octonomy

LEITFADEN

IT-Integrations-Guide

Was Ihre IT-Abteilung wirklich tun muss, damit KI-Agenten laufen und was nicht.

Ein Leitfaden für Entscheider, die KI-Agenten einführen wollen, ohne ihre IT-Abteilung zu überfordern.

INHALT

Was in diesem Leitfaden steht

EINLEITUNG

„Das kriegen wir bei uns technisch eh nicht durch.“

In nahezu jedem Gespräch über die Einführung von KI-Agenten taucht früher oder später derselbe Satz auf. Er wird selten als Frage gestellt. Meistens ist er bereits eine Schlussfolgerung — gezogen, bevor überhaupt jemand mit der eigenen IT-Abteilung gesprochen hat.

Dieser Leitfaden trennt Annahme von Fakt. Er beschreibt konkret, was bei einer octonomy-Einführung technisch tatsächlich passieren muss, was ausdrücklich nicht notwendig ist, wer welche Aufgabe übernimmt und wie ein realistischer Zeitplan aussieht. Kein Verkaufsversprechen, sondern eine nüchterne Aufschlüsselung, damit Sie selbst beurteilen können, ob Ihre IT-Abteilung der Flaschenhals ist — oder ob es nur so aussieht.

FÜR WEN DIESER LEITFADEN GEDACHT IST

Dieser Leitfaden richtet sich an Entscheider in Kundenservice, Field Service und angrenzenden Bereichen, die ein KI-Projekt grundsätzlich für sinnvoll halten, es aber bisher zurückgestellt haben — meist mit der Begründung, die eigene IT-Abteilung sei ohnehin ausgelastet oder das Thema Datenschutz zu komplex. Wenn Sie zur eigenen IT-Abteilung bislang noch kein konkretes Gespräch über ein solches Vorhaben geführt haben, ist dieser Leitfaden die Grundlage dafür — nicht als Ersatz für das Gespräch, sondern als Vorbereitung darauf.

Er ist ausdrücklich **nicht** für IT-Abteilungen geschrieben, die bereits tief in einer technischen Evaluierung stecken. Für diesen Fall steht Ihnen ein technischer Ansprechpartner direkt zur Verfügung — siehe Abschluss dieses Leitfadens.

KAPITEL 1

Die Ausrede, die Sie sich selbst erzählen

Wenn Entscheider über KI-Projekte nachdenken, entsteht meistens zuerst ein Bild: eine überlastete, unterbesetzte IT-Abteilung, die schon mit dem Tagesgeschäft kämpft. Dieses Bild ist oft nicht falsch — aber es wird auf jedes neue Vorhaben projiziert, unabhängig davon, was dieses Vorhaben tatsächlich verlangt.

Die Folge: Der Gedanke an ein KI-Projekt endet, bevor er richtig angefangen hat. Nicht, weil jemand konkret geprüft hätte, was notwendig wäre — sondern weil die Erwartung „das wird ein monatelanges IT-Projekt“ von Anfang an feststeht. Diese Erwartung ist meistens falsch, aber sie ist bequem: Sie erlaubt es, ein Thema zu beerdigen, ohne sich ernsthaft damit auseinandersetzen zu müssen.

> *Wir kriegen doch eh nichts technisch auf die Kette — die IT blockiert alles.*
>
> Ein Satz, der in fast jeder Demo auftaucht — und fast nie an einer konkreten technischen Anforderung hängt.

Woher die Sorge tatsächlich kommt

Die Sorge vor der eigenen IT-Abteilung ist selten aktuell begründet. Sie speist sich aus einer zurückliegenden Erfahrung mit einem anderen Projekt — oft mit klassischer Softwareentwicklung, bei der tatsächlich monatelange Abstimmungsschleifen, wechselnde Anforderungen und knappe Entwicklerkapazität eine Rolle gespielt haben.

Diese Erfahrung ist real. Das Problem ist nur, dass sie automatisch auf jedes neue Vorhaben übertragen wird — auch auf solche, die technisch grundlegend anders funktionieren. Ein KI-Agent, der auf bestehende Systeme lesend zugreift, hat mit einem intern entwickelten Softwareprojekt wenig gemeinsam.

Integration heißt hier: Zugriffsfreigaben und Konfiguration statt Entwicklung. Genau diese Gleichsetzung löst dieser Leitfaden auf — nicht durch ein Versprechen, sondern durch eine nachprüfbare Aufschlüsselung der Schritte.

