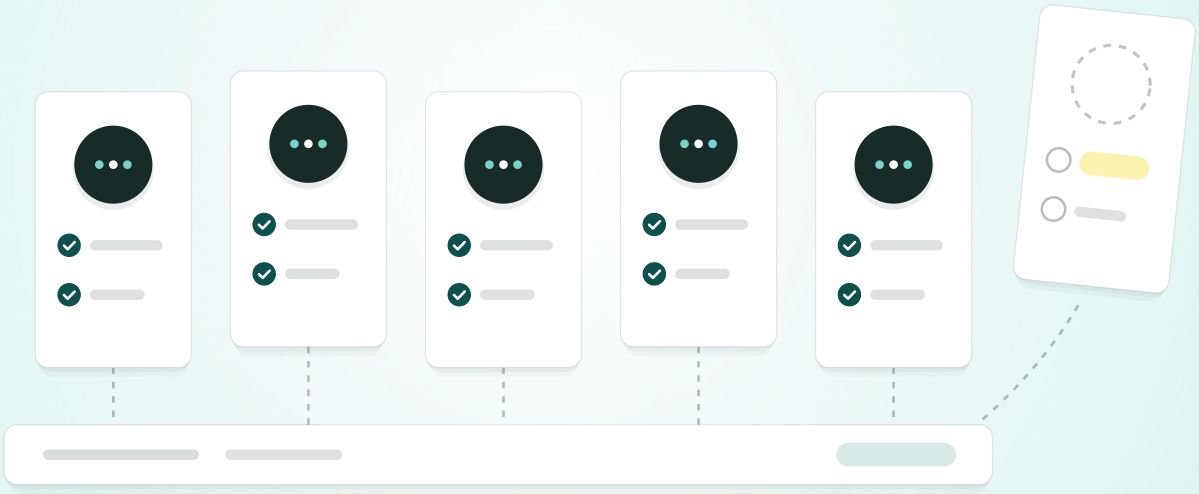


WHITEPAPER FÜR ENTSCHEIDER

Agentic AI im Mittelstand

Was KI-Agenten leisten, wo sie sich lohnen und wie der Einstieg sicher gelingt

KI-Agenten beantworten nicht nur Fragen, sie erledigen ganze Prozesse. Für den Mittelstand ist das die Chance, Routinearbeit zu bewältigen, für die Fachkräfte fehlen. Dieses Whitepaper erklärt, was KI-Agenten können, wo sie sich lohnen, welche Hürden es gibt und wie Unternehmen sicher anfangen.

Für Geschäftsführung, Finanz- und IT-Leitung im Mittelstand

HERAUSGEBER
SCALAN

STAND
November 2026

EINLEITUNG

Wenn KI nicht nur antwortet, sondern handelt

Künstliche Intelligenz ist im Mittelstand angekommen, meist als KI-Chat, der Texte formuliert und Fragen beantwortet. Die nächste Stufe heißt Agentic AI. Gemeint ist KI, die Aufgaben selbstständig erledigen kann. Für viele Unternehmen ist das die Chance, effizienter zu werden und Kosten zu sparen.

Mehr als die Hälfte der Unternehmen in Deutschland setzt inzwischen KI ein. 2024 war es erst ein Fünftel.[1] Ein KI-Chat macht einzelne Beschäftigte schneller. An den Abläufen ändert er wenig, denn die eigentliche Arbeit bleibt beim Menschen.

Agentic AI geht einen Schritt weiter. Der englische Begriff steht für KI-Systeme, die eine Aufgabe von Anfang bis Ende bearbeiten. Sie verstehen den Auftrag, planen die nötigen Schritte, nutzen dafür Programme und Daten des Unternehmens und liefern ein Ergebnis. Diese Systeme nennt man umgangssprachlich KI-Agenten. Erst rund jedes zehnte Unternehmen setzt sie bisher ein.[1]

Beispiel: Sammelpostfach

In diesem Whitepaper nutzen wir ein reales Beispiel, welches wir bereits bei Kunden eingeführt haben. Es zeigt die Unterschiede zu herkömmlichen KI-Anwendungen, die daraus resultierenden Anforderungen und die möglichen Gewinne. Stellen Sie sich vor: Im Sammelpostfach eines Unternehmens gehen jeden Tag 50 Kundenanfragen ein. Mit einem KI-Chat liest die Sachbearbeitung weiterhin jede Mail selbst und lässt sich meist beim Formulieren der Antwort helfen. Ein KI-Agent dagegen liest die Mails automatisch und direkt beim Eingang, erkennt das Anliegen, sucht die passenden Informationen selbstständig heraus und entwirft eine Antwort. Die Sachbearbeitung prüft dann nur noch den Entwurf und schickt ihn ab. Dabei kann der KI-Agent die notwendigen Informationen zur Beantwortung, etwa den zugrunde liegenden Servicevertrag oder ein Betriebshandbuch, eigenständig recherchieren. Dies spart deutlich Arbeitszeit und reduziert Fehler.

GRAFIK So arbeitet ein KI-Agent, am Beispiel Sammelpostfach



Warum jetzt

Bis 2039 erreichen 13,4 Millionen Erwerbspersonen das Rentenalter, fast jede dritte.[2] Ein Teil der Arbeit, die heute liegen bleibt oder Überstunden kostet, lässt sich mit KI-Agenten auffangen. Von selbst geschieht das allerdings nicht. KI-Agenten brauchen eine klar umrissene Aufgabe, Regeln dafür, was sie dürfen, und Menschen, die für sie verantwortlich sind. Wo das fehlt, bleibt es beim Pilotprojekt (Seite 9).

Dieses Whitepaper erklärt, was KI-Agenten können, wo sie sich lohnen, welche Hürden es gibt und wie der Einstieg sicher gelingt. Es richtet sich an Geschäftsführung, Finanz- und IT-Leitung im Mittelstand.

