abamix
AI. Applied. Governed.

MARKTANALYSE · NOVEMBER 2026

Agentic AI in deutschen Unternehmen

Elf, sechsunddreißig, eins: Was die Zahlen zu KI-Agenten messen und was sie offenlassen

AUTOR Prof. Dr. Amadou Sienou

VERSION 1.1

DATUM 11.11.2026

STATUS Freigegeben

ÜBERSICHT

Inhalt

	Kernaussage	3
	Executive Summary	4
1	Drei Zahlen, drei Fragen	5
2	Was als KI-Agent zählt	8
3	Die Evidenz zur Verbreitung	10
4	Warum die Befunde auseinanderliegen	13
5	Die Lücke zwischen Pilot und Betrieb	16
6	Ein Modell zur Einordnung von Agenten	19
7	Regulierung und Mitbestimmung	23
8	Entscheidungen vom Pilot bis zum Betrieb	25
9	Lieferantenbestätigungen im Einkauf	27
10	Welche Daten für ein belastbares Lagebild fehlen	30
11	Fazit	32
12	So unterstützt abamix	33
	Quellen	34

Kernaussage

Zählen Sie Fälle, nicht Agenten. Elf, sechsunddreißig, eins: Drei Studien liefern drei Prozentwerte zu KI-Agenten und beantworten drei verschiedene Fragen. Bitkom zählt, wer unter den mit KI befassten Unternehmen Agenten einsetzt. eco und Civey zählen, wie breit Agenten nach eigener Angabe verteilt sind. Lünendonk zählt, wer sie durchgängig in mehreren Kernprozessen betreibt. Die amtliche Statistik erhebt 2025 keine Agenten. Für eine Investitionsentscheidung zählt deshalb keine nationale Quote, sondern eine Zahl aus dem eigenen Prozess: die Vollkosten je korrekt abgeschlossenem Fall, gemessen in einem steuerbaren Betrieb.

Executive Summary

Agenten sind in deutschen Unternehmen angekommen. Wie viele davon verlässlich Arbeit erledigen, misst niemand. Bitkom meldet 11 % Agenteneinsatz unter Unternehmen, die KI nutzen, planen oder diskutieren [1]. eco und Civey berichten 36 % Einsatz, davon 25 % in einzelnen Abteilungen und 11 % flächendeckend [2]. Lünendonk findet unter 180 Groß- und Mittelstandsunternehmen im DACH-Raum 1 % mit durchgängiger Integration in mehrere Kernprozesse [3]. Die Werte widersprechen sich nicht. Sie messen verschiedene Dinge.

Drei Befunde prägen das Lagebild. Erstens liegt Deutschland bei der allgemeinen KI-Nutzung mit 26 % über dem EU-Durchschnitt von 20 %, eine Agentenkategorie erhebt die amtliche Statistik aber nicht [9]. Zweitens bleibt die Skalierung auch international schmal: Weltweit berichten 23 % der Befragten von skalierten Agenten in mindestens einer Funktion, in keiner einzelnen Funktion jedoch mehr als 10 % [12]. Drittens verschiebt die Verordnung (EU) 2026/1744 die Hochrisikopflichten des AI Act auf Dezember 2027 und August 2028 [26, 27]. Das schafft Zeit für steuerbare Betriebsmodelle, aber keinen Aufschub für Sicherheit und Mitbestimmung.

Entscheidung für die Geschäftsleitung. Finanzieren Sie einen abgegrenzten Prozess mit gemessener Ausgangslage und klaren Eingriffsrechten. Geben Sie den Regelbetrieb erst frei, wenn echte Fälle, bekannte Ausnahmen und eine getestete Rückfalllösung stabil laufen. Entscheiden Sie über eine Ausweitung anhand der Vollkosten je korrekt abgeschlossenem Fall.

Zentrale Unsicherheit

Für den Anteil überprüfbar produktiver und skalierter Agentensysteme in Deutschland liegt keine repräsentative Betriebsstatistik vor. Alle verfügbaren Agentenquoten beruhen auf Selbstauskünften.

KAPITEL

01

Drei Zahlen, drei Fragen

Die meistzitierten Zahlen zu KI-Agenten beantworten selten die Frage, die eine Geschäftsleitung stellt.

Die Geschäftsleitung will wissen, ob ein Agent im eigenen Prozess verlässlich und wirtschaftlich arbeitet. Die Umfragen fragen, ob Agenten eingesetzt, geplant oder diskutiert werden. Zwischen beiden Fragen liegt die eigentliche Arbeit: Integration, Prüfung, Ausnahmebehandlung und Verantwortung.

11 %

Setzt das Unternehmen Agenten ein?

Bitkom [1]

36 %

nach eigener Angabe zum Einsatz

davon 11 % flächendeckend

1 %

Tragen Agenten durchgängig mehrere Kernprozesse?

Lünendonk [3]

Abbildung 1: Elf, sechsunddreißig, eins: drei Studien, drei Fragen

Die Messtreppe

Die drei Zahlen lassen sich drei Stufen zuordnen. Jede Stufe misst etwas anderes. Die Werte stammen aus verschiedenen Studien mit verschiedenen Grundgesamtheiten und bilden deshalb keinen Trichter.

Stufe	Frage	Wert	Bezugsgruppe
Einsatz	Setzt das Unternehmen Agenten ein?	11 %	Deutschland, Unternehmen ab 20 Beschäftigten mit KI-Bezug [1]
Verbreitung	In welchem Umfang kommen Agenten nach eigener Angabe zum Einsatz?	36 %, davon 11 % flächendeckend	Deutschland, 500 Unternehmen, online [2]
Kernprozess	Tragen Agenten durchgängig mehrere Kernprozesse?	1 %	DACH, 180 Groß- und Mittelstandsunternehmen [3]

Zum Vergleich: Die allgemeine KI-Nutzung liegt laut amtlicher Statistik bei 26 % der Unternehmen ab zehn Beschäftigten [9]. Sie misst den Zugang zu KI, nicht den Einsatz von Agenten.

Reichweite und Betriebsleistung

Die Verfügbarkeit einer Funktion misst Reichweite. Der Anteil korrekt und fristgerecht bearbeiteter Fälle bei bekanntem Risiko misst betriebliche Leistung. Für Investitionsentscheidungen ist diese Unterscheidung wesentlich, denn der Markt kann bei der Zahl zugänglicher Agenten wachsen, ohne bei der Zahl verlässlich automatisierter Vorgänge zu wachsen.

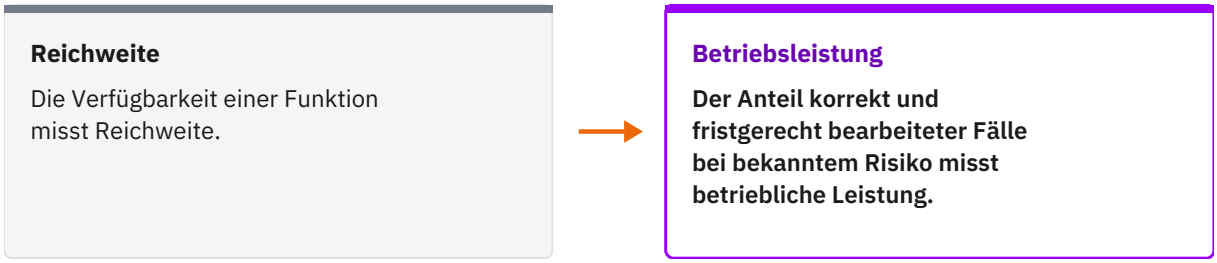


Abbildung 2: Reichweite und Betriebsleistung

Leseregel

Allgemeine KI-Nutzung, Agentennutzung, Regelbetrieb und Skalierung sind unterschiedliche Messgrößen. Diese Analyse bewertet jede Zahl auf der Ebene, auf der sie erhoben wurde, und mittelt keine Quoten verschiedener Studien.

Untersuchungsrahmen und Methode

Die Analyse wertet öffentlich zugängliche Primärquellen und dokumentierte Sekundärquellen bis zum 11. November 2026 aus. Sie vergleicht Deutschlanderhebungen, nutzt eine DACH-Studie für Reifestufen und zieht EU-Statistik, internationale Befragungen, technische Quellen und Projektbeispiele zur Einordnung heran. Erhebungszeitpunkt, Grundgesamtheit, Frageformulierung, Antwortkategorien und Art des Nachweises werden gemeinsam beurteilt. Werte von Herstellern, Beratungen und Analystenhäusern sind als solche gekennzeichnet. Die Analyse umfasst keine eigene Befragung und keine gepoolte Schätzung.