KAPITEL 2

Was tatsächlich technisch passieren muss

Eine octonomy-Einführung besteht aus einer überschaubaren Anzahl konkreter Schritte. Keiner davon erfordert eigene Softwareentwicklung.

AUFGABE	GESCHÄTZTER AUFWAND	TYPISCHERWEISE INVOLVIERT
Lesezugriff auf relevante Wissensquellen einrichten (z. B. SharePoint, CRM, Ticketsystem)	**ca. 30–45 Minuten**	IT-Administrator
Relevante Datenquellen und Formate benennen	**ca. 1 Stunde**	Fachbereich mit IT
Datenschutzrechtliche Prüfung / Auftragsverarbeitungsvertrag	**2–3 Tage** (rechtliche Prüfung, kein technischer Aufwand)	Datenschutzbeauftragter
API- bzw. OAuth-Freigabe für betroffene Systeme	**ca. 1 Stunde**	IT-Administrator
Ansprechpartner für punktuelle Rückfragen während der Einrichtung	**laufend, wenige Minuten pro Rückfrage**	IT oder Fachbereich

Auffällig an dieser Liste: Kein einziger Punkt erfordert eine mehrwöchige, durchgehende Bindung von IT-Kapazität. Es handelt sich um punktuelle Freigaben und kurze Abstimmungen — keine Projektphase im klassischen Sinn.

Der DSGVO-Check nimmt in der Regel am meisten Kalenderzeit in Anspruch, bindet dabei aber keine technischen Ressourcen, sondern läuft parallel zur restlichen Einrichtung.

DER ENTSCHEIDENDE UNTERSCHIED

octonomy liest aus Ihren bestehenden Systemen, statt sie zu verändern.

Das reduziert den technischen Eingriff auf ein Minimum — und ist der Grund, warum die im nächsten Kapitel beschriebenen Sorgen in den allermeisten Fällen unbegründet sind.

Typische Wissensquellen, die angebunden werden

Welche Systeme im Einzelfall relevant sind, hängt vom Anwendungsfall ab. In der Praxis handelt es sich meist um eine Auswahl aus:

- Dokumentenablagen wie **SharePoint, Google Drive** oder **Confluence**
- Ticketsysteme wie **Zendesk, Freshdesk** oder ein internes Helpdesk-Tool
- CRM-Systeme wie **HubSpot, Salesforce** oder branchenspezifische Systeme
- Technische Dokumentation, Handbücher und Schaltpläne — auch als PDF oder Scan
- ERP-Systeme, sofern strukturierte Daten wie Ersatzteillisten benötigt werden

Keine dieser Anbindungen erfordert eine Änderung am Quellsystem selbst. Es wird ausschließlich lesend zugegriffen — vergleichbar mit der Berechtigung, die auch ein neuer Mitarbeiter für seinen Aufgabenbereich erhalten würde.

Zwei Beispiele aus der Praxis

FIELD SERVICE

Ein Anbieter mit rund 40 Technikern im Außendienst benötigte für die technische Einrichtung drei Termine à 30 Minuten: Zugriffsfreigabe auf das Ticketsystem, Abstimmung der relevanten Schaltpläne und Handbücher, ein kurzer technischer Check. Die datenschutzrechtliche Prüfung lief parallel und war nach vier Werktagen abgeschlossen.

< 3 h

gesamter IT-Aufwand

KUNDENSERVICE

Ein Serviceteam mit angebundenem Ticketsystem und einer SharePoint-Wissensdatenbank benötigte lediglich eine gemeinsame Session mit IT und Fachbereich, um Zugriffsrechte zu vergeben und die relevanten Ordner zu benennen.

1 Tag

bis zur ersten Agenten-Version für interne Tests

Beide Beispiele folgen demselben Muster: Der Aufwand konzentriert sich auf wenige, klar abgegrenzte Termine — nicht auf ein durchlaufendes Projekt.

KAPITEL 3

Was NICHT passieren muss

Die folgenden Punkte werden in Discovery-Gesprächen regelmäßig als Sorge genannt — und sind in der Praxis kein Bestandteil einer octonomy-Einführung.

Keine eigene Softwareentwicklung
Es wird kein Code geschrieben, der gewartet werden muss.

Kein Umbau Ihrer Systemlandschaft
Bestehende Systeme bleiben unverändert.

Keine dedizierte Vollzeit-IT-Ressource
Der Aufwand ist punktuell, nicht durchgehend.