VERSTEHEN

Vom KI-Chat zum KI-Agenten

Automatisierung im Unternehmen lässt sich grob in drei Stufen beschreiben. Klassische Softwareentwicklung ist gut für deterministische Abläufe geeignet, KI-Chats helfen reaktiv einzelnen Menschen, und KI-Agenten übernehmen ganze Aufgaben. Erst mit KI-Agenten zeigt sich die Wirkung im Betriebsergebnis.

Die erste Stufe ist die regelbasierte Automatisierung. Softwareprogramme übertragen Daten von einem System ins andere oder lösen nach festen Regeln Buchungen aus. Das funktioniert zuverlässig, solange jeder Fall gleich aussieht und die Daten gleich sind. An einer Mail in eigenen Worten oder an einem Beleg in ungewohntem Format scheitert sie.

Die zweite Stufe sind KI-Chats. Sie verstehen Sprache, formulieren Texte und fassen Dokumente zusammen. Laut McKinsey sehen 80 % der Befragten ihre persönliche Produktivität durch KI verbessert, aber nur 37 % eine Wirkung auf das Betriebsergebnis.[3] Der Grund ist einfach. Ein KI-Chat wartet, bis jemand fragt, und die eigentliche Arbeit bleibt beim Menschen.

Die dritte Stufe sind KI-Agenten. Sie verbinden das Sprachverständnis der KI-Chats mit der Fähigkeit zu handeln. Ein Agent versteht den Kontext und den Inhalt eines Dokuments und folgt zeitgleich den gegebenen Anweisungen an ihn. Damit bearbeitet er die Aufgabe nach den Regeln des Unternehmens und liefert proaktiv ein fertiges Ergebnis, das ein Mensch dann prüfen kann (sogenanntes Human-in-the-Loop). Das „kann“ ist bewusst gewählt, denn technisch ist die Prüfung nicht notwendig. Der KI-Agent könnte auch ohne Prüfung den Prozess bis zum Ende durchführen, aber gerade in der Einführung empfehlen wir zusätzliche Prüfschritte.

Die Übersicht ordnet die drei Stufen ein, dazu die KI-Assistenten, die viele Programme inzwischen mitbringen.

ART	EINSATZGEBIET	EINSATZGRENZEN
Regelbasierte Automatisierung	gleichförmige Abläufe nach festen Regeln, etwa Daten zwischen Systemen übertragen	scheitert an Abweichungen, die niemand vorgesehen hat
KI-Chat	Fragen beantworten, Texte entwerfen, Dokumente zusammenfassen	handelt nicht selbst, die Arbeit bleibt beim Menschen
KI-Assistent in Standardsoftware	Unterstützung innerhalb eines Programms, etwa Zusammenfassungen in der Bürosoftware	endet an der Grenze dieses Programms
KI-Agent	wiederkehrende Aufgaben mit Dokumenten, bei denen man Kontext und Inhalt verstehen muss, typischerweise semi- und unstrukturierte Daten wie Mails, Belege oder PDF-Dateien	darf nur, was ihm das Unternehmen erlaubt, und braucht klare Regeln

VERSTEHEN · WERKZEUG

Wie selbstständig ein Agent arbeiten darf

Ein KI-Agent sollte nur so viel Handlungsspielraum haben, wie er für die jeweilige Aufgabe benötigt. Diese Grenzen muss das Unternehmen sowohl technisch als auch fachlich festlegen. Die Autonomie-Leiter beschreibt dafür sechs Stufen. Für den Einstieg empfehlen wir den Human-in-the-Loop-Ansatz.

Je mehr ein Agent allein erledigen darf, desto mehr Zeit spart er, und desto wichtiger werden feste Grenzen. Deshalb sollte das Unternehmen die Stufe für jeden Vorgang oder Prozess einzeln festlegen, gemeinsam mit dem Fachbereich, der die Aufgabe verantwortet. Sinnvoll ist es, vorsichtig zu beginnen und die Autonomie erst zu erhöhen, wenn sich der Agent über Wochen bewährt hat und Menschen immer seltener eingreifen müssen.

Wie selbstständig ein Agent arbeitet, hängt von drei Stellschrauben ab: dem Umfang der Aufgabe, seinen Rechten in den angebundenen Systemen und der Frage, ob ein Mensch jedes Ergebnis prüft. Die Leiter zeigt am Beispiel des Sammelpostfachs, in welcher Reihenfolge Unternehmen daran drehen. Höher ist nicht automatisch besser, der Business Case auf Seite 8 rechnet mit Stufe 3.

WERKZEUG

Autonomie-Leiter

empfohlener Einstieg

STUFE	AUFGABE DES AGENTEN	ZUGRIFF	ROLLE DES MENSCHEN	BEISPIEL
1 Antwort zuliefern	beantwortet die Kernfrage einer eingehenden Anfrage	liest Wissen und Daten	übernimmt die Antwort und handelt	nennt zu jeder Anfrage den Lieferstatus
2 Arbeitsschritt vorbereiten	erledigt den ganzen Arbeitsschritt	wie Stufe 1	überträgt das Ergebnis und sendet	formuliert die vollständige Antwortmail
3 Entwurf im System	legt Ergebnisse in Arbeitssystemen ab	schreibt Entwürfe außerhalb der Kernsysteme	prüft jeden Entwurf und sendet	legt die Antwort als Entwurf im Postfach ab
4 Selbstständig ohne Kernsystem	erledigt Routinefälle allein, auch nach außen	wie Stufe 3, dazu senden	prüft Stichproben, bearbeitet Ausnahmen	beantwortet Standardanfragen selbst und legt den Rest als Entwurf vor
5 Kernsystem mit Freigabe	bereitet Änderungen in Kernsystemen vor	schreibt im Kernsystem nach Freigabe	gibt jede Änderung frei	trägt neue Liefertermine in die Warenwirtschaft ein
6 Kernsystem selbstständig	ändert Daten in Kernsystemen allein, in festen Grenzen	wie Stufe 5, ohne Einzelfreigabe	prüft Stichproben, bearbeitet Ausnahmen	verschiebt Liefertermine in festen Grenzen selbst

Auf den Stufen 4 und 6 gibt ein Mensch nicht mehr jeden Fall frei, er überwacht. Er prüft Stichproben und bekommt alle Fälle, bei denen der Agent unsicher ist. Nach außen schreibt der Agent nur mit geprüften Textbausteinen und als KI erkennbar. Nach einem Vorfall geht es eine Stufe zurück.