KAPITEL

02

Was als KI-Agent zählt

> **Wer „Agent“ sagt, kann ein Produktfeature, einen Ticketbearbeiter oder eine Prozesskette meinen.**
>
> Für die Reifeanalyse zählt das beobachtbare Verhalten im Geschäftsprozess. Produktnamen und die Zahl bereitgestellter Lizenzen sagen darüber wenig.

Arbeitsdefinition

Ein KI-Agent verfolgt ein vorgegebenes Ziel und wählt innerhalb festgelegter Grenzen anhand des Kontexts die nächsten Schritte oder Werkzeuge. Das System kann auf Unternehmensdaten zugreifen, Zwischenergebnisse auswerten und Aktionen auslösen. Der Handlungsspielraum kann auf lesenden Zugriff, interne Änderungen oder externe Aktionen begrenzt sein. Eine menschliche Freigabe für bestimmte Aktionen ist mit agentischem Verhalten vereinbar. Anthropic unterscheidet vorab codierte Abläufe von Agenten, bei denen das Modell seine Schritte und Werkzeuge dynamisch steuert [15].

Form	Beobachtbares Verhalten	Beispiel im Einkauf
Assistenz	Liefert auf Anfrage Text oder Analyse.	Eine Lieferantenbestätigung zusammenfassen.
KI-Workflow	Folgt vorgegebenen Schritten und nutzt KI für eine Teilaufgabe.	Felder aus einem PDF extrahieren und per Regel abgleichen.
KI-Agent	Wählt Schritte oder Werkzeuge anhand des Falls.	Bestellung suchen, fehlende Angaben prüfen, Klärungsweg wählen.

Agentische Elemente und feste Prozessschritte kommen oft im selben System vor. Ein Modell kann aus mehreren zulässigen Suchwegen wählen, während eine feste Regel die Änderung einer Bestellung sperrt. Eine Freigabe begrenzt die Wirkung des Systems, ohne seine Fähigkeit zur eigenständigen Bearbeitung innerhalb dieses Rahmens aufzuheben.

Jede Studie zählt einen anderen Agenten

Die Studien verwenden unterschiedliche Definitionen. Befragte können deshalb sehr verschiedene Systeme meinen, wenn sie „Agent“ ankreuzen.

Quelle	Was als Agent gilt
Bitkom [1]	Ein Agent „handelt selbstständig, indem er zum Beispiel Preisvergleiche durchführt, Angebote einholt und auch Entscheidungsoptionen ausarbeitet“.
eco und Civey [2]	„Autonome KI-Agenten“; die Pressemitteilung veröffentlicht keine Abgrenzung.
McKinsey [12]	Systeme auf Basis von Foundation Models, die mehrstufige Arbeitsabläufe planen und ausführen.
Lünendonk [3]	Reifestufen von Exploration über Pilot bis zur durchgängigen Integration in Kernprozesse.

Gartner warnt zusätzlich vor „Agent Washing“: Von den Tausenden Anbietern mit Agentenangebot hält das Analystenhaus nur „about 130“ für echte Agentenanbieter [13]. Das ist eine Einschätzung, keine Zählung. Sie erklärt aber, warum Selbstauskünfte zur Agentennutzung auch umbenannte Assistenzfunktionen enthalten können.

> **Was das für Sie heißt.**
>
> Fragen Sie bei jeder Agentenzahl zuerst, welche Systeme die Befragten gemeint haben können.

KAPITEL

03

Die Evidenz zur Verbreitung

> **Deutschland nutzt KI breiter als der EU-Durchschnitt; für Agenten gibt es nur Umfragen mit abweichender Basis.**
>
> Die folgende Tabelle führt die Agentenbefunde mit ihren Aussagegrenzen zusammen.

Entscheidungsfolge

Die allgemeine KI-Verbreitung zeigt, wie viele Unternehmen Zugang zu ersten Anwendungen haben. Sie liefert keine Quote für delegierte Prozessschritte und keine Aussage über die Qualität der Ausführung.

Agentenbefunde für Deutschland und DACH

Quelle und Bezugsgruppe	Kernergebnis	Aussagegrenze
Bitkom, 603 Unternehmen ab 20 Beschäftigten, telefonisch, KW 28 bis 33 2026 [1]	57 % nutzen KI. Unter den Unternehmen, die KI nutzen, planen oder diskutieren, setzen 11 % Agenten ein, 29 % planen und 31 % diskutieren den Einsatz. Für 24 % sind Agenten kein Thema.	Basis der Agentenquote sind 95 % der Befragten, nicht alle. Der betriebliche Umfang wird nicht ausgewiesen.
eco und Civey, 500 Unternehmen, online, 18.09. bis 03.10.2026 [2]	25 % Einsatz in einzelnen Abteilungen, 11 % flächendeckend, 18 % Test oder Pilot, 7 % konkret geplant, 33 % kein Einsatz geplant.	Statistischer Fehler je nach Frage 9,1 bis 9,4 Prozentpunkte. Keine veröffentlichte Agentendefinition. Selbstauskunft zum Umfang.
Deutscher Mittelstands-Bund und Salesforce, rund 700 Teilnehmende, Befragung November 2025 [7]	16,6 % nutzen Agenten, gegenüber 8,7 % in der Vorjahreserhebung. 51,2 % nutzen oder testen KI.	Stichprobenziehung und Gewichtung nicht offengelegt. Mitherausgeber ist ein Agentenanbieter.
Lünendonk, 180 IT- und Fachbereichsverantwortliche, gehobener Mittelstand und Konzerne, DACH, telefonisch, April bis Juni 2026 [3, 4]	18 % Exploration oder Test, 58 % Pilot, 19 % Einsatz in einzelnen Aufgabenbereichen, 1 % durchgängig in mehreren Kernprozessen.	Kein Deutschlandwert. Studienpartner sind Beratungs- und IT-Dienstleister. Die genannten Kategorien ergeben zusammen 96 %.

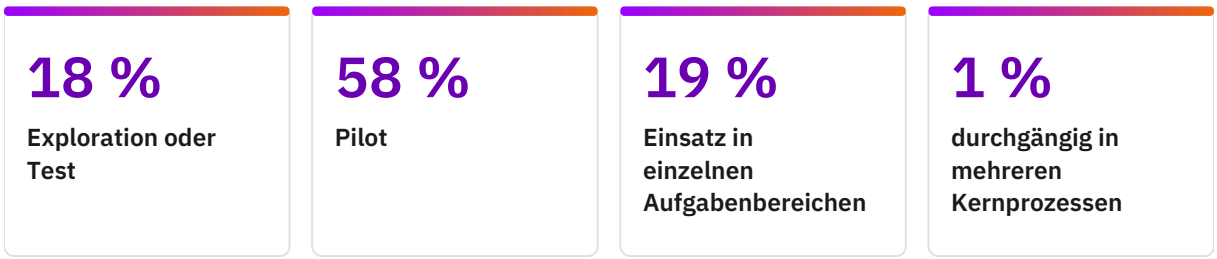


Abbildung 3: Reifestufen in der Lünendonk-Stichprobe (DACH, 180 Unternehmen)

Allgemeine KI-Nutzung als Rahmen

Eurostat weist für 2025 aus, dass 20,0 % der EU-Unternehmen ab zehn Beschäftigten mindestens eine KI-Technologie nutzen, nach 13,5 % im Vorjahr. Deutschland liegt mit 25,97 % auf Rang 8 von 27. Die Spanne reicht von 5,21 %

in Rumänien bis 42,03 % in Dänemark [9]. Die Erhebung ist EU-weit harmonisiert; in Deutschland ist die Teilnahme freiwillig [8]. Sie enthält 2025 keine Agentenkategorie.

Destatis meldet für Deutschland denselben Wert von 26 %, nach Größe 23 % für 10 bis 49 Beschäftigte, 36 % für 50 bis 249 und 57 % ab 250 Beschäftigten [8]. Seit 2025 zählt Destatis nach dem EU-Unternehmensbegriff, der Vergleich mit dem Vorjahreswert ist daher nur eingeschränkt möglich. Das ifo Institut meldet für Mai 2026 54,5 % KI-Nutzung in Geschäftsprozessen, nach 40,9 % im Vorjahr; 16 % planen und 21,6 % diskutieren den Einsatz [10]. Das IAB misst für 2025 in 24 % der Betriebe generative KI, nach 5 % im Jahr 2023; Betriebe ab 200 Beschäftigten liegen bei 48 %, Betriebe unter zehn Beschäftigten bei 21 % [11].

Die Werte unterscheiden sich, weil Einheit, Frage und Zeitpunkt verschieden sind. Eurostat und Destatis zählen Unternehmen und definierte Technologien, ifo fragt nach Nutzung in Geschäftsprozessen, das IAB zählt Betriebe einschließlich Kleinstbetrieben. Keine dieser Quellen misst Agenten.

