ANHANG I

Häufig gestellte Fragen

Zusatzmaterial zum Buch „PREDICTABLE“ von Thorsten Pätzold — Amazing Agents.

ANHANG I

Häufig gestellte Fragen

Aus den letzten 50 Beratungs-Gesprächen mit Mittelständlern haben wir 35 Fragen gesammelt, die immer wieder auftauchen. Die Antworten sind so direkt formuliert, wie wir sie auch im Gespräch geben würden — keine Floskeln, keine PR.

„Die meisten Bedenken zerfallen, sobald sie konkret beantwortet werden.“

I.1 Grundsätzliche Fragen

Frage 1.1

Brauche ich überhaupt Agenten — oder reicht ChatGPT für meine Mitarbeiter?

Wenn Sie nur möchten, dass Mitarbeiter Routine-Texte schneller schreiben, reicht ein Modell-Zugang (ChatGPT Plus, Claude Pro, Microsoft Copilot) tatsächlich aus. Das ist auch der richtige erste Schritt — bevor Sie über Agenten nachdenken, sollten Ihre Mitarbeiter mit einem reinen Modell-Tool umgehen können.

Agenten lohnen sich erst, wenn Sie wiederkehrende Workflows automatisieren wollen, die Anbindung an Bestandssysteme brauchen, oder Volumina so hoch werden, dass Mitarbeiter sie nicht mehr sinnvoll bewältigen. Eine grobe Faustregel: Wenn Sie pro Woche mehr als 5 Stunden für eine wiederkehrende Aufgabe aufwenden, lohnt sich die Agent-Investition fast immer.

Frage 1.2

Ist das nicht alles nur Hype, wie Blockchain damals?

Eine berechtigte Frage. Der Unterschied zu Blockchain ist messbarer Wert in Produktion, hier und jetzt. Ein Inbox-Manager, der 12 Stunden pro Woche zurückgibt, ist kein Hype — das sind Zahlen, die Ihr Steuerberater am Jahresende sieht.

Was tatsächlich Hype ist: bestimmte Marketing-Versprechen ("95% Automatisierung ab Tag 1", "AGI-Agenten 2026"), bestimmte überteuerte Anbieter und bestimmte Use Cases, die heute noch nicht reif sind. Wer aber bei den heute funktionierenden Use Cases bleibt — Inbox, Outreach, Recruiting, Daten-Analyse — bekommt soliden, berechenbaren Wert.

Frage 1.3

Wie schnell veraltet die Technologie? Investiere ich in eine Sackgasse?

Modelle veralten schnell, das stimmt — alle 6–12 Monate gibt es deutlich bessere Versionen. Architekturen veralten langsam. Eine gut entworfene Agent-Architektur (klare Schichten-Trennung, austauschbare Modelle, modulares Tool-Setup) profitiert von jedem Modell-Upgrade, ohne neu gebaut werden zu müssen.

Die Investition liegt auch nicht primär in der Technologie, sondern in der Architektur, den Prompts, der Datenintegration, den Compliance-Strukturen. Diese Investitionen sind nicht abhängig vom konkreten Modell — sie zahlen sich auch in 5 Jahren noch aus.

Frage 1.4

Müssen meine Mitarbeiter jetzt auch programmieren können?

Nein. Im Gegenteil: Wenn Ihre Agent-Strategie davon abhängt, dass Mitarbeiter programmieren, ist die Architektur falsch. Mitarbeiter sollten Agenten nutzen wie sie heute Office-Programme nutzen — ohne Programmier-Kenntnisse.

Was Mitarbeiter aber brauchen: Verständnis für Stärken und Schwächen von Sprachmodellen, Disziplin im Umgang mit Halluzinationen, ein gewisses Sensorium für sinnvolle Eskalations-Anlässe. Das ist eine Schulungs-Aufgabe von 2–4 Stunden pro Mitarbeiter, nicht ein Studium der Informatik.

Frage 1.5

Was ist der Unterschied zwischen einem Agenten und einem Chatbot?