GRUNDSATZ FÜR ALLE STUFEN

Ein Agent erhält nur die Rechte, die seine Aufgabe verlangt, festgelegt je Aufgabe. Die Anbindung an ein System kann technisch mehr, deshalb gibt die Plattform je Agent nur die nötigen Aktionen frei und sperrt alle anderen. Ein Agent, der eingehende Mails beantwortet, darf dann beispielsweise auf Stufe 6 in der Warenwirtschaft nur Liefertermine verschieben, aber keine Preise ändern, nichts stornieren und keine Stammdaten anlegen. So erhält das Unternehmen eine weitere Absicherung, die das Risiko zusätzlich begrenzt. Zahlungen auslösen, Daten löschen oder über Personen entscheiden darf ein Agent auf keiner Stufe.

ANWENDUNGSFÄLLE

Wo KI-Agenten sich lohnen

KI-Agenten eignen sich für wiederkehrende Aufgaben, bei denen Menschen heute semi- und unstrukturierte Dokumente wie Mails, Verträge, Rechnungen oder Belege lesen, den Inhalt verstehen und nach gewissen Regeln verarbeiten. Für den Einstieg empfiehlt sich eine Aufgabe, die häufig vorkommt, spürbar Arbeitszeit bindet und ohne Schreibrechte in Kernsystemen wie der Warenwirtschaft auskommt.

Ein Vorgang ist ein guter Kandidat, wenn drei Dinge zusammenkommen. Er fällt häufig an, täglich oder gesammelt zu einem Stichtag. Die Daten sind unstrukturiert und verlangen Verständnis, werden aber nach klaren Regeln bearbeitet. Und das Wissen, wie die Aufgabe richtig erledigt wird, ist bereits in Vorlagen, Richtlinien oder früheren Fällen vorhanden.

Weniger für den Einstieg geeignet sind seltene Einzelfälle und Aufgaben, die Schreibrechte in Kernsystemen wie dem ERP benötigen. Was ein Mensch mit einem KI-Chat gut allein schafft, etwa Gesprächsnotizen zusammenfassen, braucht ebenfalls keinen Agenten. Entscheidungen über Personen gehören aus rechtlichen Gründen immer in Menschenhand.

Womit anfangen

In unseren Gesprächen mit Führungskräften aus dem Mittelstand hörten wir eine einfache Faustregel.[4] Am besten beginnt man mit der Aufgabe, die alle ungern erledigen. Der Agent liest dafür aus dem Postfach oder über lesende Anbindungen aus Systemen wie CRM und liefert Entwürfe, die das Team prüft. Gerade diese Anbindungen bringen großen Mehrwert, weil der Agent mit aktuellen Daten arbeitet. Schreibrechte in Kernsystemen kommen erst später dazu (Seite 4). Nach unserer Erfahrung eignen sich die folgenden acht Beispiele gut für den Einstieg mit Anbindung an Systeme.

SERVICE, ÖFFENTLICHER BEREICH

Kundenanfragen

Mails, Dateiablage → Antwortentwürfe

Der Agent ordnet jede Anfrage Kategorien zu und entwirft die Antwort, die Sachbearbeitung prüft und sendet.

QUALITÄT UND SERVICE

Beschwerden und Reklamationen

Mails, Ticketsystem → erfasste Fälle mit Antwortentwurf

Der Agent erfasst Auftrag, Mangel und Dringlichkeit, entwirft eine Antwort nach den Vorgaben des Unternehmens und gibt den Fall an die zuständige Stelle.

VERTRIEB

Angebotsanfragen

Mail, Preisliste, CRM → Angebotsentwurf mit offenen Fragen

Der Agent liest Anfragen mit Stücklisten oder Zeichnungen, ordnet die Positionen passenden Artikeln und Preisen zu, entwirft das Angebot und listet offene Fragen auf, der Vertrieb prüft und sendet.

EINKAUF

Leistungsverzeichnisse

Mail, Dateiablage, CRM → Zuordnung und Anfrageunterlagen

Der Agent ordnet jede Position einer Ausschreibung passenden Produkten zu, markiert unklare Positionen und bereitet die Anfragen an Lieferanten vor.

EINKAUF

Auftragsbestätigungen

Mail, Dateiablage, ggf. ERP → Liste der Abweichungen

Der Agent gleicht jede Auftragsbestätigung eines Lieferanten mit der Bestellung ab und meldet abweichende Preise, Mengen oder Liefertermine.

FINANZEN

Reisekosten

Mail, Richtlinien → Liste der Abweichungen

Der Agent gleicht Belege mit der Reisekostenrichtlinie ab und markiert, was nicht passt.

PERSONAL

Fragen an die Personalabteilung

Mail, Richtlinien, Ticketsystem → Antworten mit Fundstelle

Der Agent beantwortet wiederkehrende Fragen, etwa zu Urlaub oder Dienstwagen, und nennt die Stelle in der Richtlinie.

PERSONAL

Bewerbungseingang

Mail, Bewerbermanagement → Übersicht für die Auswahl

Der Agent prüft Bewerbungen auf Vollständigkeit und fasst die Qualifikationen im Abgleich mit dem Stellenprofil zusammen, die Auswahl trifft die Personalabteilung (Seite 10).

ANWENDUNGSFÄLLE · WERKZEUG

Den richtigen Anwendungsfall finden

Anwendungsfälle für KI-Agenten gibt es in jedem Unternehmen viele. Aber mit welchen sollte man starten? Wir geben Ihnen eine einfache Scorecard zur Hand, mit der Sie Vorschläge strukturiert bewerten und eine Priorisierung ableiten können.

