Den ersten KI-Agenten bauen

Vier Bausteine, ein System-Prompt, ein Sicherheitsnetz

Ein Chatbot antwortet, ein Agent handelt. Der Unterschied entsteht nicht durch besseres Prompten, sondern durch einen Bauplan: **Auslöser, Eingabe, Verarbeitung, Ergebnis**, dazu eine Plattform, die die Software tatsächlich bedient.

DIE VIER BAUSTEINE JEDES WORKFLOWS

AUSLÖSER
Neue E-Mail, ausgefülltes Formular oder ein fixer Zeitpunkt, etwa täglich 18 Uhr.

EINGABE
Texte, PDFs, CRM-Daten. Alles, was der Agent lesen darf.

VERARBEITUNG
Extrahieren, klassifizieren, zusammenfassen.

ERGEBNIS
Datenbankeintrag, Entwurfsmail, Ticket, Freigabevorschlag.

DER SYSTEM-PROMPT IN FÜNF TEILEN

1. **Rolle und Ziel.** Wofür der Agent da ist.
2. **Konkrete Aufgaben.** Nummeriert, nicht als Fließtext.
3. **Vorgehensweise.** In welcher Reihenfolge.
4. **Fehlerkultur.** „Erfinde niemals Daten.“
5. **Tool-Regeln.** Wann welches Tool benutzt wird.

DAS SICHERHEITSNETZ

- **Menschliche Freigabe.** Bei allem, was Geld bewegt oder Daten löscht.
- **Harte Limits.** Zahl der Aktionen, Summen, fester Empfängerkreis.
- **Logbuch.** Jede Aktion nachvollziehbar.
- **Testphase nur mit Leserechten.** Schreiben erst, wenn es sitzt.

BEISPIEL: DER RECHNUNGSAGENT

WAS ER TUT UND WO ER ANHÄLT
Er greift E-Mails am Postfach für Rechnungen ab, sichert den PDF-Anhang, lässt ihn analysieren und schreibt eine neue Zeile in eine Tabelle: Typ, Lieferant, Nummer, Datum, Fälligkeit, Betrag, Währung, Kostenstelle, Bemerkung.
Beträge über 1.000 Euro bekommen automatisch eine rote Markierung für die Zweitprüfung.

DIE BEIDEN PLATTFORMEN

	Make	n8n
Bewertung	8,9 von 10	8,2 von 10
Anbieter	Celonis SE, Deutschland	n8n GmbH, Deutschland
Stärke	breite Anbindung, No-Code-Baukasten	Datenhoheit und Anpassbarkeit

SCHRITT 5: TESTEN UND SKALIEREN

MIT HISTORISCHEN DATEN, NICHT MIT LAUFENDEN
Den Agenten zuerst an alten Rechnungen durchlaufen lassen und den Prompt dort nachschärfen, wo er stolpert, etwa bei Fremdwährungen oder Gutschriften.

MERKSÄTZE

Dem Chatbot sagst du, was du brauchst. Der Agent erledigt es, aber nur im abgesteckten Rahmen.

Der Agent bereitet vor. Die Verantwortung übernimmt er nicht. Ein falsch konfigurierter Agent mit Schreibrechten trägt falsche Beträge ein oder verschickt unkontrolliert E-Mails.