Keine neue Infrastruktur
Keine Neuanschaffung von Hardware.

Keine Team-Schulung
Das IT-Team muss keine neue Technologie erlernen.

Kein neues Framework
Kein Entwickler, der sich einarbeiten muss.

Der letzte Punkt trifft eine häufig unausgesprochene Sorge: dass am Ende doch wieder ein einzelner, ohnehin überlasteter Entwickler gebraucht wird, der „das nicht so einfach nebenbei macht“. Bei octonomy entfällt genau diese Abhängigkeit — die Einrichtung erfolgt über Zugriffsfreigaben und Konfiguration, nicht über kundenseitige Entwicklung.

Und die Verantwortung? Die technische Funktion des Agenten liegt bei octonomy, die fachliche Freigabe der Inhalte weiterhin bei Ihrem Team. Es entsteht keine Grauzone — die Verantwortlichkeiten sind klarer abgegrenzt als bei einer selbst entwickelten Lösung, bei der Wartung und Haftung oft an einer einzelnen Person hängen bleiben.

> *Ich baue mir inzwischen selbst Agenten für Dinge, für die ich früher tagelang auf ein Entwickler-Ticket gewartet hätte. Das ist der eigentliche Unterschied — nicht die Technik an sich, sondern dass ich nicht mehr warten muss.*
>
> Head of Tech Support · anonymisiert

Die Frage ist nicht: „Schafft unsere IT das?“ Die Frage ist: „Was genau müsste unsere IT dafür schaffen?“

KAPITEL 4

Rollenverteilung: wer macht was

Unklare Zuständigkeiten sind einer der häufigsten Gründe, warum Projekte gedanklich schon vor dem Start scheitern. Die folgende Übersicht macht die Verantwortlichkeiten explizit.

AUFGABE	OCTONOMY-TEAM	IHRE IT	FACHBEREICH
Technische Anbindung einrichten	**Umsetzung**	**Freigabe erteilen**	—
Relevante Wissensquellen benennen	Beratung	—	**Umsetzung**
Datenschutzrechtliche Dokumentation	Vorlage bereitstellen	**Prüfung / Freigabe**	—
Testen der Agenten-Antworten	**Umsetzung**	—	**Fachliche Abnahme**
Laufender Betrieb & Monitoring	**laufend**	—	Nutzung im Alltag

Ihre IT-Abteilung ist an genau zwei Stellen gefragt: Zugriffsfreigaben und datenschutzrechtliche Prüfung.

Beides sind punktuelle, klar abgrenzbare Aufgaben — keine fortlaufende Projektverantwortung. Der laufende Betrieb liegt bei octonomy, die fachliche Nutzung bei Ihrem Team.

Und wenn eine dieser Rollen intern gar nicht besetzt ist?

In kleineren Organisationen gibt es häufig keine datenschutzbeauftragte Person oder keine dedizierte IT-Administration im klassischen Sinn. Das ist kein Ausschlusskriterium: Die Freigaben können von derselben Person übernommen werden, die ohnehin für Systemzugänge zuständig ist — etwa Geschäftsführung oder externe IT-Dienstleister. Entscheidend ist nicht die Organisationsgröße, sondern dass es überhaupt eine Person gibt, die Zugriffsrechte vergeben kann.

KAPITEL 5

Die häufigsten Einwände im Detail

„Unsere Systeme sind alt und historisch gewachsen.“

Für die Anbindung reicht in aller Regel ein Lesezugriff auf bestehende Systeme — unabhängig davon, wie alt oder individuell gewachsen sie sind. Eine Ablösung oder Modernisierung ist keine Voraussetzung. Wo ein direkter Systemzugriff technisch nicht möglich ist, werden Dokumente und Exporte als Wissensquelle genutzt.

„Unsere IT hat aktuell keine Kapazität für ein neues Projekt.“

Ein berechtigter Einwand gegen ein klassisches IT-Projekt — er trifft aber nicht auf punktuelle Freigaben zu, die insgesamt wenige Stunden in Anspruch nehmen. Es entsteht keine durchgehende Projektlast, gegen die eine ohnehin ausgelastete IT-Abteilung ankämpfen müsste.