Ein Anwendungsfall ist eine Aufgabe, ein Vorgang oder ein Prozess, den ein KI-Agent übernehmen soll. Die Vorschläge sammelt man am besten in den Abteilungen des Unternehmens, denn wer eine Aufgabe täglich erledigt, weiß, wo sie Zeit kostet. Danach bewertet ein kleines Team aus Anwendern, IT und Finanzen jeden Vorschlag. Unsere Scorecard hilft Ihnen, mit sechs Merkmalen und einem Punktesystem schnell zu einer groben Priorisierung zu kommen und gute Kandidaten für den Einstieg zu identifizieren.

WERKZEUG

Scorecard für Anwendungsfälle

MERKMAL	0 PUNKTE	1 PUNKT	2 PUNKTE
Aufwand heute	unter 10 Stunden im Monat	10 bis 30 Stunden im Monat	über 30 Stunden im Monat
Feste Regeln	jeder Fall ist ein Einzelurteil	viele Ausnahmen	klare Regeln trotz unterschiedlicher Eingänge
Fehlerfolgen	wirken sofort nach außen	intern, aber aufwendig zu korrigieren	fallen beim Prüfen auf
Wissen und Unterlagen	nur in den Köpfen	teilweise aufgeschrieben	Regeln, Vorlagen und Beispiele liegen vor
Anbindung	braucht Schreibrechte in Kernsystemen	braucht eine neue Schnittstelle	liest über vorhandene Anschlüsse, etwa Postfach, CRM oder Ticketsystem
Vorhandene Software	erledigt die Aufgabe schon	erledigt sie teilweise	erledigt sie nicht

Auswertung

- **10 bis 12 Punkte:** für den Start geeignet
- **7 bis 9 Punkte:** für später vormerken
- **0 bis 6 Punkte:** zurückstellen

Ausnahme: Null Punkte bei den Fehlerfolgen oder bei der vorhandenen Software heißen zurückstellen, unabhängig von der Summe.

BEISPIEL

Das Sammelpostfach aus der Einleitung

Aufwand heute rund 46 Stunden im Monat	2 Punkte	**Wissen und Unterlagen** Antworten erst teilweise aufgeschrieben	1 Punkt
Feste Regeln klare Regeln für wiederkehrende Anfragen	2 Punkte	**Anbindung** liest über Postfach und Dateiablage	2 Punkte
Fehlerfolgen fallen beim Prüfen der Entwürfe auf	2 Punkte	**Vorhandene Software** keine übernimmt diese Aufgabe	2 Punkte

Summe — **11 von 12 Punkten**

Damit eignet sich das Sammelpostfach für den Start. Es fehlt nur eine Sammlung geprüfter Antworten, die das Team vorher anlegt.

NUTZEN

Was KI-Agenten bringen

KI-Agenten sparen Arbeitszeit, doch ihr Nutzen reicht weiter. Sie beschleunigen Abläufe, sorgen für gleichbleibende Qualität und halten Wissen im Unternehmen. Für den Mittelstand zählt vor allem, dass sie Routinearbeit auffangen, für die keine zusätzlichen Fachkräfte zu finden sind.

Die folgenden sechs Vorteile zeigen, was sich im Alltag ändert, wenn ein Agent eine Aufgabe übernimmt.

Entlastung im Arbeitsalltag

Der Agent übernimmt Routineaufgaben wie Recherchieren, Sortieren, Abgleichen und Vorformulieren. Die Mitarbeitenden prüfen, entscheiden und kümmern sich um die Fälle, die Erfahrung verlangen.

Schnellere Bearbeitung

Ein Agent bereitet jeden Eingang sofort vor, auch abends und in der Urlaubszeit. Morgens liegen die Entwürfe bereit, statt dass Anfragen warten, bis jemand Zeit hat.

Höhere Qualität

Der Agent wendet die vorgegebenen Regeln in jedem Fall gleich an und kann schnell sehr große Datenmengen verarbeiten. Zudem wird jeder Schritt protokolliert. Das erleichtert Prüfungen und die Einarbeitung neuer Beschäftigter.

Hilfe gegen den Fachkräftemangel

Bleiben Stellen unbesetzt oder gehen erfahrene Beschäftigte in Rente, fangen Agenten einen Teil der Arbeit auf.

Wissen bleibt im Unternehmen

Der Prozessablauf, den ein Agent ausführt, ist in schriftlicher Form dokumentiert und gehört dem Unternehmen. Er geht nicht verloren, wenn jemand das Unternehmen verlässt.

Wachstum ohne gleichen Personalaufbau

Steigt die Zahl der Anfragen oder Belege, bearbeitet der Agent sie mit. Nicht jede Spitze verlangt eine neue Stelle.

Wie viel davon sich in Euro ausdrücken lässt, zeigt der Business Case auf der nächsten Seite. Er rechnet mit der eingesparten Arbeitszeit und zwei weiteren Effekten, die sich messen lassen. Was schnellere Antworten und gleichmäßigere Qualität darüber hinaus bringen, ist nicht eingerechnet.

NUTZEN · WERKZEUG

Der Business Case für den ersten Agenten

Schon der erste KI-Agent lohnt sich, wenn er eine Aufgabe übernimmt, die genug Arbeitszeit bindet. Diese Vorlage zeigt den Business Case anhand unseres Beispiels, des Sammelpostfachs.

Diese Rechnung stellt zwei Größen gegenüber. Auf der einen Seite stehen die eingesparte Arbeitszeit, bewertet mit einem durchschnittlichen Stundensatz, und weitere Effekte, die sich messen lassen. Auf der anderen Seite stehen die Kosten für Plattform und KI-Nutzung, Einführung und Betreuung. Weil ein Mensch weiterhin jeden Entwurf prüft, zeigt die Rechnung **die Untergrenze der Einsparungen**: Je selbstständiger ein Agent arbeiten darf, desto mehr spart er.

