

KOSTENLOSER PRAXIS-GUIDE

AI Agent geplant?

Erst Mehrwert, Kosten und Kontrolle klären.

AI AGENT DECISION & READINESS CHECK

10 Fragen, die zeigen, was schon geklärt ist – und welche Punkte vor Pilot oder Go-live noch offen sind.

Niemand muss alle Antworten kennen. Aber vor dem Go-live sollten alle Antworten geklärt sein.

Prüfen Sie Business Value, Nutzung, Identität, Daten, Datenschutz, Ownership, Lizenzierung, FinOps & Kosten, Security, Compliance und Betrieb. Weitere Stellen wie HR oder Betriebsrat werden bei Bedarf eingebunden.

Zeitersparnis ist nicht automatisch Kosteneinsparung.

Entscheidend ist, ob frei werdende Kapazität tatsächlich genutzt, Kosten vermieden oder zusätzlicher Wert geschaffen wird.

BUSINESS VALUE

NUTZUNG

LIZENZIERUNG

FINOPS

DATENSCHUTZ

SECURITY

IN 15 MINUTEN ZUR ERSTEN EINSCHÄTZUNG - GEMEINSAM ZUR ENTSCHEIDUNG

Die Checkliste ist ein gemeinsames Arbeitsblatt: Der anfordernde Fachbereich beschreibt Bedarf und Nutzen, die technischen und Governance-Rollen ergänzen Architektur, Rechte, Kosten und Betrieb.

AGENT-STECKBRIEF

Angaben eintragen – ohne Ja/Nein-Bewertung.

Agent / Use Case**Fachbereich / Antragsteller****Business Owner (Use Case & Business Value)****Maker / Agent Builder (erstellt den Agenten)****Agent Owner (Betrieb & Lifecycle)****Plattform / Runtime****Tools / Automationen****Geplanter Pilot / Go-live****Kostenstelle** z. B. Kostenstelle, Projekt-ID oder AI Cost Tag**Budgetfreigabe durch** Wer gibt Lizenz- und Verbrauchskosten frei?

SO NUTZEN SIE DEN CHECK

Ein HR-Agent als gemeinsames Beispiel

Fiktives Beispiel: Ein Unternehmen möchte einen internen AI Agent einsetzen, der wiederkehrende Fragen zu Urlaub, Reisekosten, Arbeitszeit und HR-Richtlinien beantwortet. Bei bestimmten Anliegen darf er einen definierten Workflow anstoßen.

300

Anfragen / Monat

10 Min.

manueller Aufwand heute

70 %

Ziel: direkt gelöste Standardfragen

BEISPIEL - WAS DIESE ANNAHMEN BEDEUTEN KÖNNTEN**210**

erfolgreiche Outcomes

35 Std.

frei werdende Kapazität

150 €

fiktive Agent-Kosten

0,71 €

Kosten / erfolgreichem Outcome

Annahme: 70 % direkte Antworten ohne manuellen HR-Aufwand; 30 % bleiben manuell. Bei 50 €/Std. = 1.750 € Kapazitätswert. Reines Rechenbeispiel – keine Herstellerpreise. Zeitwert ist nicht automatisch Cash-Einsparung.

AI-ACT-HINWEIS Reines HR-Q&A fällt typischerweise nicht unter die Annex-III-Personalfälle. Beeinflusst der Agent Auswahl, Bewertung, Beförderung, Kündigung, Aufgabenverteilung oder Leistungsüberwachung, Hochrisiko-Einstufung prüfen; die Annex-III-Pflichten gelten ab 02.12.2027.

WER BRINGT WELCHE PERSPEKTIVE EIN?

1 Fachbereich / Antragsteller

Kennt die häufigsten Fragen, den heutigen Ablauf, die Nutzer und das gewünschte Ergebnis.

2 Business Owner

Verantwortet fachlich Use Case und Business Value: Was soll messbar besser werden?

3 Maker / Agent Builder

Baut und konfiguriert den Agenten, z. B. in Copilot Studio, Microsoft Foundry oder einer API-basierten Runtime: Wissen, Tools, Actions und Workflows.

4 Agent Owner

Verantwortet den Agenten nach Go-live: Qualität, Änderungen, Monitoring und Lifecycle.

5 Plattform / Agent Admin

Verantwortet Runtime, Environments, Policies, Connectoren, Agent-Identitäten, Berechtigungen, Capacity und das Agenten-Inventar.

6 FinOps und Lizenzmanagement

Prüft Lizenzen, verbrauchsbasierte Nutzung, Capacity, Kosten, Cost per Outcome und wirtschaftlichen Nutzen.

