abamix
AI. Applied. Governed.

EXECUTIVE PAPER · NOVEMBER 2026

Agentic AI in der Enterprise-Architektur

Was Entscheider über autonome Agenten und die Rolle der Enterprise-Architektur wissen müssen

AUTOR Prof. Dr. Amadou Sienou, abamix GmbH, Stuttgart

VERSION 1.0

DATUM 06.11.2026

STATUS Freigegeben

www.abamix.com

ÜBERSICHT

Inhalt

	Das Wichtigste in Kürze	3
1	Warum Agentic AI eine Architekturfrage ist	4
2	Was sich in den drei Domänen ändert	5
3	Neue Betriebsrisiken	7
4	Die EA-Funktion als Steuerungsinstanz	8
5	Governance in vier Schichten — und wie sie technisch greift	10
6	Der regulatorische Rahmen	12
7	Was bei Ihnen zu entscheiden ist	14
8	So unterstützt abamix	15
	Quellen	16

Das Wichtigste in Kürze

Agentic AI ist keine IT-Technologiefrage, sondern eine Enterprise-Architektur-Frage.

Agentic KI-Systeme sind autonome Agenten, die Ziele selbständig planen, Werkzeuge aufrufen und Entscheidungen sequenziell treffen. Sie greifen gleichzeitig in Business Architecture, Informationssystem-Architektur und Infrastruktur-Architektur ein — kontinuierlich, weil Modell-Updates das Verhalten ohne internen Release verändern, und dezentral, weil Fachbereiche beginnen, bevor die Strukturen bereitstehen.

- **Business Architecture:** Prozesse müssen als Zielarchitektur definiert sein, bevor ein Agent gebaut wird.
- **Informationssystem-Architektur:** Agenten sind eine neue Applikationsklasse und eine neue Akteurskategorie mit eigenen Integrationsmustern, Datenzugriffsanforderungen und Lebenszykluseigenschaften.
- **Infrastruktur-Architektur:** Sie ist Enabler, aber nicht primärer Engpass. Die Engpässe liegen in API-Governance, Datenqualität und Sicherheitsarchitektur.
- **Betrieb:** Data Drift, Model Drift, Bias und Halluzination verlangen eine eigene Monitoring-Architektur, die über klassisches IT-Monitoring hinausgeht.
- **Governance:** Sie wirkt nur in vier aufeinander aufbauenden Schichten — strategisch, architektonisch, operativ und technisch.

Was bei Ihnen zu entscheiden ist: Wer verantwortet die Entscheidungen Ihrer Agenten? Wie viel Autonomie lassen Sie zu? Und wo beginnen Sie — bei der Governance, bei der laufenden Nutzung oder bei der ersten Spezifikation?

KAPITEL

01

Warum Agentic AI eine Architekturfrage ist

Enterprise-Architektur verbindet Strategie und Betrieb. In TOGAF [1] gliedert sie sich in drei Domänen: Business Architecture, Informationssystem-Architektur und Infrastruktur-Architektur. Frühere Technologiewellen ließen sich einer dieser Domänen zuordnen: Cloud Computing der Infrastruktur, ERP-Standardisierung der Informationssystem-Architektur, Lean-Methoden der Business Architecture.

Agentic AI betrifft alle drei zugleich. Ein Agent im Einkaufsprozess definiert die Capability „Lieferantenbewertung“ neu, bildet eine neue Applikationsklasse mit Zugriff auf ERP und Stammdaten und verlangt neue Plattform- und Sicherheitskomponenten.

Entscheidend sind zwei Eigenschaften: Der Änderungsimpuls ist kontinuierlich, und der Adoptionsimpuls ist dezentral. Ohne Steuerung entsteht, was Enterprise-Architektur historisch verhindern soll: redundante Agenten, inkompatible Datenmodelle, inkonsistente Compliance-Standards und Tool-Integrationen, die niemand wiederverwenden kann.

Ein Copilot, der auf eine Anfrage antwortet, ist kein Agent. Ein System, das eigenständig eine Einkaufsanfrage analysiert, Lieferantendaten aus dem ERP abruft, eine Bewertungsmatrix erstellt und eine Empfehlung produziert, ist ein Agent.