Im Beispiel kosten 50 E-Mails am Tag zu je drei Minuten heute rund 23.100 € im Jahr. Mit dem Agenten prüft der Mitarbeiter nur noch die Entwürfe, im Schnitt eine Minute je Anfrage. Zudem landen weniger Mails an der falschen Stelle und Kunden fragen seltener nach. Nach allen Kosten ergeben sich Einsparungen im ersten Jahr in Höhe von 8.730 €. Die Aufgabe kostet damit 38 % weniger als heute, ab dem zweiten Jahr 49 % weniger.

WERKZEUG **Business-Case-Vorlage**

8.730 €
Ergebnis im ersten Jahr
–38 % Kosten gegenüber heute

11.230 €
in jedem weiteren Jahr
–49 % Kosten gegenüber heute

rund 2,7 Monate
bis die Einführung bezahlt ist

POSTEN	ANNAHME IM BEISPIEL	BETRAG IM ERSTEN JAHR	EIGENER ANWENDUNGSFALL
Menge	50 Anfragen am Tag an 220 Arbeitstagen	11.000 Anfragen	
Arbeitszeit heute	3 Minuten je Anfrage, 42 € je Stunde	23.100 €	
Arbeitszeit mit Agent	1 Minute je Anfrage für Prüfen und Senden	7.700 €	
Eingesparte Arbeitszeit	367 Stunden	**15.400 €**	
Weniger Fehlleitungen	550 Anfragen (5 %), je 3 Minuten an falscher Stelle	1.150 €	
Weniger Nachfragen	550 Nachfragen (5 %), je 1 Minute und 0,45 €	630 €	
Plattform und KI-Nutzung	0,45 € je Anfrage	–4.950 €	
Einführung, einmalig	2 Personentage zu je 1.250 €	–2.500 €	
Betreuung im Betrieb	2 Stunden im Monat	–1.000 €	
Ergebnis im ersten Jahr	38 % weniger Kosten als heute	8.730 €	
Ergebnis ab dem zweiten Jahr	ohne Einführung, 49 % weniger Kosten als heute	11.230 €	
Amortisation der Einführung	Einführung ÷ Überschuss im Monat	rund 2,7 Monate	

Die Annahmen sind konservativ gewählt und ersetzen keine Messung im eigenen Unternehmen. Nicht eingerechnet sind mehr Abschlüsse durch schnellere Antworten und eine kürzere Einarbeitung. Jede weitere Anfrage kostet mit Agent nun 1,15 € statt ursprünglich 2,10 €.

Zwei Hinweise machen die Rechnung belastbar. Erstens misst der Fachbereich zwei Wochen lang Menge und Dauer der Aufgabe, dazu Fehlleitungen und Nachfragen, bevor der Agent startet. Zweitens wird gesparte Zeit erst dann zu Geld, wenn sie Überstunden, Aushilfen oder Neueinstellungen ersetzt oder liegengebliebene Arbeit erledigt.

HÜRDEN

Die häufigsten Bedenken und was hilft

In unseren Gesprächen mit Führungskräften aus dem Mittelstand kamen dieselben Bedenken immer wieder.[4] Keines davon ist ein Grund, auf KI-Agenten zu verzichten. Jedes verlangt aber eine klare Antwort, bevor der erste Agent startet.

Wer haftet, wenn ein Agent einen Fehler macht?

Nach außen haftet in erster Linie das Unternehmen, wie bei Fehlern seiner Beschäftigten oder seiner Software. Abgeben lässt sich die Haftung nicht, begrenzen lässt sie sich aber schon. An dieser Stelle ist der wichtigste Baustein eine geeignete Plattform zum Betrieb der Agenten, die detaillierte Berechtigungen und volle Transparenz ermöglicht. So kann im Ernstfall nachvollzogen werden, dass die Handlungen sorgfältig vollzogen wurden (Seite 10).

→ Rechte begrenzen und protokollieren

Rechnet sich das für uns?

Ja, wenn der Agent eine Aufgabe übernimmt, die genug Arbeitszeit bindet, und die resultierenden Effekte auch monetär beziffert werden. Im Sammelpostfach bleiben nach Abzug aller Kosten im ersten Jahr rund 8.700 €, mit einer Kostenreduktion um 38 %. Die Einführung ist nach knapp drei Monaten bezahlt (Seite 8). Entscheidend ist der heutige Aufwand. Nicht eingerechnet sind indirekte Effekte wie mehr Abschlüsse durch schnellere Antworten und eine kürzere Einarbeitung. Auch diese müssten berücksichtigt werden. Deshalb steht am Anfang eine Messung, wie viel Zeit die Aufgabe kostet.

→ heutigen Aufwand messen, mit einer zeitintensiven Aufgabe beginnen

Brauchen wir dafür eigene Entwickler?

Nicht unbedingt. Viele KI-Agenten lassen sich heute in normaler Sprache anweisen, statt sie zu programmieren. Dies kann vom (Fach-)Anwender selbst übernommen werden. Eine zweite Person prüft den Agenten, bevor er in Betrieb geht, und die IT legt zentral Budget, Modelle und verfügbare Schnittstellen fest.

→ Anwender weist den KI-Agenten selbst an

Was passiert mit unseren Daten?

Vier Fragen klären das Wesentliche. Wo werden die Daten verarbeitet? Trainiert der Anbieter damit KI-Modelle? Wie lange speichert er sie? Gibt es einen Vertrag zur Auftragsverarbeitung nach der Datenschutz-Grundverordnung? Diese Fragen sollten Sie an eine Agentenplattform stellen. Grundanforderung sollte sein, dass die Datenverarbeitung auf die EU beschränkt ist und Training mit eigenen Daten vertraglich ausgeschlossen ist.

→ Verarbeitung in der EU, kein Training

Warum bleiben so viele Projekte im Pilotstadium?

Laut Gartner werden bis Ende 2027 über 40 % der Projekte mit KI-Agenten eingestellt, vor allem wegen steigender Kosten, unklaren Nutzens und fehlender Risikokontrollen.[5] Oft fühlt sich nach dem Start niemand für den Agenten verantwortlich, und jedes Projekt klärt Rechte, Kosten und Haftung von vorn. Abhilfe schaffen Regeln, die einmal für alle Agenten gelten, und für jeden Agenten eine verantwortliche Person im Fachbereich.

