werden muss, ist das Risiko gering. Wenn eine falsche Aktion Geld überweist, einen Vertrag beendet oder einen Menschen benachteiligt, braucht der Vorgang eine deutlich stärkere Kontrolle.

> **Beispiel: Terminbuchung**
> Ein Agent darf drei freie Termine anbieten und nach Auswahl des Kunden den Termin eintragen. Er darf aber bestehende Termine nicht verschieben, keine privaten Blockzeiten aufheben und keine Buchung außerhalb der Geschäftszeiten erzeugen. So bleibt die Aufgabe automatisiert, ohne den gesamten Kalender freizugeben.

3. Die KI-Ampel für kleine Unternehmen

Die Ampel ist keine Rechtsklassifizierung, sondern ein internes Arbeitsmodell. Sie zwingt dazu, jede Aufgabe nach Wirkung und Risiko zu betrachten. Ein und dieselbe Tätigkeit kann je nach Unternehmen unterschiedlich eingestuft werden. Eine automatisch versendete Terminbestätigung ist etwas anderes als eine automatisch versendete Kündigung.

GRÜN - selbstständig im definierten Rahmen

• Informationen aus freigegebenen Quellen suchen

• Texte, Zusammenfassungen und Entwürfe erstellen

• Daten nach festen Regeln kategorisieren

• Erinnerungen und Wiedervorlagen anlegen

• Standardtermine innerhalb klarer Grenzen buchen

• interne Statusberichte aus vorhandenen Daten erstellen

GELB - Agent arbeitet, Mensch bestätigt

• Nachrichten an Kunden in Sonderfällen

• Preisnachlässe, Gutschriften und Kulanz

• Bestellungen oberhalb einer Bagatellgrenze

• Änderungen an Rechnungen oder Vertragsdaten

• Veröffentlichung von Marketinginhalten mit Preisen oder Versprechen

• Löschung oder Änderung wichtiger Kundendaten

ROT - menschliche Entscheidung im Mittelpunkt

• Einstellung, Ablehnung oder Kündigung von Mitarbeitern

• größere oder ungewöhnliche Zahlungen

• Änderung von Bankverbindungen und Zahlungsempfängern

• rechtswirksame Sondervereinbarungen außerhalb freigegebener Vorlagen

• irreversible Löschung geschäftskritischer Daten

• ausschließlich automatisierte Entscheidungen mit erheblicher Wirkung auf Personen

> **Wichtig**
> „Rot“ bedeutet in diesem Buch nicht automatisch „gesetzlich verboten“. Es bedeutet: Die Auswirkung ist so groß, dass ein Mensch die Entscheidung oder ausdrückliche Freigabe übernehmen sollte. Ob darüber hinaus rechtliche Verbote oder besondere Pflichten gelten, hängt vom konkreten Einsatzfall ab.

Ampel nicht nur einmal festlegen

Agenten verändern sich, wenn neue Werkzeuge oder Datenquellen angeschlossen werden. Ein Agent, der nur Entwürfe erstellt, kann grün sein. Sobald er zusätzlich E-Mails versenden und Preise ändern darf, steigt das Risiko. Prüfen Sie die Ampel daher immer erneut, wenn Berechtigungen, Datenquellen oder Aufgaben erweitert werden.