Internationale Einordnung

McKinsey hat im Juli 2025 weltweit 1.993 Personen aus 105 Ländern befragt. 88 % berichten KI-Nutzung in mindestens einer Funktion. 23 % skalieren ein agentisches System in mindestens einer Funktion, weitere 39 % experimentieren. In keiner einzelnen Funktion berichten mehr als 10 % eine Skalierung von Agenten [12]. Die Basis sind Befragte, nicht Unternehmen, und eine Deutschlandauswertung fehlt.

Capgemini meldet für die Produktentwicklung der Automobilindustrie, dass 68 % Agentic AI nutzen oder pilotieren [18]. Laut Studienbericht nutzen 35 % der Hersteller und Zulieferer Agentic AI, weitere 33 % pilotieren [19]; die Pressemitteilung nennt die beiden Werte in umgekehrter Reihenfolge [18]. Befragt wurden im Juli 2026 400 Hersteller, 160 Zulieferer der ersten Ebene und 240 Technologieanbieter in zwölf Ländern. Nur 5 % berichten eine voll ausgereifte KI-Governance [18].

KAPITEL

04

Warum die Befunde auseinanderliegen

> **Die Abstände zwischen den Studien entstehen vor der ersten Antwort: bei Basis, Frage und Erhebungsweg.**
>
> Ein Durchschnitt der Quoten hätte deshalb keine definierte Bezugsgröße.

Konsequenz

Verwenden Sie jede Quote als Ergebnis ihrer Studie. Eine gemeinsame nationale Adoptionsquote für Agenten lässt sich aus den veröffentlichten Daten nicht ableiten.

Drei Prüffragen für jede Agentenzahl

Jede Agentenzahl lässt sich mit drei Fragen einordnen: Wer wurde gefragt? Was zählt als Agent? Was heißt Einsatz? Die Definitionstabelle in Kapitel 2 beantwortet die zweite Frage, die folgende Übersicht die erste und die dritte.

Studie	Wer wurde gefragt	Basis der Agentenfrage	Was als Einsatz zählt
Bitkom [1]	Unternehmen ab 20 Beschäftigten; telefonisch; Juli bis August 2026	KI-befasste Unternehmen	Status: im Einsatz, geplant, diskutiert
eco und Civey [2]	Unternehmen, Größe nicht ausgewiesen; online, quotiert und gewichtet; September bis Oktober 2026	alle Befragten	Umfang: einzelne Abteilungen oder flächendeckend
Lünendonk [3]	Verantwortliche aus gehobenem Mittelstand und Konzernen; telefonische Interviews; April bis Juni 2026	alle Befragten	Reifestufe bis zur durchgängigen Integration in Kernprozesse
Eurostat [9]	Unternehmen ab 10 Beschäftigten; amtliche Erhebung, in Deutschland freiwillig; 2025	keine Agentenfrage	Nutzung einer KI-Technologie

Die Differenz zwischen 11 und 36 Prozent

Bitkom weist 11 % für eine Teilgruppe aus. eco und Civey melden 36 % als Summe aus Abteilungsnutzung und flächendeckendem Einsatz in ihrer Stichprobe. Bitkom beschreibt Agenten anhand selbstständiger Handlungen. eco fragt nach dem Umfang, in dem „autonome KI-Agenten“ zum Einsatz kommen, ohne eine technische Abgrenzung zu veröffentlichen [1, 2].

Auch nach gedanklicher Angleichung der Basis bliebe ein deutlicher Abstand. Welche Anteile auf Frageverständnis, Auswahl und Gewichtung, Zusammensetzung oder Erhebungszeitraum entfallen, lässt sich ohne vergleichbare Mikrodaten nicht bestimmen. Die eco-Fehlerspanne von 9,1 bis 9,4 Prozentpunkten beschreibt die Unsicherheit innerhalb einer Erhebung. Messunterschiede zwischen Studien quantifiziert sie nicht [2].

Reichweite und Eingriffstiefe sind verschiedene Größen

Ein Rechercheagent kann in vielen Abteilungen verfügbar sein und rein lesend arbeiten. Ein Agent in einem einzelnen Einkaufsteam kann dagegen Bestellungen zuordnen, Prüfungen auslösen und Klärungsfälle eröffnen. Die eco-Kategorie „flächendeckend“ misst berichtete Verbreitung. Lünendonks 1 % verlangt durchgängige Integration in mehrere Kernprozesse. Beide Angaben können gleichzeitig zutreffen [2, 3].

Aussage	Sicherheit der Einordnung
KI insgesamt ist breit in die Unternehmenspraxis vorgedrungen.	Gut gestützt durch amtliche und nichtamtliche Erhebungen; das Niveau hängt von Abgrenzung und Einheit ab. [8–11]
Unternehmen setzen Agenten ein und erproben weitere Anwendungen.	Mehrere Erhebungen zeigen Aktivität; die absoluten Quoten weichen erheblich voneinander ab. [1–3, 7]
Die Agentennutzung im Mittelstand hat sich binnen eines Jahres etwa verdoppelt.	Innerhalb einer Studienreihe berichtet, von 8,7 % auf 16,6 %; Stichprobe nicht offengelegt. [7]
Der Anteil produktiv skalierter Agenten in Deutschland hat einen bestimmten Wert.	Offen. Es fehlen eine gemeinsame Definition und repräsentative Betriebsdaten.
Die Nutzung stieg von September auf Oktober um 25 Punkte.	Nicht ableitbar. Erhebungen und Bezugsgrößen unterscheiden sich. [1, 2]

KAPITEL

05

Die Lücke zwischen Pilot und Betrieb

> **Die meisten Agenten stehen im Pilot, und der Übergang in den Betrieb ist der Engpass.**
>
> In der Lünendonk-Stichprobe befinden sich 58 % im Pilot und weitere 18 % in Exploration oder Test [3]. 66 % der Befragten haben weniger als ein Viertel ihrer KI-Pilotprojekte in den Regelbetrieb überführt [5]. Die veröffentlichten Texte beziehen diese Zahl teils auf KI-Pilotprojekte allgemein, teils auf pilotierte Agenten [5, 6]. Sie wird hier deshalb auf KI-Pilotprojekte bezogen, nicht ausschließlich auf Agenten.

Was den Übergang bremst

Als Hemmnisse nennt Lünendonk [3]:

- IT-Infrastruktur,
- fehlende Integrationsschichten und Datenanbindung,
- Sicherheits- und Datenschutzbedenken,
- fehlendes Fachpersonal,
- unkoordinierte Initiativen.

98 % der Befragten wollen in Datenqualität und Datenintegration investieren, 94 % in Orchestrierungsplattformen. 73 % erwarten, dass Agenten bestehende Anwendungen ergänzen statt ablösen [3]. Capgemini kommt in der Automobilentwicklung zu einem verwandten Befund. Dort sehen 60 % Verzögerungen vor allem in Prozessineffizienzen, nicht in der Technik. 45 % der Hersteller haben noch keine umfassende, bereichsübergreifende KI-Strategie [19].

Abbruch- und Erfolgsquoten richtig lesen

Quelle	Befund	Art der Aussage
Gartner, Juni 2025 [13]	Mehr als 40 % der Agentic-AI-Projekte werden bis Ende 2027 abgebrochen, wegen steigender Kosten, unklarem Nutzen oder unzureichender Risikokontrollen.	Analystenprognose, keine gemessene Quote; gestützt unter anderem auf eine Umfrage unter 3.412 Webinar-Teilnehmenden.
MIT Project NANDA, Juli 2025 [14]	95 % der Organisationen erzielen keinen messbaren Ertrag aus generativer KI. Bei Unternehmenslösungen evaluieren 60 %, 20 % pilotieren, 5 % erreichen den Produktivbetrieb.	Vorläufiger, nicht begutachteter Bericht zu generativer KI allgemein; Interviews, Konferenzbefragung und öffentliche Fälle; enges Erfolgskriterium.
Lünendonk, 2026 [3, 5]	66 % bringen weniger als ein Viertel ihrer KI-Piloten in den Regelbetrieb.	Projektquote je Unternehmen in einer nicht repräsentativen DACH-Stichprobe.
Deutscher Mittelstands-Bund und Salesforce [7]	Weniger als 5 % haben KI-Versuche eingestellt.	Eingestellte KI-Versuche auf Unternehmensebene, nicht abgebrochene Agentenprojekte.

Die Werte widersprechen sich nur scheinbar. Ein Unternehmen kann KI weiter nutzen und trotzdem die meisten Piloten nicht in den Betrieb bringen. Gartner zählt Projekte, die Mittelstandsstudie Unternehmen. Für Deutschland und die EU liegen keine gemessenen Abbruchquoten für Agentenprojekte vor.