KAPITEL

02

Was sich in den drei Domänen ändert

Business Architecture. Der Zielprozess muss vor der Agent-Implementierung vollständig definiert sein. Wer diesen Pfad verkürzt, skaliert die Qualitätsmängel des Ist-Prozesses, statt sie zu beseitigen. Das Betriebsmodell erhält eine dritte Akteurskategorie: autonome Systeme, die kognitive Zwischenarbeit ausführen und im Fehlerfall an menschliche Rollen eskalieren. Die Prüffrage lautet nicht, ob ein Agent einen Prozess verbessern kann, sondern ob die Capability strategisch relevant genug ist, um Investition und Governance-Aufwand zu rechtfertigen.

Informationssystem-Architektur. Agenten arbeiten probabilistisch, über mehrere Schritte und mit breitem Tool-Zugriff über Systemgrenzen; ihr Verhalten ändert sich ohne formalen Release. Sie sind zugleich Akteure im Prozessmodell: Jeder Agent braucht einen namentlich benannten Agent-Owner, einen definierten Entscheidungsrahmen und Eskalationspfade. Ein konsistentes Schichtenmodell ordnet die Bausteine den EA-Domänen zu:

BUSINESS-SCHICHT	Prozesse, Capabilities, Rollen (Business Architecture Domain)
MOTIVE GATEWAY	Governance-Enforcement PDP/PEP · CO-1 bis CO-5 · EU AI Act
ORCHESTRIERUNGS-SCHICHT	Agent-Koordination, Routing, Human-in-the-Loop-Mechanismen
KOGNITIONS-SCHICHT	LLM-Inference, RAG, Memory, Reasoning-Framework
TOOL-SCHICHT	Tool-Registry, Berechtigungs- kontrolle, Adapter, Logging
INTEGRATIONS-SCHICHT	API-Gateway, Connectoren, Event-Streams, ERP-Adapter
DATEN-SCHICHT	Strukturierte Daten (ERP, CRM), Vektordatenbanken (RAG-Corpus), Master Data, Evidence Store
INFRASTRUKTUR-SCHICHT	Cloud, Compute, Netzwerk, Sicherheit (Infrastruktur-Architektur Domain)

Abbildung 1: Ein konsistentes Schichtenmodell für agentic Systeme in Konzernumgebungen

Infrastruktur-Architektur. Cloud-Infrastrukturen unterstützen agentic Workloads prinzipiell. Neu sind die Angriffsflächen, allen voran Prompt Injection und übermäßige Handlungsbefugnis von Agenten [2]. Die Wahl zwischen externer API, internem Deployment und Hybridansatz ist eine Architektur- und Business-Entscheidung; für deutsche Konzerne in regulierten Branchen ist der Hybridansatz typischerweise der geeignete Einstieg. Als grobe Orientierung kosten agentic Tasks fünf- bis fünfzehnmal mehr als Single-Turn-Interaktionen; Governance gehört deshalb als Betriebskosten-Komponente in den Business Case.

> **Frage an Ihre Organisation:** Ist jeder produktive Agent als eigene Applikationsklasse im Application Portfolio erfasst — mit einer namentlich benannten verantwortlichen Person?

KAPITEL

03

Neue Betriebsrisiken

Agentic Systeme haben Qualitätsprobleme, die bei klassischer Software nicht existieren und die klassische Softwaretests nicht erkennen. Sie entstehen durch Veränderungen der Umwelt oder durch Eigenschaften der statistischen Lernmodelle selbst, nicht durch Programmier- oder Konfigurationsfehler.

Risiko	Was geschieht	Wie es sichtbar wird
Data Drift	Eingabedaten verändern sich, etwa durch neue Terminologie oder neue ERP-Versionen	Statistische Verteilung der Eingaben
Model Drift	Anbieter-Updates verändern das Verhalten, ohne dass intern Code geändert wurde	Behavioral-Test-Score nach Modell-Update
Process-Level Bias	Historische Muster und ungleich repräsentierte Bereiche verzerren Entscheidungen	Akzeptanzraten nach Nutzersegmenten
Halluzination	Plausibel formulierte, faktisch falsche Aussagen	Stichprobenbasierte Review-Rate, Quellenabweichungs-Rate
Rückkopplung	Mitarbeitende akzeptieren Agenten-Outputs systematisch, statt sie zu bewerten	Ablehnungsrate von Agenten-Empfehlungen

Für Hochrisiko-Systeme verlangt der EU AI Act zusätzlich eine Beobachtung nach dem Inverkehrbringen durch den Anbieter und eine Überwachung des Betriebs durch den Betreiber [3].