Ein Chatbot beantwortet Fragen. Ein Agent erledigt Aufgaben. Konkret: Ein Chatbot kann Ihnen sagen, was in einer FAQ-Liste steht. Ein Agent kann eine Anfrage entgegennehmen, im CRM nach dem Kunden suchen, einen Vorgang anlegen, eine Antwort verfassen und sie zur Freigabe vorlegen.

Der technische Unterschied: Agenten haben Zugriff auf Tools, persistentes Memory und sind in Workflows eingebettet. Chatbots haben in der Regel nur Zugriff auf eine begrenzte Wissensbasis und keine Aktions-Möglichkeit nach außen.

Frage 1.6

Macht KI meine Mitarbeiter überflüssig?

In den meisten Mittelstands-Setups: nein. Die typische Konsequenz ist nicht Stellenabbau, sondern Aufgaben-Verschiebung. Mitarbeiter machen weniger Routine-Arbeit und mehr werthaltige Arbeit — Beziehungen, Beratung, Strategie, Eskalationen.

Wir haben in 50+ Projekten genau einen Fall gesehen, in dem Stellen entfallen sind — und das war eine Sondersituation mit ohnehin geplanter Restrukturierung. In allen anderen Fällen wurden bestehende Stellen produktiver, und manchmal entstehen sogar neue Rollen (Agent-Owner, Operations-Verantwortlicher).

Die kritische Größe ist Wachstum: Wenn Sie wachsen, ohne neue Stellen aufzubauen, finanzieren sich Agenten oft aus eingesparten Neueinstellungen.

I.2 Kosten und ROI

Frage 2.1

Was kostet ein Agent-Setup wirklich — alle Kosten zusammen?

Drei Kostenblöcke: Setup einmalig, Betrieb monatlich, Wartung pro Quartal.

Setup einmalig: 500–2.500 Euro je nach Komplexität. Inbox-Manager am unteren Ende, Outreach-Agent oder Multi-Agent-Setups am oberen Ende. Hierin enthalten: Anforderungs-Aufnahme, Tool-Anbindung, Prompt-Design, Tests, Schulung.

Betrieb monatlich: 400–1.800 Euro pro Agent. Setzt sich zusammen aus Modell-Tokens (typisch 100–400 Euro), Hosting/Infrastruktur (100–300 Euro), Wartung/Support (200–1.100 Euro).

Wartung pro Quartal: 8–20 Stunden pro Agent für Anpassungen, Updates, Optimierungen. Bei externer Wartung 800–2.500 Euro pro Quartal.

Gesamtkosten Jahr 1 für einen typischen Inbox-Manager: ca. 13.000–19.000 Euro. Jahr 2 ohne Setup: ca. 11.000–15.000 Euro.

Frage 2.2

Ab wann rechnet sich ein Agent?

Faustregel: ab 8 eingesparten Stunden pro Woche bei einem inneren Stundensatz von 60–80 Euro. Das ergibt einen Bruttowert von ca. 24.000 Euro pro Jahr — bei realistischem 65%-Automatisierungsgrad ein Effektivwert von ca. 15.600 Euro pro Jahr. Damit sind Setup und Anlaufphase nach etwa drei Monaten verdient — der Rest des Jahres ist Ertrag.

Wenn Sie unter dieser Schwelle liegen, lohnt sich der Aufwand selten. Wenn Sie deutlich darüber liegen (z.B. 15–20 Stunden / Woche bei einem Geschäftsführer mit 100 Euro Stundensatz), ist der ROI oft schon nach wenigen Wochen erreicht.

Frage 2.3

Versteckte Kosten — gibt es die?

Drei häufig vergessene Posten. Erstens: interner Aufwand für Konfiguration, Schulung und laufende Pflege. Plant man pro Agent 4–8 interne Stunden pro Monat ein. Zweitens: Datenschutz-Beratung. Bei sensitiven Use Cases können externe Datenschutz-Berater 2.000–5.000 Euro kosten — einmalig, dann jährlich kleinere Updates. Drittens: Anbieter-Anpassungen. Wenn ein Modell-Anbieter seine Preise ändert oder ein Tool seine API umstellt, fällt Mehraufwand an. Plant man 8–15% der Betriebskosten als Risiko-Reserve.