Was Agenten in Tests leisten

TheAgentCompany prüft Agenten in einer simulierten Softwarefirma mit 175 Aufgaben aus sechs Rollen, darunter Projektmanagement, Administration und Finanzen [29]. Im Forschungsbericht erledigt das beste Modell 30,3 % der Aufgaben vollständig und erreicht 39,3 % der Teilpunkte, bei Kosten von über 4 US-Dollar je Aufgabe [29]. Ein öffentliches Leaderboard weist inzwischen 42,9 % als Bestwert aus [32]. Auch dieser Wert lässt die Mehrheit der Aufgaben unerledigt. Die Simulation ist vereinfacht und bildet Berechtigungen, Ausnahmen und Fehlerfolgen eines echten Betriebs nicht ab.

Projektbelege aus dem Feld

Analysearbeit.

Die Deutsche Telekom berichtet aus ersten Pilotprojekten: In einem Projekt im öffentlichen Sektor sank der Aufwand für Recherche und Erstellung umfangreicher interner Vermerke von rund sechs Stunden auf unter eine Stunde [16]. Ein weiteres Beispiel aus einem Krankenhaus nennt keine Zeitersparnis. Messmethode, Fallzahl und Fehlerquote nennt die Mitteilung nicht.

Industrielles Engineering.

Siemens hat den Eigen Engineering Agent nach eigener Angabe mit mehr als 100 Unternehmen in 19 Ländern pilotiert und am 20. April 2026 allgemein verfügbar gemacht [17]. Der Hersteller nennt eine zwei- bis fünffach schnellere Ausführung, bis zu 50 % Effizienzgewinn und bis zu 80 % höhere Lösungsqualität. Diese Werte sind nicht unabhängig geprüft, und „pilotiert“ ist nicht gleichbedeutend mit dauerhaftem Betrieb.

Evidenzgrenze

Die Fallbelege stützen technische Machbarkeit. Keiner nennt Fehlerquoten, Eingriffsraten oder Kosten je Vorgang. Für einen belastbaren Vergleich wären Ausgangswerte, vergleichbare Fallgruppen und vollständige Kosten erforderlich.

Was das für Sie heißt.

Planen Sie den Übergang vom Pilot in den Betrieb als eigenes Vorhaben mit Verantwortung und vorab vereinbarter Kennzahl, nicht als Abschluss des Piloten.

KAPITEL

06

Ein Modell zur Einordnung von Agenten

> **Ein Agent ist so reif wie sein schwächster Betriebsnachweis, nicht wie sein bester Testlauf.**
>
> Das folgende Modell bewertet einzelne Anwendungen. Es verbindet den Status im Betrieb mit prüfbaren Nachweisen und ist keine Hochrechnung aus den Studien. Die Autonomie wird separat beschrieben, weil ein breit eingeführter Agent bewusst geringe Rechte haben kann.

Stufe	Betriebsstatus	Nachweis für die Einstufung
0	Exploration	Aufgabe, Prozessverantwortung und Einsatzgrenzen sind beschrieben. Tests bleiben in einer isolierten Umgebung.
1	Pilot	Reale oder realitätsnahe Fälle laufen befristet. Das Fachteam prüft Normalfälle, Ausnahmen und kritische Fehler.
2	Begrenzter Regelbetrieb	Echte Fälle werden fortlaufend in einem abgegrenzten Prozess bearbeitet. Zuständigkeit, Freigaben, Monitoring und Rückfallweg sind eingerichtet.
3	Skalierter Regelbetrieb	Mehrere Teams oder Prozesse nutzen den Agenten dauerhaft. Betriebsnachweise und Qualitätsgrenzen gelten je Einsatzbereich. Änderungen sind kontrolliert.

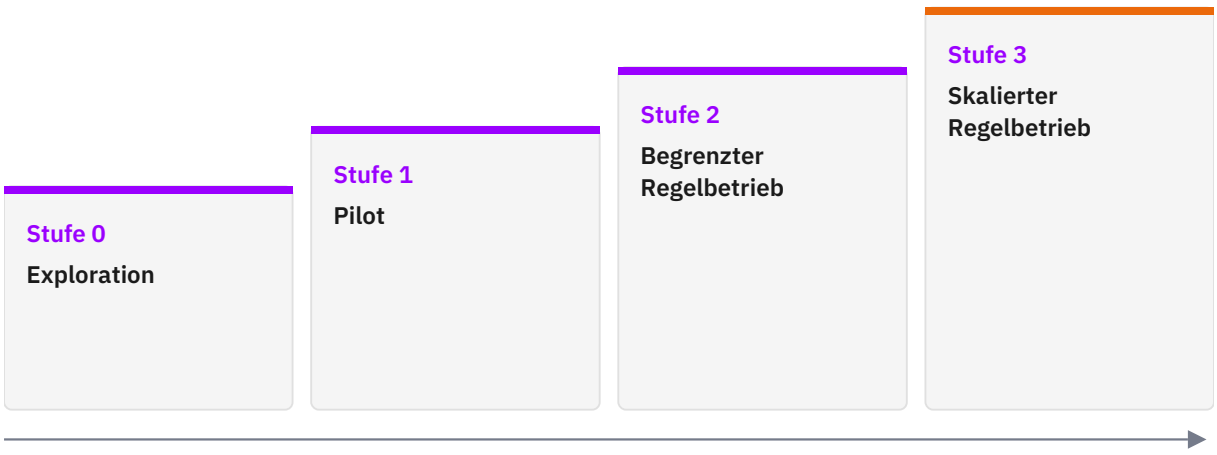


Abbildung 4: Vier Stufen der Betriebsreife eines Agenten

Rechte und Verantwortung

Für jeden Agenten werden erlaubte Aktionen, Systeme und Datenbereiche dokumentiert. Praktische Abstufungen sind lesender Zugriff, Vorschläge mit Freigabe, begrenzte interne Schreibaktionen und externe oder schwer rückgängig zu machende Aktionen. Der Prozessverantwortliche bestimmt die Grenzen je Aktion. So kann derselbe Agent Liefertermine lesen, ein internes Ticket eröffnen und den Versand einer Reklamation zur Freigabe vorlegen. Jeder Agent steht mit Verantwortlichem, Risikoklasse und Steuerungsmodus in einem Register. Freigaben laufen über einen festgelegten Workflow, nicht über Einzelabsprachen.

Sicherheit als Betriebseigenschaft

Der Betrieb braucht eine eigene technische Identität oder eine nachvollziehbare delegierte Identität, restriktive Berechtigungen und ein Protokoll über Systemzugriffe und Aktionen. Anweisungen in einer eingehenden E-Mail oder einem Dokument werden als Daten behandelt. Zugriff und erlaubte Aktionen werden außerhalb des Sprachmodells durchgesetzt. Wiederholte Aufrufe dürfen keine doppelten Buchungen oder Nachrichten erzeugen. Stoppen, Rechte entziehen und manuell weiterarbeiten gehören in den getesteten Rückfallweg.

Diese Anforderungen sind inzwischen in Leitlinien beschrieben, aber noch in keiner verbindlichen Prüfnorm:

Quelle	Beitrag für den Betrieb
OWASP, Dezember 2025 [22]	Top 10 der Risiken agentischer Anwendungen, darunter Zielübernahme (Agent Goal Hijack), Missbrauch von Werkzeugen, Missbrauch von Identitäten und Rechten, Vergiftung von Gedächtnis und Kontext sowie kaskadierende Fehler. Community-Taxonomie, keine Norm.
BSI und ANSSI, August 2025 [23]	Zero-Trust-Prinzipien für LLM-basierte Systeme als Grundlage sicherer agentischer Systeme: minimale Zugriffsrechte, transparente Entscheidungswege, kritische Entscheidungen unter menschlicher Aufsicht.
BSI, Fassung Oktober 2026 [24]	Basisschutz gegen indirekte Prompt Injection: „KI-Agenten wird eine menschliche Bestätigung von sicherheitskritischen Aktionen dringend empfohlen.“
NIST und NCCoE, Februar 2026 [21]	Konzeptpapier zu Identität und Autorisierung von Software- und KI-Agenten: Identifikation, Autorisierung, Delegation, Protokollierung, Nichtabstreitbarkeit und Kontrollen gegen Prompt Injection. Entwurf mit dem Ziel eines Praxisleitfadens.

Die Unternehmen setzen dieselben Schwerpunkte, zumindest in ihren Absichten. In der eco-Befragung würden 47 % eine automatisierte Notabschaltung vorsehen, 45 % eine strikte Rechte- und Rollenvergabe, 37 % Sicherheitsaudits, 32 % ein Monitoring der Ausgaben und 31 % transparente Handlungsprotokolle [2]. Die Antworten beschreiben geplante Maßnahmen, keine eingerichteten Kontrollen.