Je nach Use Case kommen weitere Stellen hinzu: Datenschutz, Security und Compliance; HR/Betriebsrat nur bei Beschäftigtenbezug bzw. wenn Mitbestimmung einschlägig ist. Sie prüfen die jeweils notwendigen Guardrails vor Pilot oder Go-live.

GEMEINSAMER WEG

Bedarf → Business Value → Architektur → Lizenzierung & Kosten → Governance → Pilot → Betrieb & Messen

SO STARTEN SIE

Sie müssen nicht alles selbst beantworten. Starten Sie mit den Fragen, die Sie aus Ihrer Rolle beantworten können. Offene Punkte sind kein Fehler – sie zeigen, welche Fachstelle als Nächstes eingebunden werden muss.

1 Fachbereich startet: Use Case, Mehrwert und erwartete Nutzung vorab ausfüllen.

2 Business Owner koordiniert die Review und lädt nur die für offene Punkte nötigen Rollen ein.

3 Vorbereitung: ca. 10-15 Min. je Rolle · gemeinsame Review: ca. 30 Min.

AI AGENT READINESS CHECK

Business Value, Nutzung und Verantwortung

Die ersten fünf Fragen starten beim fachlichen Bedarf und führen Schritt für Schritt zu Daten, Autonomie und dauerhafter Ownership.

BEWERTUNG Ja = geklärt (0) · Teilweise = offene Punkte (1) · Nein = nicht geklärt (2)

1

Haben Sie geklärt, welchen konkreten Mehrwert der Agent schaffen soll und wie dieser gemessen wird?

WER SOLLTE MITDENKEN? Fachbereich / Antragsteller + Business Owner

Beschreiben Sie das heutige Problem, den gewünschten Nutzen und eine messbare Baseline, z. B. Bearbeitungszeit, Fehlerquote, Wartezeit oder Qualität.

RED FLAG Der Nutzen wird nur mit „effizienter“, „moderner“ oder „wir wollen AI nutzen“ beschrieben.

NÄCHSTER SCHRITT Ausgangswert, Zielwert und mindestens eine messbare Erfolgsgröße festlegen.

☐ Ja (0)☐ Teilweise (1)☐ Nein (2)

Notiz:

2

Haben Sie geklärt, wer den Agenten nutzen wird, wie häufig und zu welchen Spitzenzeiten?

WER SOLLTE MITDENKEN? Fachbereich / Antragsteller + FinOps und Lizenzmanagement

Schätzen Sie reale Nutzer, Vorgänge, Nutzungshäufigkeit, Adoption und Spitzenlast – nicht nur die maximal mögliche Zielgruppe.

RED FLAG Die Planung basiert auf theoretischen Nutzerzahlen statt auf erwarteter realer Nutzung.

NÄCHSTER SCHRITT Adoptionsannahme, Nutzungsvolumen und Spitzenzeiten dokumentieren.

☐ Ja (0)☐ Teilweise (1)☐ Nein (2)

Notiz:

3

Haben Sie geklärt, was der Agent selbst tun darf und in wessen Identität er handelt?

WER SOLLTE MITDENKEN? Fachbereich / Antragsteller + Maker / Agent Builder + Plattform / Agent Admin

Trennen Sie Antworten, Aktionen und autonome Ausführungen. Handelt der Agent im Auftrag eines angemeldeten Nutzers oder mit eigener Identität? Ruft er Tools oder andere Agenten auf? Definieren Sie Human Approval, Grenzen und Abbruchregeln.

RED FLAG Unklar, in wessen Identität der Agent handelt – oder Tool-/Agent-zu-Agent-Aufrufe umgehen Freigaben und Zuständigkeiten.

NÄCHSTER SCHRITT Ausführungsmodus (delegiert/autonom), Identität, erlaubte Actions/A2A-Aufrufe, Approval und Abbruchregeln dokumentieren.

☐ Ja (0)☐ Teilweise (1)☐ Nein (2)

Notiz:

4

Haben Sie geklärt, welche Daten, Tools und externen Komponenten der Agent braucht und ob sie freigegeben sind?

WER SOLLTE MITDENKEN? Fachbereich / Antragsteller + Maker / Agent Builder + Security

Klären Sie Datenquellen, APIs, Connectoren, Tools und MCP-Server. Prüfen Sie Herkunft, Aktualität, Berechtigungen und minimal notwendige Zugriffe. Kann der Agent E-Mails, Dokumente oder Webseiten mit versteckten Anweisungen verarbeiten?

RED FLAG Ungeprüfte Tools/MCP-Server oder fremde Inhalte können Verhalten beeinflussen – oder der Agent hat mehr Rechte als nötig.

NÄCHSTER SCHRITT Quellen und Tools freigeben, Trust/Provenienz prüfen, untrusted Inhalte absichern und Least Privilege umsetzen.