Mit diesen drei Posten in der Rechnung wird der ROI realistischer. Ohne sie überschätzen Sie die Rendite typischerweise um 15–25%.

Frage 2.4

Lohnt sich ein günstigeres Modell oder lieber das teurere?

Bei Routine-Aufgaben (Klassifikation, einfache Antwort-Entwürfe) reichen günstigere Modelle völlig aus. Sie können hier 60–80% der Modell-Kosten sparen, ohne dass die Qualität spürbar leidet.

Bei anspruchsvollen Aufgaben (Reasoning, lange Dokumenten-Analyse, kritische Entscheidungen) lohnt sich das teurere Modell: die Output-Qualität ist deutlich besser, was sich in weniger Halluzinationen und weniger menschlicher Nacharbeit zeigt.

Unsere Empfehlung in den meisten Setups: polyglott arbeiten. Ein günstiges Modell für Massen-Operationen, ein hochwertiges für die anspruchsvollen Schritte. Das Routing zwischen den Modellen wird im Agent-Prompt eingebaut und ist technisch unproblematisch.

Frage 2.5

Wie messe ich den ROI ehrlich, ohne mich selbst zu täuschen?

Drei Disziplinen. Erstens: Zeit-Messung mit historischer Baseline. Vor dem Agent-Setup zwei Wochen lang protokollieren, wie viel Zeit für die Aufgabe aufgewendet wird. Diese Baseline ist Gold wert.

Zweitens: Stunden-Tracking pro Mitarbeiter, der mit dem Agent arbeitet. Nicht Schätzungen, sondern reale Daten — wenn nötig über zwei Wochen Stichproben.

Drittens: Quality-Tracking. Wie viele Outputs muss ein Mensch korrigieren? Wie hoch ist die Eskalations-Rate? Sind Kunden zufriedener oder unzufriedener? Diese Qualitätsdimension wird oft vergessen — und kann den nominellen ROI sowohl deutlich steigern als auch reduzieren.

Wichtig: ROI nicht von der Person messen lassen, die für das Projekt verantwortlich ist. Die hat einen Bestätigungs-Bias. Eine externe oder neutrale interne Person macht die Messung.

I.3 DSGVO und Compliance

Frage 3.1

Sind ChatGPT und Claude überhaupt DSGVO-konform nutzbar?

Ja, aber nicht out-of-the-box. Sie brauchen einen AVV (Auftragsverarbeitungsvertrag) mit dem Anbieter, geeignete Standardvertragsklauseln (SCC) für den Drittland-Transfer in die USA, und sollten mindestens ein Opt-out vom Daten-Training konfigurieren — bei Enterprise-Plänen ist das oft Default.

Für sensitive Use Cases (besondere Datenkategorien wie Gesundheits- oder Sozialdaten) sind US-Anbieter problematisch — hier sollten Sie EU-Anbieter wie Mistral oder lokale Open-Source-Modelle nutzen. Für die meisten Mittelstands-Use-Cases mit "normalen" personenbezogenen Daten sind die US-Anbieter mit AVV und SCC aber vertretbar.

Frage 3.2

Was passiert bei einer DSGVO-Prüfung?

Eine Aufsichtsbehörde fragt im Wesentlichen sechs Dinge: Verzeichnis von Verarbeitungstätigkeiten, AVVs mit allen Auftragsverarbeitern, Datenfluss-Dokumentation, DSFA falls erforderlich, technische und organisatorische Maßnahmen, und Beweise der Betroffenen-Rechte-Umsetzung.

Wenn Sie diese sechs Dokumente sauber haben, ist die Prüfung in der Regel unproblematisch — selbst wenn einzelne Punkte nicht perfekt sind. Wenn ein oder mehrere Dokumente fehlen, wird es kritisch: Bußgelder bis 4% des Jahresumsatzes oder 20 Mio. Euro sind möglich.

Der Aufwand für die sechs Dokumente liegt initial bei 16–40 Stunden — keine Raketen-Wissenschaft, aber nicht trivial. Investieren Sie das, bevor Sie produktiv gehen.

Frage 3.3

Brauche ich für jeden Agent eine eigene DSFA?