„Datenschutz wird das ohnehin nie durchwinken.“

octonomy arbeitet DSGVO-konform von Beginn an. Ein Auftragsverarbeitungsvertrag ist Standard, keine Ausnahme. Daten verlassen nicht unkontrolliert Ihr System — jede Antwort ist auf Basis Ihrer eigenen Quellen nachvollziehbar. Konkret bedeutet das:

- Verarbeitung und Hosting ausschließlich in der EU
- Klar dokumentiertes Löschkonzept für nicht mehr benötigte Daten
- Protokollierung von Zugriffen — wer wann auf welche Inhalte zugegriffen hat
- Keine Nutzung Ihrer Daten zum Training öffentlicher oder fremder KI-Modelle

Für Datenschutzbeauftragte ist damit keine Grundsatzdiskussion notwendig, sondern eine Prüfung anhand konkreter Unterlagen — ein Standardvorgang, kein Sonderfall.

„Wir hatten schon einmal ein KI-Projekt, das im Sand verlaufen ist.“

Diese Erfahrung ist häufiger ein Erwartungsmanagement-Problem als ein technisches. Viele KI-Projekte bleiben in einer endlosen Pilotphase stecken, weil Umfang und Ziel nie klar definiert wurden. octonomy arbeitet mit unit-getesteten Agenten und einem festen Zeitrahmen bis zum produktiven Go-Live — gerade um diese Art von Projekt-Limbo zu vermeiden.

„Wer haftet, wenn der Agent eine falsche Information ausgibt?“

octonomy-Agenten antworten ausschließlich auf Basis Ihrer eigenen, freigegebenen Dokumente und Systeme — nicht auf Basis von Vermutungen. Jede Ausgabe ist mit einer nachvollziehbaren Quellenangabe versehen, sodass Antworten jederzeit überprüfbar sind. Zusätzlich werden Agenten vor dem produktiven Einsatz fachlich getestet und freigegeben, ähnlich wie bei der Qualitätssicherung von Software. Verantwortlichkeiten sind dadurch von Anfang an klar zugeordnet, nicht erst im Streitfall.

„Müssen wir extra Personal einstellen, das sich um das System kümmert?“

Nein. Der laufende Betrieb — Monitoring, Wartung, technische Anpassungen — liegt bei octonomy. Auf Ihrer Seite wird lediglich eine Ansprechperson benötigt, die fachliche Rückfragen beantworten kann; das ist üblicherweise eine bereits bestehende Rolle im Fachbereich, keine Neueinstellung.

DAS MUSTER HINTER ALLEN EINWÄNDEN

Jeder dieser Einwände ist gegen ein klassisches Softwareprojekt berechtigt — und verliert seine Grundlage, sobald man prüft, was konkret verlangt wird.

KAPITEL 6

Sicherheit im Detail

Für Organisationen mit eigenem Security- oder Compliance-Team reicht eine allgemeine Zusicherung selten aus. Die folgenden Punkte sind der eigentliche Kern des internen Freigabeprozesses und lassen sich direkt an das zuständige Team weiterleiten.

01 **Verschlüsselung in transit und at rest**
Daten sind sowohl während der Übertragung als auch bei der Speicherung verschlüsselt.

02 **Rollenbasierte Zugriffskontrolle**
Zugriff auf Wissensquellen wird nur für die tatsächlich benötigten Systeme und Zeiträume vergeben, nicht pauschal.

03 **Lückenloses Audit-Log**
Protokollierung aller Zugriffe und Änderungen, jederzeit einsehbar.

04 **Verarbeitung ausschließlich in der EU**
Keine Datenübertragung in Drittstaaten ohne gesonderte Prüfung.

05 **Kein Modelltraining mit Ihren Daten**
Ihre Inhalte bleiben ausschließlich für Ihre eigenen Agenten nutzbar.

06 **Vertraglich geregelte Datenlöschung**
Klare Regelung der Löschung bei Vertragsende.

Diese Punkte ersetzen keine individuelle Sicherheitsprüfung, decken aber die Fragen ab, die in den meisten internen Freigabeprozessen zuerst gestellt werden. Für größere Organisationen empfiehlt es sich, dieses Kapitel direkt an das Security- oder Compliance-Team weiterzugeben.

KAPITEL 7

Realistische Timeline: Kickoff bis Go-Live

Die folgende Übersicht zeigt, wie sich der IT-seitige Aufwand über den Implementierungszeitraum verteilt. Auffällig: Der Aufwand konzentriert sich auf einzelne Tage, nicht auf einen durchgehenden Zeitraum.