☐ Ja (0)☐ Teilweise (1)☐ Nein (2)

Notiz:

5

Haben Sie Ownership, Sponsor, Betrieb und Lifecycle des Agenten dauerhaft geregelt?

WER SOLLTE MITDENKEN? Business Owner + Agent Owner + Plattform / Agent Admin

Klären Sie Business Owner und Agent Owner. Bei Microsoft Entra Agent ID: Sponsor festlegen; Owner und Manager nach Bedarf ergänzen. Agent im Agenten-Verzeichnis / Agent 365 oder vergleichbarem Inventar erfassen und Übergabe bei Rollenwechsel oder Weggang regeln.

RED FLAG Der Maker verlässt das Team – und Agent, Identität, Rechte oder Betrieb hängen weiterhin an seinem persönlichen Konto.

NÄCHSTER SCHRITT Sponsor/Owner, Inventar, technische Identität, Lifecycle, Vertretung und Offboarding/Transfer dokumentieren.

☐ Ja (0)☐ Teilweise (1)☐ Nein (2)

Notiz:

AI AGENT READINESS CHECK

Lizenzierung, Kosten, Governance und Betrieb

Die zweiten fünf Fragen klären, ob der geplante Ausführungsweg lizenzierbar, wirtschaftlich steuerbar und verantwortbar betrieben werden kann.

BEWERTUNG Ja = geklärt (0) · Teilweise = offene Punkte (1) · Nein = nicht geklärt (2) · Frage 9: Nicht einschlägig = 0

6

Haben Sie geklärt, welche Lizenzen, Kapazitäten und Abrechnungsregeln für den Agenten gelten?

WER SOLLTE MITDENKEN? FinOps und Lizenzmanagement + Platform / Agent Admin

Prüfen Sie den Pfad je Runtime: M365/Copilot (USL oder UBB, Spending Policy, Credit Requests/Approval, Credits, Capacity/Pre-Purchase/PAYG), Foundry/Azure (Standard/PAYG oder PTU/Reservation) oder API (Token-/Commit-Vertrag). Falls eingesetzt, Governance-Lizenzen wie Agent 365 bzw. M365 E7 berücksichtigen.

RED FLAG Technisch bereit, aber Billing-Pfad, Capacity/Commit, Governance-Lizenz, Nutzungsrechte oder Kostenstelle sind ungeklärt.

NÄCHSTER SCHRITT Billing- und Governance-Pfad, Vertrags-/Capacity-Quelle, Kostenstelle und Consumption-Regeln dokumentieren.

☐ Ja (0)☐ Teilweise (1)☐ Nein (2)

Notiz:

7

Haben Sie realistisch abgeschätzt, welche Nutzung und Kosten entstehen können?

WER SOLLTE MITDENKEN? FinOps und Lizenzmanagement + Maker / Agent Builder

Planen Sie Low/Expected/High, Fehlversuche, autonome/langlaufende Runs, Spitzenlast und Limits. Prüfen Sie Modell-, Routing- und Default-Strategie passend zum Use Case (Advisor) und rechnen Sie bei Multi-Agent-Szenarien die gesamte Kette – nicht nur einen Modellaufruf.

RED FLAG Ein Einzelpreis ersetzt End-to-End-Forecast, Capacity-Prüfung, Modell-Right-Sizing und Limits.

NÄCHSTER SCHRITT Advisor-Benchmark, Kettenkosten, Budgetlimit, Capacity-Auslastung und Reaktion bei Überschreitung festlegen.

☐ Ja (0)☐ Teilweise (1)☐ Nein (2)

Notiz:

8

Haben Sie Agenten-Sicherheit, Datenschutz, Compliance und die AI-Act-Einstufung geklärt?

WER SOLLTE MITDENKEN? Security + Datenschutz + Compliance / Legal

Prüfen Sie zwei Ebenen: (a) Agenten-Risiken wie versteckte Anweisungen/Goal Hijack, Tool- oder MCP-Missbrauch, zu weite Rechte, Memory-/Context-Manipulation, unsichere Agent-zu-Agent-Kommunikation und technische Notabschaltung. (b) AI Act: Transparenz nach Art. 50 und Hochrisiko-Einstufung, z. B. bei Personalentscheidungen nach Anhang III.

RED FLAG Untrusted Inhalte können privilegierte Aktionen auslösen – oder AI-Act-Klassifizierung/Transparenz ist ungeklärt.

NÄCHSTER SCHRITT Threat Model, Tool-Allowlist, Least Privilege, Monitoring/Kill Switch sowie AI-Act-Einstufung und Transparenzpflicht dokumentieren.

☐ Ja (0)☐ Teilweise (1)☐ Nein (2)

Notiz:

9

Haben Sie geprüft, ob Mitbestimmung relevant ist und – falls ja – die erforderlichen Stellen eingebunden?