→ Regeln für alle, Verantwortliche je Agent

Wie reagieren Belegschaft und Betriebsrat?

Beschäftigte fragen zuerst, was KI für ihre Arbeit bedeutet. Hilfreich ist eine klare Aussage der Geschäftsführung: Agenten übernehmen Routine, die Verantwortung bleibt beim Menschen. Den Betriebsrat bindet das Unternehmen früh ein, denn bei solchen Systemen bestimmt er in der Regel mit. Seit Februar 2025 verpflichtet die KI-Verordnung der EU Unternehmen zudem, für ausreichende KI-Kompetenz ihrer Beschäftigten zu sorgen.[6]

→ früh informieren und schulen

SICHERHEIT UND RECHT

Sicher einsetzen: Leitplanken für KI-Agenten

Fehler lassen sich bei KI-Agenten tatsächlich mehr ausschließen als bei Menschen, nur leider nie vollständig. Entscheidend ist deshalb, vorab festzulegen, welche Berechtigungen ein Agent hat, um den größten möglichen Schaden zu begrenzen. Fünf Leitplanken bilden dafür die Grundlage.

Ein KI-Agent arbeitet mit Daten des Unternehmens, liest Inhalte und handelt in angebundenen Systemen. Damit das sicher geschieht, legt ein Unternehmen Regeln fest und die Plattform setzt diese technisch durch. Diese fünf Leitplanken beschreiben, worauf es dabei ankommt.

1

Rechte so viel wie nötig, so wenig wie möglich

Ein Agent bekommt nur die Aktionen, die seine Aufgabe verlangt, etwa Mails lesen und Entwürfe anlegen, aber nicht senden oder löschen. Wo möglich, gelten die Rechte nur für die betroffenen Datensätze und nur bis zu einem festgelegten Umfang der Änderung. Die Plattform sollte das technisch durchsetzen, denn ein fehlendes Recht schützt zuverlässiger als ein Verbot in der Anweisung.

2

Freigabe vor jeder Wirkung nach außen

Alle Handlungen, welche nach außen wirken, sollte zunächst ein Mensch freigeben. So fallen Fehler auf, bevor sie wirken.

3

Schutz vor eingeschleusten Anweisungen durch die Architektur

Angreifer können in Mails oder Dokumenten Anweisungen verstecken, die einen Agenten umsteuern sollen. Fachleute sprechen von Prompt Injection. Verlässlich abfangen lässt sich das nur im Aufbau der Plattform. Sie muss jeden Ablauf kapseln, eingehende Inhalte getrennt ablegen, sie dem Agenten nie als Anweisung übergeben und Manipulationsversuche blockieren.

4

Budgets und Sofortstopp

Verschiedene Budgets, etwa je Durchlauf und Monat, begrenzen die Kosten und machen Ausreißer früh sichtbar. Mit einem Sofortstopp lässt sich jeder Agent jederzeit anhalten.

5

Protokoll jeder Ausführung

Eingang, Ergebnis, Freigaben und Systemzugriffe sollten für jede Ausführung festgehalten werden. So lässt sich nachvollziehen, was der Agent getan hat.

RECHT Was aktuell gilt, in aller Kürze

Haftung
Für Fehler seiner Agenten haftet in erster Linie das Unternehmen. Es sollte den möglichen Schaden begrenzen und seine Sorgfalt belegen können. Ob solche Belege bei KI-Agenten entlasten, haben Gerichte noch nicht entschieden.

KI-Verordnung der EU
Seit Februar 2025 müssen Unternehmen für ausreichende KI-Kompetenz der Beschäftigten sorgen, die mit KI arbeiten.[6] Kommunizieren Kunden direkt mit einem Agenten, muss das erkennbar sein. Für Systeme, die Bewerbungen auswerten, gelten ab Dezember 2027 zusätzliche Pflichten.[7]

Datenschutz
Verarbeitet ein Agent personenbezogene Daten, braucht es mit dem Anbieter einen Vertrag zur Auftragsverarbeitung. Entscheidungen, die Menschen rechtlich betreffen, trifft ein Mensch.[8]

Betriebsrat
Kann ein System Leistung oder Verhalten von Beschäftigten erfassen, bestimmt der Betriebsrat in der Regel mit.[9] Wer ihn früh einbindet, kommt schneller voran.

Stand November 2026, keine Rechtsberatung.

UMSETZEN

Was Unternehmen für den Einstieg brauchen

Für den ersten KI-Agenten braucht ein mittelständisches Unternehmen weder eine KI-Abteilung noch eigene Entwickler. Es braucht Wissen in der Führung, eine gute Datenbasis, klare Verantwortlichkeiten und von Anfang an eine gemeinsame Plattform mit Überblick.

Wissen in der Führung

Geschäftsführung und Führungskräfte sollten verstehen, was KI-Agenten können und was nicht. Dazu gehört, dass KI wie Menschen Fehler macht und deshalb Prüfungen und Grenzen braucht. Für den Anfang reicht oft eine kurze Schulung.

Gute Datenbasis

Agenten arbeiten mit digitalen Daten. Für den Einstieg genügt, was ohnehin digital vorliegt, also Mails, PDF-Dokumente, Tabellen und Daten aus vorhandenen Systemen, die der Agent lesend abruft. Später werden Anbindungen an Kernsysteme und weitere Software sinnvoll.