Bereitschaft ist nicht Berechtigung

> **Wie viel Autonomie ein Unternehmen zulassen würde, sagt nichts darüber, welche Rechte ein Agent tatsächlich hat.**
>
> Die Umfragen messen Bereitschaft. Für den Betrieb zählt die eingerichtete Berechtigung je Aktion.

In der eco-Befragung würden 40 % maximal Zuarbeit zulassen und 34 % eigenständiges Arbeiten unter menschlicher Kontrolle. 13 % würden autonome Entscheidungen in Teilprozessen zulassen und 5 % vollständig autonome Entscheidungen [2]. Civey hat im Auftrag des estnischen e-Residency-Programms 2.000 Gründer, KMU-Geschäftsführer und Selbstständige in Deutschland befragt [30]. 13 % von ihnen lassen die KI bei Routineaufgaben vollständig autonom handeln.

52 % nennen zu weitreichenden Zugriff auf Konten und Daten als größte Sorge, 50 % die unklare Haftung [30]. Der Auftraggeber hat ein Interesse am Thema, und die Grundgesamtheit ist mit Unternehmensumfragen nicht vergleichbar.

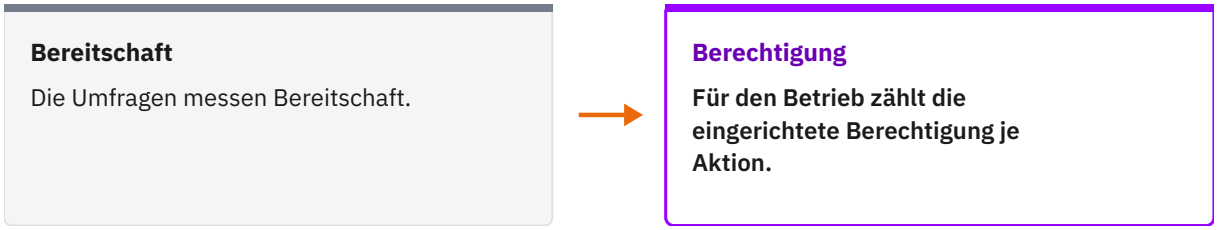


Abbildung 5: Bereitschaft und Berechtigung

Das Vertrauen kann vom Arbeitsschritt abhängen. In der Automobilentwicklung vertrauen 59 % der Befragten Agenten in Forschung und Konzept, aber nur 40 % in der Entwicklung [18].

Für künftige Erhebungen ist deshalb die Reichweite der delegierten Handlung zu dokumentieren. Eine Leseberechtigung und eine Freigabeberechtigung haben unterschiedliche Wirkungen. Welche Rechte ein Unternehmen einräumt, hängt vom Prozess und den Folgen einer fehlerhaften Aktion ab. Eine einheitliche Autonomiestufe für ein ganzes Unternehmen würde diesen Unterschied verdecken.

Ein Betriebsmodell ist steuerbar, wenn Verantwortung, Freigabe, Eskalation und Kennzahlen im laufenden Betrieb nachweisbar sind, nicht erst im Konzept.

KAPITEL

07

Regulierung und Mitbestimmung

> **Der AI Act reguliert Verwendungszwecke, nicht Agenten.**
>
> Eine Agentenfunktion allein entscheidet die Einstufung nicht. Maßgeblich sind der vorgesehene Verwendungszweck, die Rolle des Unternehmens und die geltenden Fristen [25]. Die Angaben in diesem Kapitel geben den Stand vom 11. November 2026 wieder und ersetzen keine Rechtsberatung.

Die geänderte Zeitachse des AI Act

Mit der Verordnung (EU) 2026/1744 vom 8. Juli 2026, dem „Digital Omnibus on AI“, wurden die Fristen der Verordnung (EU) 2024/1689 geändert. Sie wurde am 24. Juli 2026 im Amtsblatt veröffentlicht und ist seit dem 27. Juli 2026 in Kraft [33, 34].

Gilt ab	Pflicht
2. Februar 2025	Verbotene Praktiken (Art. 5) und KI-Kompetenz (Art. 4)
2. August 2025	Pflichten für KI-Modelle mit allgemeinem Verwendungszweck
2. August 2026	Transparenzpflichten nach Art. 50, soweit nicht abweichend geregelt
2. Dezember 2026	Kennzeichnung nach Art. 50 Abs. 2 für bereits am Markt befindliche Systeme
2. Dezember 2027	Hochrisikosysteme nach Anhang III (Art. 6 Abs. 2), bisher 2. August 2026
2. August 2028	Hochrisikosysteme nach Anhang I (Art. 6 Abs. 1), bisher 2. August 2027

Die Änderungsverordnung hat auch Art. 4 abgeschwächt: Anbieter und Betreiber müssen Maßnahmen ergreifen, um ein ausreichendes Maß an KI-Kompetenz zu fördern, statt es sicherzustellen [33, 34].

Anhang III nennt unter anderem Beschäftigung und Personalauswahl sowie die Prüfung der Kreditwürdigkeit [25]. Ein Agent in der Bewerberauswahl berührt damit einen gelisteten Bereich, ein Agent für Lieferantenbestätigungen nicht ohne Weiteres. Die Einstufung im Einzelfall bleibt eine rechtliche Prüfung.

Zuständigkeit in Deutschland

Das Gesetz zur Marktüberwachung und Innovationsförderung von künstlicher Intelligenz (KI-MIG) vom 22. Juli 2026 ist seit dem 29. Juli 2026 in Kraft [28]. Nach § 2 Abs. 1 ist die Bundesnetzagentur die für die Einhaltung der Verordnung (EU) 2024/1689 zuständige Marktüberwachungsbehörde, soweit das Gesetz nichts anderes bestimmt. Für Produkte nach Anhang I bleiben die bisherigen Marktüberwachungsbehörden zuständig, für Finanzdienstleistungen die BaFin. Das Gesetz sieht außerdem mindestens ein KI-Reallabor (§ 13) und ein nicht öffentliches Register für bestimmte Hochrisikosysteme (§ 20) vor [28].

Die Unternehmen erwarten mehr Betroffenheit. In der Bitkom-Befragung sehen sich 37 % als Anwender vom AI Act betroffen, nach 23 % im Vorjahr; weitere 34 % prüfen dies. Die Betroffenen rechnen im Schnitt mit 2,1 Hochrisiko-Systemen [1]. Das ist eine Selbsteinschätzung, keine rechtliche Klassifikation.

Mitbestimmung

Agenten, die Arbeitsvorgänge protokollieren, können technische Einrichtungen im Sinne von § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz sein, die zur Überwachung von Verhalten oder Leistung geeignet sind. Hinzu kommen Unterrichtungsrechte nach § 90 und die Hinzuziehung von Sachverständigen bei KI nach § 80 Abs. 3 [31]. Empirische Daten zur Verbreitung von Betriebsvereinbarungen über KI-Agenten liegen nicht vor.

Das Betriebskonzept hält fest, wer die Einstufung prüft, welche Nachweise erforderlich sind, wann der Betriebsrat beteiligt wird und bei welchen Prozessänderungen erneut geprüft wird.

> **Was das für Sie heißt.**
>
> Nutzen Sie den Aufschub der Hochrisikopflichten, um Einstufung, Nachweise und die Beteiligung des Betriebsrats festzulegen, bevor ein Agent in den Regelbetrieb geht.

KAPITEL

08

Entscheidungen vom Pilot bis zum Betrieb

> **Freigegeben wird ein Prozess, nicht ein Modell.**
> Die Entscheidung über den Regelbetrieb stützt sich auf Prozessdaten aus dem eigenen Haus. Benchmarks und Herstellerangaben ersetzen sie nicht.

Praktische Freigaberegel

Legen Sie Schwellenwerte vor dem Pilot fest. Für kritische Fehler braucht es klare Abbruchregeln. Ein gutes Durchschnittsergebnis kann eine unzulässige Aktion oder einen unbemerkten schweren Fehler verdecken.

Einen Prozess mit klaren Grenzen auswählen

Ein geeigneter Einstieg hat wiederkehrende Fälle, erreichbare Daten und einen Prozessverantwortlichen. Das Team dokumentiert erwartetes Ergebnis, bisherige Bearbeitungszeit, Fehlerarten und Kosten. Es prüft, wo eine feste Regel genügt und wo variable Eingaben oder mehrere mögliche Bearbeitungswege agentisches Verhalten rechtfertigen. Ein hoher Automatisierungsgrad ist keine Voraussetzung für einen wirtschaftlichen Einstieg. Kandidaten werden im Wertstrom verankert, bevor sie bewertet werden. Was nicht in die erste Welle gehört, steht mit Begründung auf einer schriftlichen Zurückstellungsliste; sie macht die Auswahl für Sponsoren nachvollziehbar.