> **Frage an Ihre Organisation:** Bemerken Sie heute, wenn ein Modell-Update des Anbieters das Verhalten eines produktiven Agenten verändert?

KAPITEL

04

Die EA-Funktion als Steuerungsinstanz

Die zentrale EA-Leistung ist nicht die Gestaltung einzelner Domänen, sondern die Sicherstellung ihrer Konsistenz. Fehlt sie, entstehen typische Lücken auf drei Achsen:

Alignment-Achse	Typische Lücke ohne EA-Steuerung	Konsequenz
Business–IS	Agent ohne dokumentierten Capability-Bezug implementiert	Falsche Automatisierung; strategisch nicht ausgerichtete Investition
IS–Infrastruktur	Datenzugriffsanforderung überschreitet Infrastrukturlatenz	Produktionsausfall; Agent nicht betreibbar
Business–Infrastruktur	Compliance-Anforderung bestimmt nicht das Deployment-Modell	Regulatorische Exposition; nachträgliche Architekturänderung

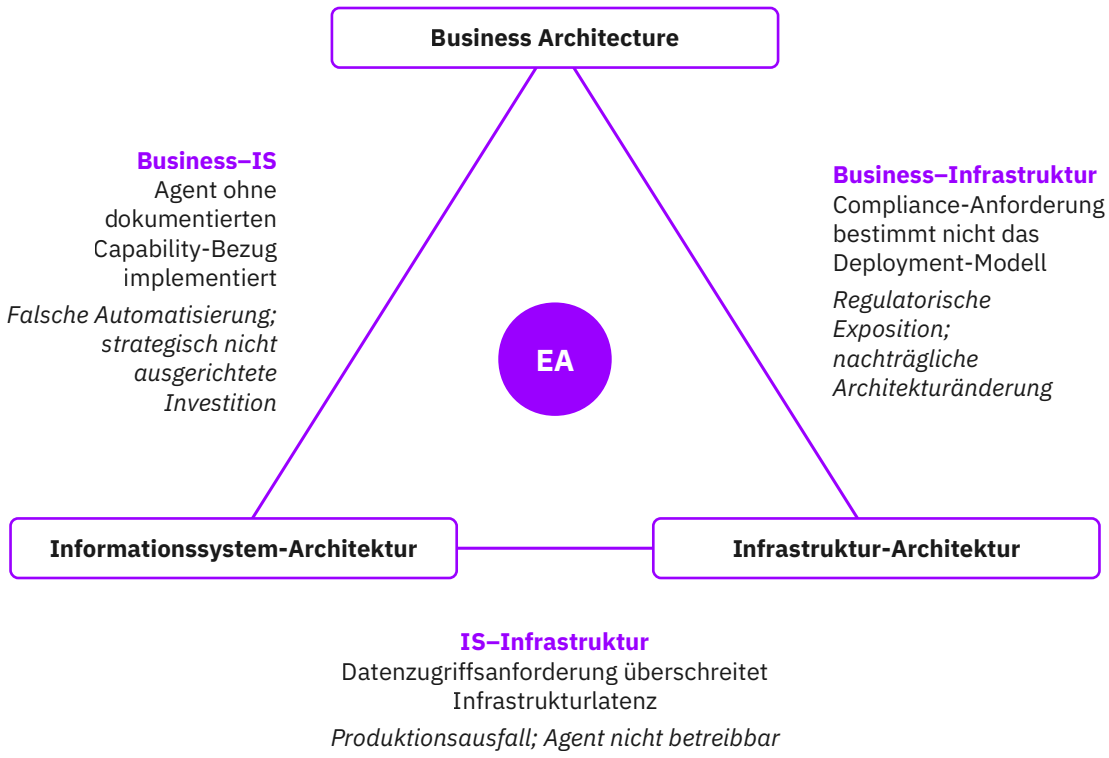


Abbildung 2: Die Alignment-Aufgabe: Kohärenz über alle Domänen

Wirksam wird diese Steuerung erst mit Entscheidungsrechten, Pflichtpfaden und Sanktionsmechanismen. Das Architecture Review Board hat ein Veto-Recht für neue Agent-Typen und für LLM-Anbieter außerhalb der Approved-Liste. Drei Gates — Konzeption, Pre-Implementation und Go-Live — verlangen definierte Pflichtartefakte, von der EU-AI-Act-Klassifikation bis zum Behavioral-Test-Corpus. Nach dem Subsidiaritätsprinzip entscheiden Domain-Architekten allein, was ihre Domäne betrifft, etwa Prompt-Optimierung oder Tool-Auswahl innerhalb der Bibliothek.