Eine DSFA (Datenschutz-Folgenabschätzung) ist nach Art. 35 DSGVO Pflicht, wenn die Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt.

Faustregel: Wenn Ihr Agent automatisierte Entscheidungen über Personen trifft (Recruiting, Bonität, Kunden-Kategorisierung), ist eine DSFA praktisch immer erforderlich. Wenn Ihr Agent nur Routine-Operationen ausführt (Mail-Klassifizierung, Datenextraktion ohne Bewertung), ist eine DSFA oft nicht zwingend, aber empfehlenswert.

Im Zweifel: DSFA durchführen. Der Aufwand (2–8 Stunden) ist gering im Vergleich zu den Konsequenzen einer fehlenden DSFA bei einer Prüfung.

Frage 3.4

Wie gehe ich mit dem Recht auf Löschung um, wenn das Memory die Daten enthält?

Das ist die schwierigste DSGVO-Anforderung in Agent-Setups, und sie muss von Tag 1 mitgedacht werden. Drei Lösch-Pfade müssen funktionieren:

Erstens: aktive Memory-Daten — direkter Lösch-Befehl pro Person, der alle Memory-Stellen durchsucht und löscht. Zweitens: Konversations-Logs — entweder kurze Aufbewahrungsfristen (30–90 Tage), oder Lösch-Fähigkeit pro Person. Drittens: Backup-Systeme — entweder Backups, die nicht zurückgehen lassen, oder Lösch-Fähigkeit auch in Backups.

In der Praxis bedeutet das: Sie brauchen ein Lösch-Skript, das alle drei Pfade abdeckt, und Sie sollten es einmal pro Quartal testen — sonst funktioniert es im Ernstfall nicht.

Frage 3.5

Was ist mit dem EU AI Act?

Der EU AI Act ist seit 2024 in Kraft und betrifft auch Mittelständler. Drei Risiko-Stufen sind relevant:

Minimales Risiko (Inbox-Manager, Standard-Daten-Analyst): keine zusätzlichen Pflichten außer denen aus DSGVO. Begrenztes Risiko (Bots mit Kunden-Kontakt): Transparenz-Pflicht — der Kunde muss erkennen können, dass er mit einer KI spricht. Hohes Risiko (Recruiting, Bonität, Kunden-Bewertung): erhebliche zusätzliche Pflichten — Risiko-Management-System, Daten-Governance, technische Dokumentation, Mensch-im-Loop, Logging.

Für die meisten Mittelstands-Setups gilt: Recruiting ist hochrisiko-relevant und braucht spezielle Aufmerksamkeit, der Rest läuft unter minimal oder begrenzt. Pflicht ist aber: einmalige Risikoeinstufung pro Use Case, dokumentiert.

Frage 3.6

Was, wenn der Agent jemanden diskriminiert?

Diskriminierung durch einen Agenten ist Ihre Verantwortung als Betreiber, nicht die des Anbieters. Das gilt insbesondere bei Recruiting-Agenten. Sie haften, nicht der Modell-Anbieter.

Drei Schutzmaßnahmen sind Pflicht: Erstens, AGG-konforme Bewertungs-Kriterien (siehe Anhang E.7). Zweitens, regelmäßiges Demografie-Monitoring der Top-Match-Verteilung. Drittens, dokumentierte Mensch-im-Loop-Architektur, sodass keine automatisierte Entscheidung ohne menschliche Bestätigung erfolgt.

Wenn dennoch Diskriminierung auftritt: sofortiger Stopp des Agenten für den betroffenen Bereich, forensische Analyse der Ursachen, dokumentierte Korrekturmaßnahmen, ggf. Information der Betroffenen. AGG-Klagen sind teuer — aber dokumentierte Compliance reduziert das Risiko erheblich.

I.4 Technische Fragen

Frage 4.1

Brauche ich eine eigene IT-Abteilung dafür?

Nein, aber Sie brauchen eine klare technische Verantwortung. Bei kleineren Mittelständlern (bis 50 Mitarbeiter) reicht oft ein externer Dienstleister, der für Setup und Wartung verantwortlich ist. Bei mittleren Mittelständlern (50–250 Mitarbeiter) ist es sinnvoll, dass ein interner Mitarbeiter (oft aus IT oder einem

fachlichen Bereich mit Technik-Affinität) die Owner-Rolle übernimmt — er ist das Bindeglied zwischen Fachseite und externem Dienstleister.