Die Freigabe an Prozessdaten knüpfen

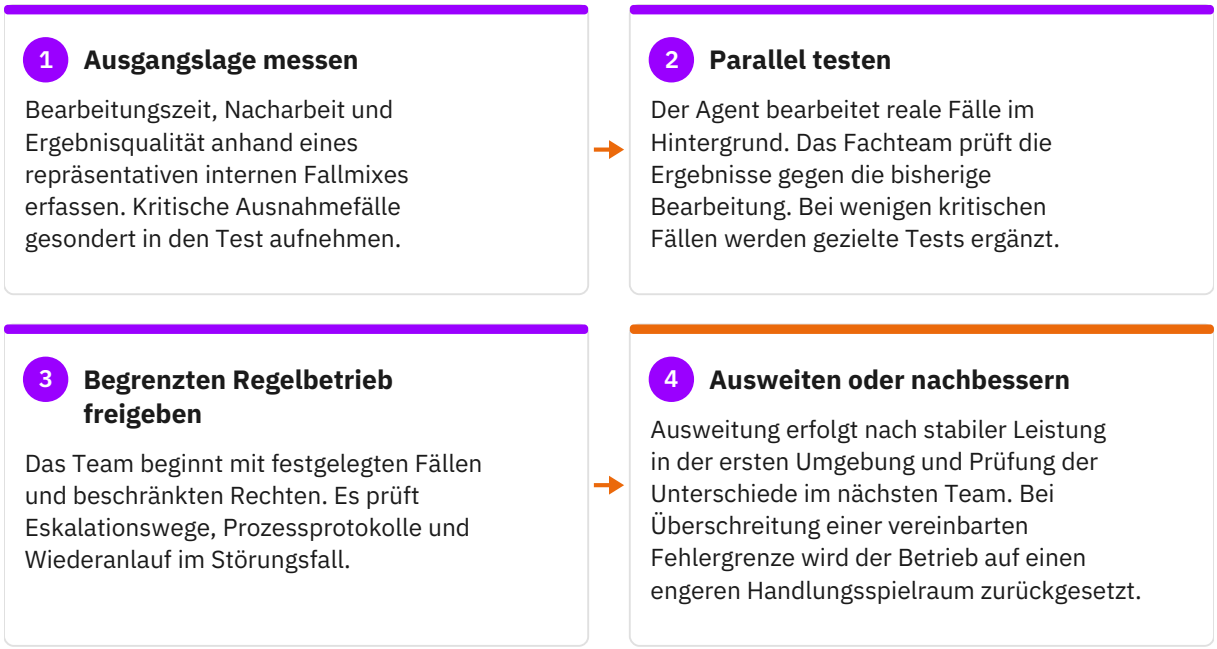


Abbildung 6: Vom Pilot zum Regelbetrieb: vier Freigabeschritte

Fünf Kennzahlen für die Geschäftsleitung

Kennzahl	Was sie zeigt
Anteil fachlich korrekter Abschlüsse	Ergebnisqualität
Quote manueller Eingriffe	verbleibende Arbeit
Durchlaufzeit	Effekt auf den Prozess
Vollkosten je korrekt abgeschlossenem Fall	Wirtschaftlichkeit
Zahl unzulässiger oder fehlerhafter Aktionen	Einhaltung der Grenzen

Die maßgebliche Kennzahl wird vor dem Pilot vereinbart und gegen eine datierte Ausgangslage gemessen. Auswertungen betrachten Normalfälle, Ausnahmen und kritische Fälle getrennt. Bei Änderungen an Modell, Werkzeugen oder Berechtigungen werden die betroffenen Tests wiederholt. Benchmarks wie TheAgentCompany untersuchen Aufgaben in einer simulierten Arbeitsumgebung [29]. Die Betriebsentscheidung braucht eigene Prozessfälle mit den dort geltenden Berechtigungen und Fehlerfolgen.

KAPITEL

09

Lieferantenbestätigungen im Einkauf

> **Der Einkauf zeigt im Kleinen, woran Agenten im Großen gemessen werden.**
>
> Ein mittelständisches Unternehmen gleicht eingehende Auftragsbestätigungen mit Bestellungen im ERP ab. Bestätigungen kommen als PDF oder per E-Mail. Abweichungen bei Menge, Preis, Artikel, Termin oder Konditionen müssen rechtzeitig erkannt werden. Heute prüfen Mitarbeitende die Eingänge, suchen die passende Bestellung und klären Abweichungen mit dem Lieferanten.

Ein Beleg aus dem Markt

Der Anbieter Perzeptron berichtet für seinen Kunden esw: Der wöchentliche Prüfaufwand für Lieferanten-Auftragsbestätigungen sank von rund 25 bis 30 Stunden auf weniger als fünf Stunden. Rund 85 % der Bestätigungen konnten vollständig automatisiert geprüft werden [20]. Das ist eine Herstellerangabe mit selbst berichteter Ausgangslage. Volumen, Zeitraum, Fehlerquote und der Aufwand für die übrigen 15 % bleiben offen. Ebenso offen ist, ob ein Agent im Sinne von Kapitel 2 arbeitet oder eine KI-gestützte Dokumentenextraktion mit Regelabgleich. Eine unabhängige Fallstudie zu diesem Prozess liegt nicht vor.

Aufgabe des Agenten

Der Agent extrahiert Angaben und sucht die Bestellung anhand zulässiger Merkmale. Preis- und Mengentoleranzen werden per Geschäftsregel geprüft. Bei mehreren möglichen Treffern oder fehlender Bestellnummer übergibt er den Fall zur Klärung. Für erkannte Abweichungen legt er einen internen Vorgang mit Belegen an. Änderungen im ERP und externe Nachrichten bleiben freigabepflichtig.

Betriebsnachweis

Der Test enthält Teilbestätigungen, falsche Zuordnungen, unterschiedliche Mengeneinheiten, geänderte Liefertermine, doppelte Nachrichten und zeitweise unerreichbare Systeme. Bewertet werden übersehene Abweichungen, Fehlalarme, korrekte Zuordnung, Bearbeitungszeit und Aufwände für Ausnahmen. Die Protokolle zeigen, auf welcher Grundlage eine Aktion ausgelöst wurde.

Illustrative Wirtschaftlichkeit

Annahme	Wert und Rechnung
Jahresvolumen und Zeit	12.000 Fälle. Bisher 6 Minuten je Fall. Im Zielbetrieb durchschnittlich 3 Minuten menschliche Arbeit einschließlich Prüfung und Nacharbeit.
Rechnerischer Kapazitätseffekt	600 Stunden pro Jahr. Bei 45 € je Stunde entspricht das 27.000 € bewerteter Kapazität.
Kostenannahme	14.000 € einmalige Einführung. 9.000 € laufende Mehrkosten pro Jahr für Betrieb, Integration und Qualitätssicherung.
Wirtschaftlicher Saldo	18.000 € jährlicher Saldo vor Einmalkosten. Rechnerisch 4.000 € im ersten vollen Betriebsjahr einschließlich Einführung.

Die Rechnung setzt voraus, dass die eingesparte Zeit wirtschaftlich genutzt werden kann. Sie beschreibt keine automatische Auszahlung oder Verringerung der Personalkosten. Steigt die durchschnittliche menschliche Restarbeit auf vier Minuten, sinkt der Kapazitätseffekt auf 400 Stunden oder 18.000 €. Der Saldo im ersten vollen Betriebsjahr fällt dann auf **minus 5.000 €**. Der rechnerische Break-even im ersten Jahr liegt bei etwa **2,6 Minuten realisierter Ersparnis pro Fall**. Eine Minute Restarbeit entscheidet also über Gewinn oder Verlust. Anlaufverzögerungen oder niedrigere Fallzahlen erhöhen die erforderliche Ersparnis.

Drei Werte fassen die Rechnung zusammen: 4.000 € Überschuss bei 3 Minuten Restarbeit, 5.000 € Verlust bei 4 Minuten Restarbeit und der Break-even bei 2,6 Minuten Ersparnis pro Fall.

4.000 €	5.000 €	2,6 Minuten
Überschuss bei 3 Minuten Restarbeit	**Verlust bei 4 Minuten Restarbeit**	**Break-even** Ersparnis pro Fall

Abbildung 7: Eine Minute entscheidet: Saldo im ersten vollen Betriebsjahr

Unsicherheit des Beispiels

Die Zahlen sind Rechenannahmen. Der Pilot muss vor allem den realen Zeitbedarf für Ausnahmen, die Fehlerfolgen und die Nutzung frei werdender Kapazität messen.