> **Frage an Ihre Organisation:** Hat Ihr Architecture Review Board ein Veto-Recht für neue Agent-Typen und für LLM-Anbieter außerhalb der Approved-Liste?

KAPITEL

05

Governance in vier Schichten — und wie sie technisch greift

In der McKinsey-Erhebung „The state of AI in early 2024“ (n = 1.363) geben 72 % der Befragten an, dass ihre Organisation KI einsetzt; nur 18 % berichten von einem unternehmensweiten Gremium mit Entscheidungsbefugnis für Responsible-AI-Governance [6]. Governance bleibt in diesen Fällen ein Richtliniendokument. Wirksame AI Governance baut vier Schichten aufeinander auf:

Schicht 1 — Strategische Governance: ein namentlich benannter AI Risk Owner, ein AI Governance Committee und die Verankerung von AI-Risiken im Enterprise Risk Management.

Schicht 2 — Architektur-Governance: die Kernkompetenz der EA-Funktion mit Principles, Architecture Review Board und Gates.

Schicht 3 — Operative Governance: Continuous Governance nach dem Go-Live, Incident Response für agentic Systeme und die Selbstbewertung des Governance-Reifegrads.

Schicht 4 — Technische Governance-Infrastruktur: Policy-as-Code am Policy Decision Point, ein Evidence Store als kryptografisch gesicherter Audit-Trail und ein automatisiertes Portfolio-Register.

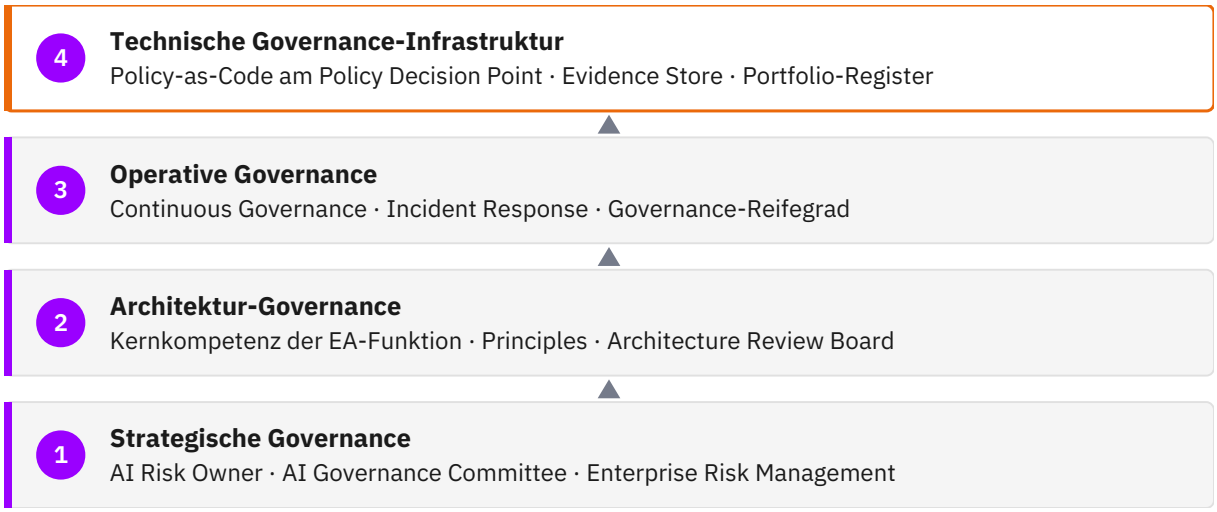


Abbildung 3: AI Governance in vier Schichten: Schicht 4 setzt Schichten 1 bis 3 voraus

Die Reihenfolge entscheidet. Konzerne im Initial-Status sollten nicht primär in technische Governance-Infrastruktur investieren, sondern zuerst einen AI Risk Owner benennen, Principles dokumentieren und das Review Board einrichten.