Bei größeren Mittelständlern lohnt sich oft eine kleine interne Agent-Operations-Funktion (1–2 Personen), die mehrere Agenten betreut.

Wichtig: Setup ist nicht das Problem — das machen externe meist schnell. Das Problem ist Wartung und Weiterentwicklung. Hier brauchen Sie kontinuierliche Verantwortung.

Frage 4.2

Wie integriere ich Agenten in meine bestehende IT-Landschaft?

Über fünf Patterns (siehe Anhang G und Kapitel 7): Direct API, Webhook, iPaaS-Plattformen wie Make oder n8n, RPA für Browser-basierte Tools ohne API, oder das neue MCP-Protokoll. In den meisten Setups kombinieren wir 2–3 Patterns.

Die zeitintensivste Phase ist meist die Anbindung an Bestandssysteme — typisch 60% des Setup-Aufwands. Wenn Ihre Bestandssysteme APIs haben, ist das straightforward. Wenn nicht, müssen Sie auf RPA oder iPaaS-Workarounds ausweichen, die etwas fragiler sind.

Frage 4.3

Was, wenn ein Modell-Anbieter pleite geht?

Risiko, aber überschaubar. Die großen Anbieter (OpenAI, Anthropic, Google, Microsoft, Mistral) sind alle solide kapitalisiert. Bei kleineren Anbietern ist das Risiko größer.

Die wichtigste Schutzmaßnahme: modulare Architektur. Wenn Ihr Setup so gebaut ist, dass Sie das Modell austauschen können, ohne den Rest neu bauen zu müssen, ist Ihr Risiko begrenzt — auch beim Komplettausfall eines Anbieters bleibt Ihr System mit einem anderen Modell innerhalb von Tagen wieder lauffähig.

In der Praxis: alle Modell-Aufrufe gehen durch eine Abstraction-Schicht in Ihrem Code, die das konkrete Modell konfiguriert. Wechsel ist dann eine Konfiguration, kein Architektur-Eingriff.

Frage 4.4

Kann ich meinen eigenen Server statt Cloud-Modell nutzen?

Ja, technisch und zunehmend wirtschaftlich. Open-Source-Modelle wie Llama, Mistral oder DeepSeek sind inzwischen leistungsfähig genug für viele Mittelstands-Use-Cases. Sie laufen auf einem GPU-Server (typisch 30.000–150.000 Euro Investition) oder in einer EU-Cloud mit dediziertem Hosting (typisch 1.500–6.000 Euro pro Monat).

Ob sich On-Prem lohnt, hängt von drei Faktoren ab. Erstens: Sensitivität der Daten (rechtfertigt sie die Investition?). Zweitens: Volumen (lohnt sich erst ab vielen Millionen Token-Aufrufen pro Monat). Drittens: Operations-Knowhow (haben Sie Leute, die GPU-Server warten können?).

Für die meisten Mittelständler: Cloud-Anbieter mit AVV und SCC ist der pragmatischere Weg. Für hochsensitive Branchen (Anwälte, Gesundheit, Behörden): On-Prem ist oft die richtige Antwort.

Frage 4.5

Wie schnell antwortet ein Agent?

Hängt vom Setup ab. Reine Klassifikations-Aufgaben: 0,5–2 Sekunden. Antwort-Entwürfe mit Recherche: 5–15 Sekunden. Komplexe Multi-Step-Workflows mit mehreren Tool-Calls: 30 Sekunden bis 3 Minuten.

Wenn Sie sub-Sekunden-Antworten brauchen (Live-Chat, Voice-Bots), müssen Sie das in der Architektur einplanen — kleinere Modelle, weniger Reasoning, gecachete Antworten. Bei den meisten Mittelstands-Use-Cases ist Latenz aber unkritisch, weil die Aufgaben asynchron laufen ("in der Nacht 200 Mails bearbeiten").

Frage 4.6

Was, wenn der Agent etwas Falsches macht? Wer haftet?