KAPITEL

10

Welche Daten für ein belastbares Lagebild fehlen

> **Das Lagebild scheitert nicht an fehlenden Umfragen, sondern an fehlenden Betriebsdaten.**
>
> Sieben Lücken schließt keine der ausgewerteten Quellen.

Lücke	Stand der Evidenz
Agenteneinsatz mit gemeinsamer Definition	Weder Eurostat noch Destatis erheben Agenten [8, 9]. Die verfügbaren Werte von 11 %, 16,6 %, 36 % und 1 % messen Verschiedenes.
Agenten im Regelbetrieb und in Kernprozessen	Repräsentativ nicht gemessen; der Wert von 1 % gilt nur für 180 Unternehmen im DACH-Raum [3].
Eingriffsrate, Fehlerquote und Kosten je Vorgang	Für deutsche Betriebe keine Feldmessung; Benchmarks sind kein Ersatz.
Abbruchquoten von Agentenprojekten	Nur eine Prognose und eine Projektquote, keine gemessene Quote für Deutschland oder die EU [3, 13].
Unabhängige Fallstudien	Für den Abgleich von Auftragsbestätigungen keine Studie mit Ausgangswert, Fehlerquote und Prüfaufwand.
Mitbestimmung	Keine Daten zu Betriebsvereinbarungen über KI-Agenten.
Amtliche Agentendefinition	Kein veröffentlichter Vorschlag der amtlichen Statistik gefunden.

Was eine wiederholbare Erhebung leisten sollte

Eine wiederholbare Deutschlanderhebung weist Unternehmen nach Größe und Branche aus. Sie verwendet über alle Wellen dieselbe Agentendefinition und zeigt den Befragten konkrete Beispiele für Assistenz, festen KI-Workflow und Agent. Planungsabsichten und reale Nutzung bekommen eigene Fragen. Fallzahlen und Antwortbasen werden je Frage veröffentlicht.

Der Mindestnachweis für Regelbetrieb lässt sich mit wenigen Angaben erheben: Datum der Inbetriebnahme, Fallvolumen in einem definierten Zeitraum, Zahl produktiv bearbeiteter Prozesse und größter erlaubter Handlungsspielraum. Ergänzend sind die Quote menschlicher Eingriffe, Ausfallzeiten und produktive Rücknahmen relevant. Freiwillig bereitgestellte Betriebskennzahlen könnten Selbstauskünfte für einen Teil der Stichprobe überprüfen. Dafür wären einheitliche Zählregeln und Verfahren zum Schutz vertraulicher Daten erforderlich. Im eigenen Haus gilt dasselbe Prinzip: Ein Betriebsnachweis zählt mehr als ein Dokument, also das Register in Betrieb, der genutzte Freigabe-Workflow und der Kennzahlenbericht.

KAPITEL

11

Fazit

> **Die Frage ist nicht, wie viele Unternehmen Agenten haben, sondern wie viele Fälle Agenten verlässlich abschließen.**
>
> Die Evidenz zeigt breite KI-Nutzung, wachsende Agentenaktivität und einen schmalen Kern im Regelbetrieb. Elf, sechsunddreißig und eins sind keine konkurrierenden Antworten auf dieselbe Frage, sondern Antworten auf drei verschiedene Fragen. Die amtliche Statistik erhebt 2025 keine Agenten. International skalieren Agenten in keiner Funktion bei mehr als einem Zehntel der Befragten. Die verschobenen Fristen des AI Act verschaffen Zeit für steuerbare Betriebsmodelle.

Für die Geschäftsleitung folgen daraus vier Merksätze:

Merksatz	Konsequenz
Zählen Sie Fälle, nicht Agenten.	Die Vollkosten je korrekt abgeschlossenem Fall sind die Zahl, auf die es ankommt.
Geben Sie Prozesse frei, nicht Modelle.	Der Regelbetrieb beginnt erst mit gemessener Ausgangslage, Rückfallweg und Abbruchregeln.
Vergeben Sie Rechte je Aktion, nicht Autonomie je Unternehmen.	Lesen, vorschlagen, intern schreiben und extern handeln sind verschiedene Entscheidungen.
Machen Sie den Betrieb steuerbar, bevor Sie ausweiten.	Verantwortung, Freigabe und Kennzahlen sind im Betrieb nachgewiesen, bevor ein zweites Team folgt.

Wer diese vier Sätze anwendet, braucht keine nationale Quote, um eine gute Entscheidung zu treffen.

KAPITEL

12

So unterstützt abamix

Dieses Papier führt zu drei Entscheidungen: welcher Prozess zuerst kommt, wie der Betrieb steuerbar wird und woran die Freigabe gemessen wird. Für jede Entscheidung steht Ihnen eine Leistung zur Verfügung.

AI Discovery
Sie verankern Ihre Kandidaten für Agenten im Wertstrom, bewerten sie und spezifizieren die erste Welle mit dem Agentic AI Canvas. Sie erhalten je spezifiziertem Use Case einen Business Case und eine schriftliche Not-now-Liste, die für jeden zurückgestellten Kandidaten begründet, warum er nicht in die erste Welle gehört.

AI Operating Model Assessment
Sie lassen Ihr KI-Betriebsmodell über acht Bausteine anhand von Bewertungskriterien verorten, nicht anhand von Selbstauskunft. Sie erhalten eine Lückenanalyse je Baustein, einen Vorschlag für ein Kennzahlensystem und eine sequenzierte Roadmap mit Abhängigkeiten.

AI Operating Model Build
Sie bringen ein steuerbares KI-Betriebsmodell in Betrieb, erst in einem Pilotbereich, dann in der Breite: benannte Verantwortliche, laufende Freigabe- und Eskalationswege, ein Register Ihrer Agenten mit Verantwortlichem und Steuerungsmodus sowie Kennzahlenberichte in Ihren vorhandenen Werkzeugen. Jedes Ergebnis belegen Sie durch einen Betriebsnachweis, gemessen an einer vorab vereinbarten Kennzahl gegen eine datierte Ausgangslage.

AI Assurance
Sie lassen KI-Systeme im Produktivbetrieb unabhängig testen: Softwarequalität, KI-Qualität, Governance-Konformität sowie generative und agentische Risiken. Sie erhalten Nachweise für Revision und Aufsicht.

Quellen

Abrufstand aller Quellen: 11.11.2026. Werte, die nur über Sekundärquellen gestützt sind, sind im Text als solche erkennbar oder hier vermerkt.

[1] Bitkom, „Erstmals nutzt die Mehrheit der Unternehmen KI“, Presseinformation, 14.09.2026. https://www.bitkom.org/Presse/Presseinformation/Erstmals-nutzt-Mehrheit-Unternehmen-KI

[2] eco – Verband der Internetwirtschaft, „eco Umfrage: Unternehmen in Deutschland setzen KI-Agenten kontrolliert ein“, Pressemitteilung zur Civey-Befragung, 14.10.2026. https://www.eco.de/presse/eco-umfrage-unternehmen-in-deutschland-setzen-ki-agenten-kontrolliert-ein-pauschale-forderungen-nach-einer-verlangsamung-der-ki-entwicklung-greifen-zu-kurz/

[3] Lünendonk, „Agentic AI – vom Copiloten zum Autopiloten“, Presseinformation, 17.09.2026. https://www.luenendonk.de/luenendonk-studie-80-prozent-der-unternehmen-sind-bei-ki-agenten-noch-in-der-pilot-und-testphase/

[4] Lünendonk, Studienseite „Agentic AI – vom Copiloten zum Autopiloten“, Erhebungszeitraum und Stichprobe. https://www.luenendonk.de/produkt/luenendonk-studie-agentic-ai-vom-copiloten-zum-autopiloten/

[5] Sopra Steria, „Regulierung fördert KI-Erfolg von Unternehmen“, Pressemitteilung zur Lünendonk-Studie, September 2026. https://www.handelsblatt.com/adv/presseportal/sopra-steria-se-sopra-steria-regulierung-foerdert-ki-erfolg-von-unternehmen---studie-66-prozent-der-unternehmen-bringen-weniger-als-ein-viertel-ihrer-ki-pilotprojekte-in-den-regelbetrieb/100266562.html

[6] CIO, „Unternehmen stecken mit Agentic AI im Testlabor fest“, 17.09.2026. https://www.cio.de/article/4221162/unternehmen-stecken-mit-agentic-ai-im-testlabor-fest.html

[7] Salesforce und Deutscher Mittelstands-Bund, „KI-Index Mittelstand 2026“, Pressemitteilung, 12.03.2026. https://www.salesforce.com/de/news/press-releases/2026/03/12/ki-index-mittelstand-2026/