ZEITRAUM	WAS PASSIERT	IT-AUFWAND
Tag 1–2	Kickoff, Benennung der Wissensquellen, Zugriffsfreigaben	**punktuell, ca. 1–2 Stunden**
Tag 2–3	Datenschutzrechtliche Prüfung läuft parallel	keine technische Bindung
Tag 3–10	Einrichtung und erste Tests des Agenten	keine laufende Bindung, ggf. kurze Rückfragen
Tag 10–15	Fachliche Abnahme, Feinjustierung der Antworten	kein IT-Aufwand, Fachbereich übernimmt
bis Tag 20	Produktiver Go-Live	kein zusätzlicher IT-Aufwand

< 20

Tage von Kickoff bis produktivem Go-Live

wenige Stunden

IT-Gesamtaufwand über den kompletten Zeitraum

In Summe entsteht über den gesamten Zeitraum von unter 20 Tagen ein IT-seitiger Gesamtaufwand von wenigen Stunden — verteilt auf punktuelle Freigaben und kurze Rückfragen. Kein Projektmitarbeiter wird über Wochen gebunden.

KAPITEL 8 · CHECKLISTE

Die 6 Fragen, die Sie Ihrer IT stellen sollten

Bevor Sie ein KI-Projekt für sich selbst als „technisch nicht machbar“ einstufen, lohnt sich ein kurzes, konkretes Gespräch. Diese sechs Fragen liefern in wenigen Minuten Klarheit.

01 Können wir einem externen System **Lesezugriff** auf einzelne Dokumentenablagen oder ein Ticketsystem geben, ohne die Systeme selbst zu verändern?

02 Wie lange dauert bei uns typischerweise die Freigabe eines **API- bzw. OAuth-Zugriffs** für ein einzelnes, klar abgegrenztes Vorhaben?

03 Gibt es bei uns bereits einen **Standardprozess für Auftragsverarbeitungsverträge**, oder müsste dieser neu aufgesetzt werden?

04 Wer wäre intern die richtige **Ansprechperson** für punktuelle Rückfragen während einer zwei- bis dreiwöchigen Einrichtungsphase?

05 Gibt es Systeme, bei denen selbst ein reiner Lesezugriff aus Sicherheitsgründen nicht infrage kommt — und falls ja, welche **Alternativen** (z. B. Dokumenten-Export) wären akzeptabel?

06 Was genau müsste passieren, damit dieses Vorhaben bei uns nicht als **„IT-Projekt“**, sondern als **„Freigabe mit punktuellem Aufwand“** eingestuft wird?

Wenn diese sechs Fragen beantwortet sind, verschwindet in aller Regel auch die pauschale Sorge — weil an ihre Stelle eine konkrete, prüfbare Einschätzung tritt.

KAPITEL 9

Begriffe kurz erklärt

Für alle, die diesen Leitfaden an Kolleginnen und Kollegen ohne IT-Hintergrund weiterreichen.

Lesezugriff	Eine Berechtigung, Informationen aus einem System einzusehen, ohne sie verändern zu können — vergleichbar mit einem Gast, der ein Buch lesen, aber nicht hineinschreiben darf.
API / OAuth-Freigabe	Eine technische Schnittstelle bzw. ein Berechtigungsverfahren, über das zwei Systeme kontrolliert Daten austauschen — ohne dass ein Mensch Daten manuell kopieren muss.
Auftragsverarbeitungsvertrag (AVV)	Ein datenschutzrechtlicher Standardvertrag, der regelt, wie ein Dienstleister mit personenbezogenen Daten umgehen darf. In der DSGVO-konformen Zusammenarbeit routinemäßig, kein Sonderfall.
Unit-getestet	Ein Qualitätssicherungsverfahren aus der Softwareentwicklung: einzelne Funktionsbausteine werden gezielt und wiederholbar getestet, bevor sie produktiv gehen — erst geprüft, dann live.
Quellenangabe	Der Hinweis, aus welchem Dokument oder System eine Antwort stammt — macht jede Ausgabe eines Agenten nachvollziehbar und überprüfbar, statt sie als unbelegte Behauptung stehen zu lassen.
Verschlüsselung (in transit / at rest)	Schutz von Daten während der Übertragung zwischen Systemen und während der Speicherung — vergleichbar mit einem verschlossenen Umschlag, der zusätzlich in einem verschlossenen Schrank liegt.
Audit-Log	Ein lückenloses Protokoll, das festhält, wer wann auf welche Daten zugegriffen hat — macht Zugriffe im Nachhinein nachvollziehbar, ohne manuelles Mitschreiben.
Rollenbasierte Zugriffskontrolle	Ein Berechtigungssystem, bei dem jede Person und jedes System nur genau die Zugriffsrechte erhält, die für die jeweilige Aufgabe notwendig sind — nicht mehr und nicht weniger.