Der Betreiber, also Sie. Modell-Anbieter haften nur in engen, vertraglich definierten Grenzen — meist auf den Wert des Service-Vertrages.

Ihre Haftung können Sie reduzieren durch: Mensch-im-Loop bei kritischen Aktionen (sodass keine wichtige Entscheidung ohne menschliche Bestätigung erfolgt), klare Prozess-Dokumentation (welche Aufgaben darf der Agent autonom, welche nicht), regelmäßige Audits, Berufshaftpflicht-Versicherung mit KI-Klausel.

Wir empfehlen jedem Mittelständler, vor Setup mit dem Versicherer zu sprechen und ggf. die Berufshaftpflicht um eine KI-Klausel zu erweitern.

Frage 4.7

Wie verhindere ich, dass der Agent Geheimnisse ausplaudert?

Drei Schichten. Erstens: technische Trennung. Geheime Daten (Geschäftsgeheimnisse, persönliche Daten) werden nicht in den Modell-Kontext gegeben, sondern bleiben in geschützten Systemen. Der Agent fragt sie nur ab, wenn nötig.

Zweitens: Prompt-Engineering. Im System-Prompt explizit definieren, was der Agent NICHT tun darf — keine Geheimnisse weitergeben, keine personenbezogenen Daten nennen, keine internen Strategien ansprechen.

Drittens: Output-Filtering. Vor jeder Ausgabe an einen externen Empfänger prüft ein zweiter Agent (oder ein Regel-System), ob die Ausgabe geheime Informationen enthält. Wenn ja: Ausgabe blockieren oder anonymisieren.

Mit diesen drei Schichten ist das Risiko sehr klein — aber niemals null. Bei extrem sensitiven Geheimnissen sollten Sie den Agenten gar nicht erst anbinden.

I.5 Organisatorische Fragen

Frage 5.1

Wer in meinem Unternehmen sollte für den Agent verantwortlich sein?

Eine Person mit drei Eigenschaften: fachliche Nähe zum Use Case (versteht, was richtig und falsch ist), Technologie-Verständnis (muss kein Programmierer sein, aber sollte Tools und Modelle einordnen können), und ausreichend Autorität, Entscheidungen zu treffen.

In kleineren Mittelständlern: oft der Geschäftsführer selbst oder ein direkt unterstellter Bereichsleiter. In mittleren Mittelständlern: meist ein Bereichsleiter oder ein Stabsmitarbeiter. Wichtig: nicht der IT-Leiter (außer der hat fachliche Nähe), sondern jemand, der den Use Case wirklich versteht.

Frage 5.2

Wie reagieren Mitarbeiter typisch auf Agent-Einführungen?

Drei Reaktions-Muster, die in fast jedem Projekt auftauchen.

Muster 1 — die Skeptischen (typisch 15–30% des Teams): "Das ersetzt mich." Diese Mitarbeiter brauchen klare Kommunikation, dass ihre Rolle sich verändert, aber nicht entfällt. Beste Strategie: einbinden in das Setup-Team.

Muster 2 — die Pragmatischen (typisch 50–70%): "Mal schauen, ob das wirklich hilft." Diese Mitarbeiter werden überzeugt durch konkrete Ergebnisse. Beste Strategie: schnelle, klare Wins zeigen.

Muster 3 — die Begeisterten (typisch 10–20%): "Endlich, wann kommt mehr?" Diese Mitarbeiter sind Ihre internen Multiplikatoren. Beste Strategie: ihnen Verantwortung geben, sie zu Owner-Stellvertretern machen.

Die Schiefverteilung ist normal. Erfolgreiche Setups erkennen sie und arbeiten mit allen drei Gruppen unterschiedlich.

Frage 5.3

Wie schule ich mein Team für die Arbeit mit Agenten?

Drei Schulungs-Module reichen meist aus.

Modul 1: Grundverständnis (1 Stunde). Was ist ein Agent, was kann er, was kann er nicht? Stärken und Schwächen von Sprachmodellen, Halluzinations-Risiko, sinnvoller Umgang.