Schicht 4 lässt sich als Middleware nach dem Muster Policy Decision Point / Policy Enforcement Point umsetzen. Das MOTIVE Gateway prüft jede LLM-Anfrage vor der Ausführung gegen fünf Control Objectives, leitet Hochrisiko-Anfragen an einen menschlichen Reviewer mit dokumentierter Freigabeentscheidung und schreibt einen unveränderlichen Audit-Trail [7]. Im Proof-of-Concept mit 200 synthetischen Aufgaben in acht regulierten Domänen stieg die Rate erfolgreicher Audit-Rekonstruktionen von 0,31 auf 0,94; die Rekonstruktionszeit sank von 4,2 auf 0,8 Stunden. Die Baseline ist aus Survey-Daten und Expertenbefragungen abgeleitet; die Verbesserungsquoten sind Größenordnungsschätzungen, keine experimentell verifizierten Kausalaussagen. Externe Replikation steht aus. Das Gateway erzwingt Policies, es ersetzt nicht die Schichten 1 bis 3.

> **Frage an Ihre Organisation:** Gibt es bei Ihnen einen namentlich benannten AI Risk Owner mit Berichtslinie zum Vorstand?

KAPITEL

06

Der regulatorische Rahmen

Der EU AI Act (Verordnung (EU) 2024/1689) [3] macht die Risikoklasse eines Agenten zur Architekturanforderung. Verbote gelten seit 2. Februar 2025, Transparenzpflichten nach Art. 50 seit 2. August 2026. Mit dem Digital Omnibus (Verordnung (EU) 2026/1744) wurden die Hochrisiko-Pflichten verschoben: für eigenständige Hochrisiko-Systeme nach Anhang III auf den 2. Dezember 2027, für KI als Sicherheitsbauteil von Produkten nach Anhang I auf den 2. August 2028 [4]. Die Verschiebung ist ein Zeitfenster für den Architekturaufbau, kein Aufschub der Klassifikation.

Risikoklasse	Typische Konzern-Use-Cases	Architektonische Mindestanforderungen
Minimal Risk	Internes Reporting, Dokumentenverarbeitung, Wissensassistenz	Keine regulatorischen Vorgaben; Best Practice empfohlen
Limited Risk	Kundeninteraktion, externe Chatbots	Transparenzpflicht (Art. 50): Nutzer muss über KI-Interaktion informiert sein
High Risk	HR-Agenten (Anhang III Nr. 4), Kreditwürdigkeitsprüfung natürlicher Personen (Anhang III Nr. 5), Sicherheitsbauteile kritischer Infrastruktur (Anhang III Nr. 2)	Risikomanagementsystem, Datengovernance-Doku., menschliche Aufsicht by Design, Konformitätsbewertung, laufendes Monitoring
Prohibited	Social Scoring, Emotionserkennung am Arbeitsplatz, biometrische Echtzeit-Fernidentifizierung im öffentlichen Raum zu Strafverfolgungszwecken (eng begrenzte Ausnahmen)	Unzulässig (Art. 5)