Klare Verantwortung

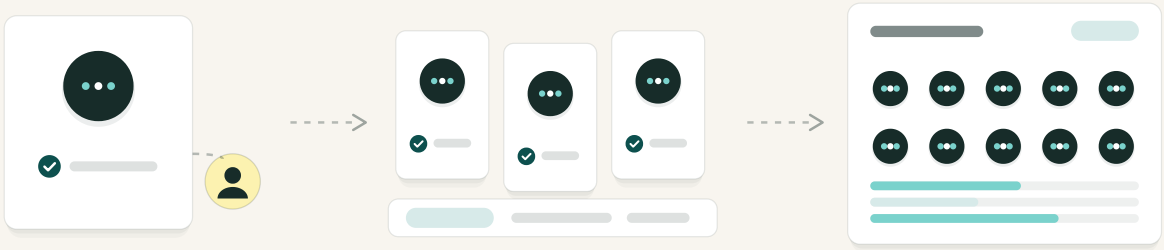
Jeder Agent hat eine verantwortliche Person, die ihn versteht, ändern und notfalls anhalten kann. Die IT sollte festlegen, worauf Agenten zugreifen dürfen, und die Geschäftsführung sollte über Budgets und Grenzen entscheiden.

Regeln für alle Agenten

Rechte, Freigaben, Budgets und Protokolle legt das Unternehmen einmal fest, nicht für jedes Projekt neu. Dann geht jeder weitere Agent schneller in Betrieb.

Eine gemeinsame Plattform

Bereits ab dem ersten Agenten sollte man auf eine Plattform setzen, denn sie bietet die Transparenz, welche Agenten es gibt, wer sie verantwortet, was sie kosten und was sie getan haben. Eine gemeinsame Plattform verhindert, dass in jeder Abteilung eine eigene Insellösung entsteht.



Erster Agent
eine Aufgabe, ein Mensch gibt frei.

Drei Agenten
gemeinsame Regeln, je Agent eine verantwortliche Person.

Zehn Agenten
eine Plattform mit Überblick über Kosten und Ergebnisse.

ONLINE-CHECK

Der Online-Check zeigt in wenigen Minuten, wo das eigene Unternehmen steht und welcher Schritt als Nächstes passt. Zum Check: scalan.ai/agentic-ai-check

UMSETZEN

Zehn Empfehlungen für den Einstieg

Unsere zehn Empfehlungen fassen zusammen, wie ein mittelständisches Unternehmen in rund drei Monaten seinen ersten KI-Agenten von der Idee bis in den Betrieb bringen kann.

1 Mit einem geeigneten Vorgang beginnen

Am Anfang steht nicht die Technik, sondern eine Aufgabe, die viel Zeit kostet und die niemand gern erledigt.

2 Vorschläge im Fachbereich sammeln

Wer die Arbeit täglich macht, kennt die besten Kandidaten. Unsere Scorecard hilft bei der Auswahl (Seite 6).

3 Den heutigen Aufwand messen

Zwei Wochen lang Menge und Dauer festhalten, bevor der Agent startet. So lässt sich der Nutzen später belegen.

4 Lesend anbinden, schreibend später

Lesezugriff auf Postfach, Ablage, CRM oder Ticketsystem macht den Agenten von Anfang an nützlich. Schreibrechte in Kernsystemen folgen erst, wenn er sich bewährt hat (Stufe 5 der Autonomie-Leiter).

5 Mit Human-in-the-Loop beginnen

Der Agent entwirft, ein Mensch prüft und gibt frei. Das entspricht den Stufen 1 bis 3 der Autonomie-Leiter (Seite 4).

6 Verantwortung benennen

Für jeden Agenten gibt es eine Person in der Abteilung, die ihn versteht, ändern und anhalten kann.

7 Governance-Regeln festlegen

Freigaben, Budgets und Protokolle gelten für alle Agenten. Rechte bekommt jeder Agent nur so viele, wie seine Aufgabe verlangt.

8 Daten schützen

Verarbeitung in der EU, kein Training mit eigenen Daten und vollständige Prozesstransparenz sollten von Anfang an gegeben sein.

9 Menschen mitnehmen

Betriebsrat und Beschäftigte früh informieren und schulen. Agenten übernehmen Routinen, die Verantwortung bleibt beim Menschen.

10 Nach 90 Tagen entscheiden

Mit den gemessenen Werten entscheiden, ob der Agent bleibt, angepasst oder beendet wird, und den nächsten Anwendungsfall angehen.

GRAFIK Der Weg in 90 Tagen



Woche 1 bis 2
Anwendungsfall auswählen, Aufwand messen, Regeln und Zugänge festlegen

Woche 3 bis 6
Agent beschreiben, mit echten Fällen testen, mit Freigabe starten

Woche 7 bis 12
im Betrieb begleiten, Werte messen, nachbessern

Woche 13
entscheiden und den nächsten Anwendungsfall wählen

HERAUSGEBER

So unterstützt SCALAN

KI-Agenten können im Mittelstand schon mit der ersten Aufgabe Arbeit abnehmen und das Unternehmen effizienter machen. Die Empfehlungen dieses Whitepapers lassen sich am einfachsten mit einer Plattform umsetzen, die Sicherheit, Governance, Transparenz und einfache Anwendung verbindet. SCALAN ist eine solche Plattform für agentische Prozessautomatisierung aus Deutschland.

WIE SCALAN DIE EMPFEHLUNGEN DIESES WHITEPAPERS UMSETZT

Sicherheit

Alle Daten sind verschlüsselt und liegen in Frankfurt. Mit SCALAN werden Daten nur mit KI-Modellen in der EU verarbeitet und nicht für Trainingszwecke genutzt. SCALAN verfolgt eine Zero Data Retention und speichert keine Eingaben und Ergebnisse bei Modellanbietern. Jeder KI-Agent ist in sich gekapselt. Eingehende Inhalte wie Mails liegen in einem getrennten Speicher und erreichen den Agenten nicht als Anweisung. Manipulationsversuche blockiert das System.

→ Setzt um: Leitplanke 3 · Empfehlung 8

Einfache Anwendung

Der Anwender beschreibt den gewünschten Ablauf in normaler Sprache als Anweisung an den KI-Agenten. Ein KI-Assistent hilft beim Beschreiben. Dadurch gelingt ein niederschwelliger, einfacher Einstieg in das Thema KI-Automatisierung.