WER SOLLTE MITDENKEN? Fachbereich / Antragsteller + HR / Betriebsrat

Prüfen Sie, ob der Agent Arbeitsverhalten, Überwachung, Leistung, Rollen oder relevante Arbeitsprozesse berührt. Bei HR-/Beschäftigtenbezug Mitbestimmung früh prüfen; ist sie nicht einschlägig, dokumentieren Sie dies.

RED FLAG NEIN = STOPP: Ein einschlägiger Mitbestimmungstatbestand ist offen oder nicht geprüft.

NÄCHSTER SCHRITT Einschlägigkeit dokumentieren; falls erforderlich, Beteiligung vor Go-live abschließen.

☐ Ja (0)☐ Teilweise (1)☐ Nein (2)☐ Nicht einschlägig (0)

Notiz:

10

Haben Sie vor dem Go-live festgelegt, wie der Agent getestet, überwacht und bei Bedarf gestoppt wird?

WER SOLLTE MITDENKEN? Business Owner + Agent Owner + FinOps und Lizenzmanagement + Security

Definieren Sie vor Go-live Testfälle und Abnahmekriterien für Qualität, Sicherheit, Identitäten/Rechte, Tools und Fehlerszenarien. Danach Erfolgsquote, Qualität, Cost per Outcome, Retries, Vorfälle und Business-KPIs im 30/90-Tage-Review messen. Technische Notabschaltung vorsehen.

RED FLAG Go-live ohne dokumentierte Abnahme, Monitoring, Eskalationsweg oder technischen Kill Switch.

NÄCHSTER SCHRITT Abnahmetest, Monitoring, Review-Takt, Eskalation und technische Abschaltung mit Verantwortlichen festlegen.

☐ Ja (0)☐ Teilweise (1)☐ Nein (2)

Notiz:

IHR ERGEBNIS

Aus Antworten eine Go-live-Entscheidung machen

Automatische Summe und Empfehlung: in Adobe Acrobat Reader ausfüllen.

Ohne automatische Berechnung Punkte manuell addieren. STOPP-Regeln gelten unabhängig von der Summe.

Punktesumme: Noch 10 offen

Empfehlung: Bitte alle Fragen beantworten

0-4 PUNKTE**PILOTIEREN**

Grundlage weitgehend geklärt. Kontrolliert testen und Messwerte sammeln.

5-9 PUNKTE**ERST KLÄREN**

Relevante Unsicherheiten bestehen. Offene Punkte vor dem Go-live bearbeiten.

10-20 PUNKTE**STOPPEN & PRÜFEN**

Entscheidungsgrundlage reicht noch nicht. Scope, Risiken und Kosten erneut prüfen.

KRITISCHE RED FLAGS

- Frage 8 = Nein: STOPP, bis Agenten-Sicherheit / Datenschutz / Compliance / AI-Act-Einstufung geklärt sind.
- Frage 9 = Nein: STOPP nur dann, wenn Mitbestimmung tatsächlich einschlägig ist.

COST & VALUE SNAPSHOT

Für die erste Entscheidung reichen wenige Kennzahlen. Der separate AI Agent Cost Calculator ergänzt die Detailrechnung für Runs, Credits, Capacity, Cost per Outcome, ROI und Cash Payback.

Vorgänge / Monat Stk.**Erfolgsquote** %**Erwartete Agent-Kosten / Monat** €**Erfolgreiche Outcomes / Monat** Stk.**Zeitersparnis / Monat** Std.**Cost per successful outcome** €**Kapazitätswert / Monat** €**ROI / Value-Hypothese** % / €

WICHTIG Zeitersparnis ist nicht automatisch Kosteneinsparung. Keine zusätzliche Rechnung ist nicht dasselbe wie kein Ressourcenverbrauch. Bewerten Sie Kapazitätswert, reale Kosten und tatsächlichen Business Value getrennt.

ENTSCHEIDUNGSNACHWEIS

Dokumentieren Sie, wer wann welche Entscheidung getroffen hat.

Entscheidung (z. B. Pilotieren / Erst klären / Go-live)**Getroffen am****Entschieden durch****Nächster Review****AI AGENT ECONOMICS TOOLKIT**

01 DECIDE Decision & Readiness Check (dieses Dokument)

03 FORECAST Cost Calculator

02 DESIGN Use Case & Solution Advisor

04 MEASURE Outcome & Value Check

Alle Tools: lizenzfrau.de/ai-agent-economics

Feedback: kontakt@lizenzfrau.de

Methodik & Quellen: Tokenomics Foundation · Microsoft · OWASP · EU AI Act
Stand: September 2026

Herstellerangaben und Vertragsbedingungen vor dem produktiven Einsatz prüfen.