[8] Destatis, IKT in Unternehmen, KI-Nutzung 2025 (Gesamtwert 26 % und freiwillige Teilnahme auf der Destatis-Seite; Größenklassen über Eurostat abgeglichen). https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Unternehmen/IKT-in-Unternehmen-IKT-Branche/Tabellen/ikti-unternehmen-kuenstliche-intelligenz.html

[9] Eurostat, „The use of artificial intelligence (AI) technologies in the European Union“, KS-01-26-009, Datensatz isoc_eb_ai, Berichtsjahr 2025. https://ec.europa.eu/eurostat/documents/7870049/23260410/KS-01-26-009-EN-N.pdf

[10] ifo Institut, KI-Nutzung in Unternehmen, Konjunkturumfrage Mai 2026, veröffentlicht 05.06.2026 https://www.ifo.de/fakten/2026-06-05/mehr-als-die-haelfte-der-unternehmen-nutzt-kuenstliche-intelligenz

[11] M. Friedrich, C. Kagerl, „Künstliche Intelligenz in deutschen Betrieben: Jeder vierte Betrieb nutzt mittlerweile generative KI“, IAB-Kurzbericht 8/2026, 05.05.2026, DOI 10.48720/IAB.KB.2608. https://doku.iab.de/kurzber/2026/kb2026-08.pdf

[12] McKinsey & Company, „The state of AI in 2025: Agents, innovation, and transformation“, 05.11.2025. https://www.mckinsey.com/~/media/mckinsey/business%20functions/quantumblack/our%20insights/the%20state%20of%20ai/november%202025/the-state-of-ai-in-2025.pdf

[13] Gartner, „Gartner Predicts Over 40% of Agentic AI Projects Will Be Canceled by End of 2027“, Pressemitteilung, 25.06.2025. https://www.gartner.com/en/newsroom/press-releases/2025-06-25-gartner-predicts-over-40-percent-of-agentic-ai-projects-will-be-canceled-by-end-of-2027

[14] A. Challapally, C. Pease, R. Raskar, P. Chari (MIT Project NANDA), „The GenAI Divide: State of AI in Business 2025“, Juli 2025 (Kopie; keine MIT-Fassung öffentlich abrufbar). https://valtao.com/wp-content/uploads/2025/11/Rapport-MIT.pdf

[15] Anthropic, „Building effective agents“, 19.12.2024. https://www.anthropic.com/research/building-effective-agents

[16] Deutsche Telekom, „Von sechs Stunden auf 60 Minuten: KI-Agent beschleunigt Analysearbeit“, Medieninformation, 06.03.2026. https://www.telekom.com/de/newsroom/aktuelles/medieninformationen/2026/03/von-sechs-stunden-auf-60-minuten

[17] Siemens AG, „Siemens launches the Eigen Engineering Agent, bringing purpose-built AI to industrial automation engineering“, Pressemitteilung, 20.04.2026. https://assets.new.siemens.com/siemens/assets/api/uuid:72c8b639-ecd8-44f3-b67c-09eb4d6e7528/HQCOPR202604167383EN.pdf

[18] Capgemini, „68% of automotive organizations use or pilot agentic AI for product development, but only 5% report mature AI governance“, Pressemitteilung, 12.10.2026. https://www.capgemini.com/news/press-releases/68-of-automotive-organizations-use-or-pilot-agentic-ai-for-product-development-but-only-5-report-mature-ai-governance-2/

[19] Capgemini Research Institute, „Rewiring automotive product development: How organizations can pull ahead in the AI race“, Studienbericht, Oktober 2026. https://www.capgemini.com/wp-content/uploads/2026/10/Rewiring-automotive-product-development_How-organizations-can-pull-ahead-in-the-AI-race_Automotive_Capgemini.pdf

[20] IT Management, „Perzeptron auf der EFX: Auftragsbestätigungen automatisiert mit KI prüfen“, 27.08.2026. https://www.it-management.today/perzeptron-auf-der-efx-auftragsklarheit-schaffen-und-auftragsbestaetigungen-automatisiert-mit-ki-pruefen

[21] NIST und NCCoE, „Accelerating the Adoption of Software and AI Agent Identity and Authorization“, Konzeptpapier, Entwurf, 05.02.2026. https://www.nccoe.nist.gov/publications/other/accelerating-adoption-software-and-ai-agent-identity-and-authorization-concept

[22] OWASP GenAI Security Project, „OWASP Top 10 for Agentic Applications“, 09.12.2025. https://genai.owasp.org/2025/12/09/owasp-top-10-for-agentic-applications-the-benchmark-for-agentic-security-in-the-age-of-autonomous-ai/

[23] BSI und ANSSI, „Design Principles for LLM-based Systems with Zero Trust – Foundation for Secure Agentic Systems“, 11.08.2025. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/ANSSI-BSI-joint-releases/LLM-based_Systems_Zero_Trust.pdf

[24] BSI, „Basisschutz gegen Indirect Prompt Injection in dokumentbasierten LLM-Chats“, Fassung vom 01.10.2026. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KI/Basisschutz_Indirect-Prompt-Injections_LLM.pdf

[25] Europäische Union, Verordnung (EU) 2024/1689 (KI-Verordnung), insbesondere Art. 4, 5, 6, 50 und Anhänge I und III. https://eur-lex.europa.eu/eli/reg/2024/1689/oj

[26] Future of Privacy Forum, „The AI Act implementation timeline: what changes under the AI Omnibus“, 2026 (zur Verordnung (EU) 2026/1744). https://fpf.org/blog/the-ai-act-implementation-timeline-what-changes-under-the-ai-omnibus/

[27] Gibson Dunn, „EU AI Act Omnibus Agreement: Postponed High-Risk Deadlines and Other Key Changes“, 2026. https://www.gibsondunn.com/eu-ai-act-omnibus-agreement-postponed-high-risk-deadlines-and-other-key-changes/

[28] Gesetz zur Marktüberwachung und Innovationsförderung von künstlicher Intelligenz (KI-MIG) vom 22.07.2026, BGBl. 2026 I Nr. 223, in Kraft seit 29.07.2026. https://www.gesetze-im-internet.de/ki-mig/BJNR0DF0B0026.html

[29] F. F. Xu et al., „TheAgentCompany: Benchmarking LLM Agents on Consequential Real World Tasks“, arXiv 2412.14161. https://arxiv.org/abs/2412.14161

[30] Civey im Auftrag von e-Residency Estland, Befragung von Gründern, KMU-Geschäftsführern und Selbstständigen, September 2026, Pressemitteilung. https://www.finanznachrichten.de/nachrichten-2026-09/69700314-jeder-dritte-unternehmer-wuerde-buerokratie-an-einen-ki-agenten-delegieren-007.htm

[31] Betriebsverfassungsgesetz (BetrVG), §§ 80, 87, 90. https://www.gesetze-im-internet.de/betrvg/

[32] alphaXiv, Leaderboard „TheAgentCompany“ (Bestwert 42,9 %, TTE-MatrixAgent mit DeepSeek-V3.2; ohne Datum des Eintrags). https://alphaxiv.org/benchmarks/carnegie-mellon-university/theagentcompany

[33] White & Case, „EU AI Omnibus enters into force, amending the AI Act“, 2026. https://www.whitecase.com/insight-alert/eu-ai-omnibus-enters-force-amending-ai-act

[34] Verordnung (EU) 2026/1744 vom 08.07.2026 (Digital Omnibus on AI), ABl. L 2026/1744 vom 24.07.2026. https://eur-lex.europa.eu/eli/reg/2026/1744/oj?locale=de

KONTAKT

Ansprechpartner

Prof. Dr. Amadou Sienou

info@abamix.com · www.abamix.com

Erstgespräch, 20–30 Minuten: meeting.abamix.com

IMPRESSUM

Herausgeber	abamix GmbH · Lothringerstr. 11 · 70435 Stuttgart
Dokument	Marktanalyse · Agentic AI in deutschen Unternehmen
Version	1.1 · 11.11.2026 · Status: Freigegeben
Autor	Prof. Dr. Amadou Sienou
Zitiervorschlag	Sienou, A. (2026). *Agentic AI in deutschen Unternehmen: Elf, sechsunddreißig, eins: Was die Zahlen zu KI-Agenten messen und was sie offenlassen*. Marktanalyse, Version 1.1. Stuttgart: abamix GmbH.

© 2026 abamix GmbH. Alle Rechte vorbehalten. Regulatorische Einschätzungen geben den Stand zum Versionsdatum wieder und ersetzen keine Rechtsberatung.



abamix

AI. Applied. Governed.

abamix GmbH · Lothringerstr. 11 · 70435 Stuttgart

info@abamix.com · www.abamix.com