→ Setzt um: Empfehlungen 1, 2 und 4 · Voraussetzungen

Governance

Für alle KI-Agenten gelten zentrale Regeln. Die Organisation legt fest, welche Handlungen KI-Agenten ausführen dürfen, und die Plattform sperrt alle weiteren. Verschiedene Budgettöpfe (etwa je Durchlauf, Agent und Abteilung) sowie ein Sofortstopp sind eingebaut. Verschiedene Rollen und Rechte im System gewährleisten nur befugte Handlungen.

→ Setzt um: Autonomie-Leiter · Leitplanken 1, 2 und 4 · Empfehlungen 5 bis 7

Transparenz

Jede Ausführung wird mit Eingabe, Gedankengängen der KI, Entscheidungen, Ergebnis und Freigaben manipulationssicher protokolliert. Ein Protokoll zeigt alle Agenten mit ihren Ausführungen und ihrem Verbrauch. So belegt das Unternehmen seine Sorgfalt und misst den Business Case mit echten Zahlen statt mit Schätzungen.

→ Setzt um: Leitplanke 5 · Empfehlungen 3 und 10 · Business Case

NACHWEISE Vertrag zur Auftragsverarbeitung · ISO 27001 · Rechenzentrum mit BSI-C5-Testat · Zero Data Retention

Das Angebot

Plattform: KI-Agenten unternehmensweit einfach und sicher betreiben.

Fertige KI-Agenten: für häufige Aufgaben, etwa das Sortieren eingehender Mails.

Maßgeschneiderte Automatisierungen: für anspruchsvolle Aufgaben, gemeinsam mit Ihnen gebaut.

Beratung: von der Auswahl der Anwendungsfälle bis zur Einführung im Team.

Aus der Praxis

Für ein produzierendes Unternehmen mit hohen Schutzanforderungen entstand auf SCALAN in wenigen Tagen ein Agent, der aus über 13.500 Rechnungen die Inventurliste erstellt.[10] Bei OMR Reviews bewerten Kunden SCALAN mit 4,9 von 5 Sternen.

ÜBER SCALAN

SCALAN ist eine Plattform für agentische Prozessautomatisierung der MTC Solutions GmbH mit Sitz in München.

DER NÄCHSTE SCHRITT

Ein erstes Gespräch dauert 20 Minuten. Wer zunächst mehr über KI-Agenten erfahren möchte, besucht die kostenlose KI-Sprechstunde.

Gespräch vereinbaren
scalan.ai/contact

KI-Sprechstunde
scalan.ai/ki-sprechstunde

ANHANG

Quellen und Begriffe

Quellen

Alle Links wurden im November 2026 abgerufen.

1 Bitkom: KI in der deutschen Wirtschaft, 14.09.2026 (603 Unternehmen ab 20 Beschäftigten). bitkom.org

2 Destatis: Mikrozensus 2024, 03.09.2025. presseportal.de

3 McKinsey: The State of AI in 2026, August 2026, über FM Magazine. fm-magazine.com

4 Herausgeber: vier Gespräche mit Führungskräften mittelständischer Unternehmen, August bis Oktober 2026, unveröffentlicht.

5 Gartner: Prognose zu Agentenprojekten bis 2027, 25.06.2025. gartner.com

6 Verordnung (EU) 2024/1689 über künstliche Intelligenz (KI-Verordnung). eur-lex.europa.eu

7 Verordnung (EU) 2026/1744 (Digital-Omnibus KI), in Kraft seit 27.07.2026. eur-lex.europa.eu

8 Datenschutz-Grundverordnung, Art. 22 und 28. eur-lex.europa.eu

9 Betriebsverfassungsgesetz, § 87 Abs. 1 Nr. 6. gesetze-im-internet.de

10 Herausgeber: Kundenprojekt Inventur, Oktober 2026, unveröffentlicht.

Begriffe

Agentic AI
englischer Begriff für KI-Systeme, die Aufgaben selbstständig erledigen, dabei Tools und Systemanbindungen nutzen und die Fähigkeit zur Selbstheilung bei Fehlern besitzen.

Anwendungsfall
eine Aufgabe, die ein KI-Agent übernehmen soll.

Autonomie-Leiter
sechs Stufen, die festlegen, wie viel ein Agent allein tun darf, welche Rechte er dafür bekommt und wie Menschen ihn kontrollieren (Seite 4).

CRM
Software für Kundenbeziehungen, in der Kontakte, Anfragen und Angebote liegen.

ERP
Software für Warenwirtschaft, Einkauf, Produktion und Buchhaltung, meist das wichtigste Kernsystem.

Freigabe
Ein Mensch bestätigt ein Ergebnis des Agenten, bevor es nach außen geht.

KI-Agent
KI-System, das eine Aufgabe nach den Regeln des Unternehmens von Anfang bis Ende bearbeitet.

KI-Chat
KI-Anwendung, die Fragen beantwortet und Texte und weitere Medien entwirft, aber nicht selbst handelt.

KI-Verordnung der EU
EU-Gesetz über künstliche Intelligenz, englisch AI Act. Es trat 2024 in Kraft und gilt schrittweise.

Kernsystem
zentrale Software eines Unternehmens, etwa Warenwirtschaft, Buchhaltung oder ein Fachverfahren.

Protokoll
Aufzeichnung jeder Ausführung eines Agenten mit Eingang, Ergebnis und Freigabe.

Vertrag zur Auftragsverarbeitung
Vertrag nach der Datenschutz-Grundverordnung, der regelt, wie ein Dienstleister personenbezogene Daten im Auftrag verarbeitet.

Impressum

Herausgeber: MTC Solutions GmbH (SCALAN), München. Büroanschrift: Hirtentäschelweg 2, 81377 München
Ansprechpartner: Tobias Veit-Seidl
Kontaktaufnahme per E-Mail bitte an hello@scalan.ai

Dieses Whitepaper gibt den Stand vom November 2026 wieder und ersetzt keine Rechtsberatung. Die Rechenbeispiele beruhen auf offen genannten Annahmen und ersetzen keine Messung im eigenen Unternehmen.