Modul 2: Konkrete Bedienung (2 Stunden). Wie nutze ich diesen spezifischen Agenten in meinem Tagesablauf? Welche Aufgaben sind wofür geeignet? Wie melde ich Probleme?

Modul 3: Kritischer Umgang (1 Stunde). Wann sollte ich den Output hinterfragen? Wann eskaliere ich? Welche typischen Fehler macht der Agent in unserem Bereich?

Gesamt: 4 Stunden initiale Schulung plus regelmäßige Updates (etwa quartalsweise 1 Stunde) — kein großer Aufwand, aber Pflicht.

Frage 5.4

Was passiert mit Mitarbeitern, deren Aufgabe der Agent übernimmt?

In den meisten Fällen: ihre Rolle verändert sich. Was vorher 60% der Zeit Routine-Arbeit war, ist nachher vielleicht 20% — der Rest sind höherwertige Aufgaben, die der Agent nicht übernehmen kann.

Wir haben ein paar Beispiele aus echten Projekten. Eine Vertriebsassistentin, die früher 70% ihrer Zeit mit Lead-Recherche verbracht hat, macht heute 30% Lead-Recherche und 40% Account-Management mit Bestandskunden — was vorher liegen blieb. Eine Buchhaltungs-Mitarbeiterin, die früher Routine-Verbuchungen gemacht hat, macht heute Analyse und Beratung der Geschäftsführung.

Wichtig: das funktioniert nur, wenn Sie die Rollenanpassung aktiv steuern. Wenn Sie die Mitarbeiter sich selbst überlassen, machen viele weiter Routine-Arbeit, die der Agent eigentlich übernehmen sollte. Das ist Verschwendung — und meist auch ein Frust-Faktor.

Frage 5.5

Soll ich einen externen Berater einbinden oder das selbst machen?

Hängt von zwei Faktoren ab: Ihrem internen Knowhow und der Komplexität des Setups.

Wenn Sie einen IT-affinen Mitarbeiter haben, der sich in Agent-Konzepte einarbeiten kann, und der Use Case nicht extrem komplex ist (klassischer Inbox-Manager): selbst machen ist oft der bessere Weg, weil das Knowhow im Haus aufgebaut wird.

Wenn Sie kein internes Knowhow haben, der Use Case komplex ist (Multi-Agent, regulierte Branche), oder Sie schnell in Produktion gehen müssen: externer Berater spart Zeit und Risiko.

Guter Mittelweg: externer Berater fürs Setup, internes Team für den Betrieb. So bekommen Sie Geschwindigkeit und Knowhow-Transfer in einem.

I.6 Strategische Fragen

Frage 6.1

Sollte ich jetzt handeln oder noch warten, bis die Technologie reifer ist?

Die Technologie ist reif für die Standard-Use-Cases (Inbox, Outreach, Recruiting, Daten-Analyse). Wer hier wartet, verschenkt Wert.

Es gibt zwei Wartens-Argumente, die wirklich greifen: Erstens, wenn Sie in einer extrem volatilen Marktphase sind (große Restrukturierung, Verkauf des Unternehmens), sollten Sie Investitionen verschieben. Zweitens, wenn Ihre Daten-Hygiene desaströs ist (chaotische Bestandssysteme, schlechte CRM-Pflege), sollten Sie zuerst aufräumen.

In allen anderen Fällen: jetzt anfangen, Pilot starten, lernen. Die Lernkurve ist nicht trivial — wer 18 Monate später startet, hat 18 Monate weniger Erfahrung. Und Wettbewerber, die jetzt anfangen, werden in 24 Monaten substantielle Effizienz-Vorteile haben.

Frage 6.2

Wo sehen Sie KI-Agenten in fünf Jahren?

Drei Entwicklungen sehen wir mit hoher Wahrscheinlichkeit. Erstens: Agenten werden zur Standard-Infrastruktur, ähnlich wie Mail oder ERP heute. Wer keinen Inbox-Manager hat, wird das Gefühl haben, hinterherzuhinken. Wer keinen Outreach-Agent hat, wird im Vertrieb nicht mehr mithalten.