KURZ ZUSAMMENGEFASST

Jedes Kapitel in einem Satz

Für alle, die diesen Leitfaden weiterleiten oder in fünf Minuten intern zusammenfassen müssen.

KAPITEL 1	Die Annahme „unsere IT schafft das nie“ entsteht meistens vor jeder konkreten Prüfung — nicht danach.
KAPITEL 2	Technisch notwendig sind Zugriffsfreigaben, benannte Datenquellen und eine datenschutzrechtliche Prüfung — zusammen wenige Stunden Aufwand.
KAPITEL 3	Nicht notwendig sind eigene Entwicklung, Systemumbauten und eine dauerhaft gebundene IT-Ressource.
KAPITEL 4	Ihre IT ist an genau zwei Stellen gefragt — Freigaben und Datenschutzprüfung, nicht am laufenden Betrieb.
KAPITEL 5	Die häufigsten Einwände — alte Systeme, Kapazität, Datenschutz, gescheiterte Vorprojekte, Haftung, Personalbedarf — halten einer konkreten Prüfung meist nicht stand.
KAPITEL 6	Verschlüsselung, Zugriffskontrolle und Audit-Logs sind Standard, nicht Sonderwunsch — relevant vor allem für Security- und Compliance-Teams.
KAPITEL 7	Der IT-Aufwand verteilt sich auf einzelne Tage innerhalb eines 20-Tage-Zeitraums, nicht auf den gesamten Zeitraum.
KAPITEL 8	Sechs konkrete Fragen an die eigene IT-Abteilung ersetzen die pauschale Vermutung durch eine geprüfte Einschätzung.
KAPITEL 9	Die zentralen Fachbegriffe verständlich erklärt, damit auch Nicht-Techniker im Unternehmen mitreden können.

ABSCHLUSS

Der ehrliche Test

Wenn Sie diesen Leitfaden bis hierhin gelesen haben, kennen Sie jetzt den tatsächlichen Umfang dessen, was Ihre IT-Abteilung leisten muss — und was nicht. Die nächste Frage beantworten Sie am besten nicht mit einer Vermutung, sondern mit einem kurzen, konkreten Gespräch.

Kein Angebot. Kein Verkaufsgespräch. Nur die ehrliche Antwort, ob Ihre IT das stemmen kann.

15 Minuten, technisch

Gespräch mit einem technischen Ansprechpartner — nicht mit einer Vertriebsperson. Ohne Verpflichtung, ohne Pitch.

Keine Vorbereitung nötig

Es reicht, wenn Sie grob wissen, welche Systeme bei Ihnen im Einsatz sind. Alles Weitere klären wir gemeinsam.

Inklusive einer ersten, ehrlichen Einschätzung, ob und wie schnell eine Umsetzung bei Ihnen realistisch ist.

octonomy.ai ↗

15-MINUTEN-TERMIN BUCHEN

octonomy

Die beste KI-Plattform für komplexes Wissen

octonomy verbindet Ihre Datenquellen, Dokumente und Systeme zu KI-Agenten, die wiederkehrende Anfragen zuverlässig und nachvollziehbar bearbeiten — im Kundenservice, im Field Service und in weiteren Bereichen mit hohem Anteil an wissensbasierten Anfragen.

Jede Antwort ist mit einer nachvollziehbaren Quellenangabe versehen. Agenten werden vor dem produktiven Einsatz unit-getestet, vergleichbar mit klassischer Softwarequalitätssicherung. Die Einführung erfolgt DSGVO-konform, direkt angebunden an Ihre bestehenden Systeme, produktiv in unter 20 Tagen.

96 %
Genauigkeit — keine Halluzinationen

< 20
Tage bis zum produktiven Go-Live

EU
Hosting & Verarbeitung, DSGVO-konform

Dieser Leitfaden ist Teil einer Reihe, die konkrete, oft unausgesprochene Fragen rund um die Einführung von KI-Agenten beantwortet — ohne Verkaufsrhetorik, mit Fokus auf das, was in der Praxis tatsächlich zählt.