Zweitens: Modelle werden günstiger und besser, in einer Größenordnung, die heute schwer vorstellbar ist. Was heute 1.000 Euro pro Monat an Modell-Kosten ist, wird in fünf Jahren wahrscheinlich 50–100 Euro sein.

Drittens: Spezialisierte Agenten werden austauschbar. Sie kaufen einen "Recruiting-Agent für Steuerkanzleien" als Standard-Produkt, das Sie nur konfigurieren müssen. Custom-Setups bleiben für Spezialfälle.

Unsicher ist, was über die heute reifen Use Cases hinausgeht — autonome Geschäftsprozesse, KI-zu-KI-Verhandlungen, Agent-Märkte. Vielleicht. Vielleicht nicht.

Frage 6.3

Was ist der größte Fehler, den Mittelständler bei Agent-Setups machen?

Drei klassische Fehler, die wir immer wieder sehen.

Erster Fehler: zu viele Use Cases gleichzeitig. Drei Pilot-Agenten parallel, jeder ohne klare Owner — am Ende läuft keiner produktiv. Beste Strategie: ein Pilot zur Zeit, vollständig durchziehen, dann der nächste.

Zweiter Fehler: zu hohe Erwartungen am Anfang. Verkäufer versprechen 95% Automatisierung — die Realität sind 60–80% in Phase 1. Wenn die Erwartung 95% war, wirkt 70% wie Scheitern, obwohl es ein Erfolg ist.

Dritter Fehler: DSGVO und Compliance nach hinten geschoben. "Erst zum Laufen bringen, dann sauber machen" — das funktioniert nicht. DSGVO-Themen müssen von Tag 1 dabei sein, sonst muss später viel umgebaut werden.

Frage 6.4

Wie unterscheide ich seriöse Anbieter von Schaumschlägern?

Vier Kriterien.

Erstens: konkrete Cases mit Zahlen. Seriöse Anbieter zeigen ihnen reale Cases mit messbaren Ergebnissen — nicht generische Versprechen. Wenn Sie keine konkreten Cases sehen, ist das ein Warnsignal.

Zweitens: realistische Versprechen. Wer Ihnen verspricht, in 14 Tagen einen produktiven Agent mit 95% Automatisierungsgrad zu liefern, lügt entweder oder hat selbst keine Erfahrung. Seriös sind 14–30 Tage Setup, 60–80% Automatisierungsgrad in Phase 1.

Drittens: DSGVO-Bewusstsein. Seriöse Anbieter sprechen von sich aus über AVV, SCC, EU-Hosting, DSFA. Wenn Sie diese Themen erst ansprechen müssen, ist der Anbieter nicht reif für deutsche Mittelständler.

Viertens: Langfristigkeit. Frage, ob der Anbieter auch Wartung und Weiterentwicklung übernimmt — oder nur ein Setup-Geschäft macht. Der zweite Typ ist der teuerste, weil Sie dann allein dastehen.

Frage 6.5

Wenn ich nur einen Tipp aus diesem Buch mitnehme — welcher sollte es sein?

Berechnen Sie. Den Wert, die Kosten, das Risiko. Mit den Vorlagen aus Anhang D, ehrlich und konservativ.

Wenn Sie in den Zahlen einen klaren Wert sehen: starten Sie mit einem Pilot. Wenn nicht: wählen Sie einen anderen Use Case oder warten Sie ab.

Alles andere — Architektur, Anbieter, Prompts, Compliance — sind handwerkliche Fragen, die mit guter Beratung lösbar sind. Aber die Mathematik vor dem Start ist Ihre Verantwortung. Niemand sonst macht sie für Sie.

„It's predictable when you do the math.“

Dieses Dokument ist Anhang I zum Buch „PREDICTABLE — Wie KI-Agenten Ihr Business von Spielzeug zu Infrastruktur transformieren“ (Thorsten Pätzold, Amazing Agents, Pirmasens 2026). Verweise auf Kapitel beziehen sich auf das Buch, Verweise auf andere Anhänge auf die übrigen Dokumente des Werkzeugkastens.

Alle zehn Anhänge: www.amazing-agents.com/predictable.

It's predictable when you do the math.

AMAZING AGENTS

Pirmasens · 2026

www.amazing-agents.com