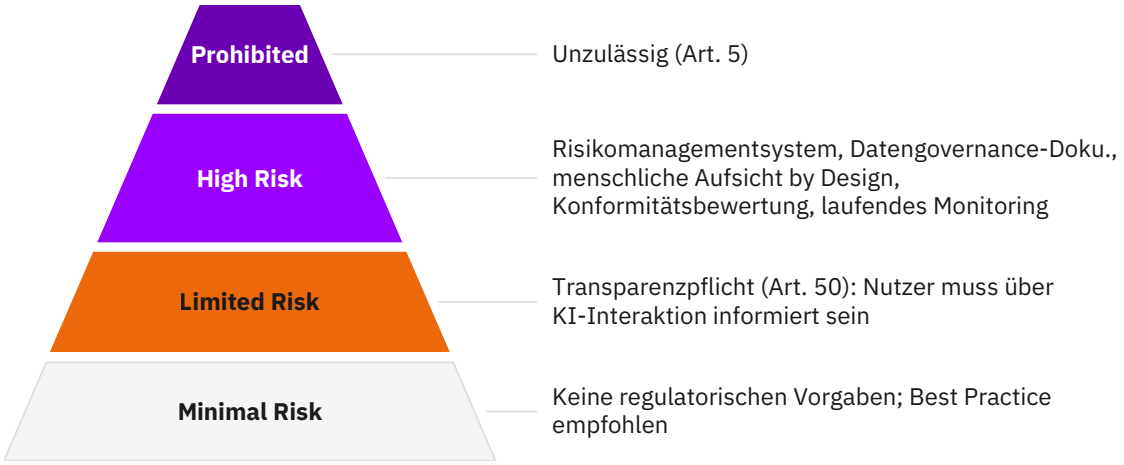


Abbildung 4: EU AI Act: Risikoklassen und architektonische Mindestanforderungen

Ob ein Agent in eine Hochrisiko-Kategorie fällt, bestimmt die Business Architecture, nicht die IT-Implementierung. Für HR- und Kreditentscheidungs-Agenten kommt Art. 22 DSGVO hinzu: Ein nominaler Human-in-the-Loop reicht nicht aus, wenn der Prüfer faktisch keine inhaltliche Prüfung vornehmen kann [5].

> **Frage an Ihre Organisation:** Ist jeder geplante Agent nach EU AI Act klassifiziert, bevor die technische Designarbeit beginnt?

KAPITEL

07

Was bei Ihnen zu entscheiden ist

Drei Entscheidungen liegen bei Ihnen:

1. **Verantwortung:** Wer ist AI Risk Owner, und wer verantwortet als Agent-Owner jeden einzelnen Agenten?
2. **Autonomie:** Welche Entscheidungen dürfen Agenten selbst treffen, und wo ist menschliche Prüfung architektonisch verbindlich?
3. **Einstieg:** Beginnen Sie bei der Governance-Grundlage, bei der bereits laufenden Nutzung oder bei der ersten Spezifikation?

Die Umsetzung folgt drei Horizonten. Im Fundament (3–6 Monate) entstehen AI Architecture Principles, die EU-AI-Act-Klassifikation, das Agent-Portfolio-Register und ein benannter AI Risk Owner. In der Skalierung (6–18 Monate) werden Standards operationalisiert: Tool-Adapter-Bibliothek, RAG-Standard, Monitoring und Incident Response. In der Transformation (18–36 Monate) wird AI Governance zur regulären Funktion. Horizont 1 muss abgeschlossen sein, bevor Horizont 2 skaliert.

Die häufigste Fehlinvestition ist technische Governance-Infrastruktur ohne strategische und prozedurale Governance-Grundlage.

KAPITEL

08

So unterstützt abamix

Wo Sie beginnen, hängt von Ihrer Ausgangslage ab. Diese Angebote schließen die Lücken, die dieses Paper beschreibt.

Executive Briefing Session
Ihr Führungsgremium klärt Steuerungsmodi, die Klassifizierung der Agentenautonomie, Entscheidungsrechte und Eskalation sowie die Risikobereitschaft.

AI Operating Model Assessment
Sie erhalten ein evidenzbasiertes Reifegradprofil über die acht Bausteine Ihres Betriebsmodells, eine Lückenanalyse je Baustein und eine sequenzierte Roadmap mit Abhängigkeiten.

AI Intervention
Nutzen Ihre Teams KI bereits uneinheitlich, überführen wir genau drei Arbeitsfälle in einen Soll-Workflow mit dokumentierten Entscheidungsregeln, Quality Gates, Rollen und Eskalationen.

Sovereign AI Architecture
Sie erhalten die Zielarchitektur für den gesteuerten KI-Betrieb: Agent Registry mit Verantwortlichkeiten, Steuerungsmodus je Agent, Design der Policy-Enforcement-Schicht, Architektur der Audit-Nachweise und eine Deployment-Entscheidung.

AI Managed Governance
Wir pflegen mit Ihnen das Agenten- und Modellregister und das Policy Pack, überprüfen den Steuerungsmodus je Agent und bereiten die Nachweise für Interne Revision und Aufsicht auf.

Quellen

Rechtsstand und Online-Quellen: 6. November 2026.

[1] The Open Group (2022): The TOGAF Standard, 10th Edition. Reading: The Open Group.

[2] OWASP Foundation (2024): OWASP Top 10 for LLM Applications 2025 (LLM01 Prompt Injection, LLM06 Excessive Agency).

[3] Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (KI-Verordnung). ABl. L, 12.7.2024.

[4] Verordnung (EU) 2026/1744 (Digital Omnibus zur KI-Verordnung), ABl. vom 24.7.2026, in Kraft seit 27.7.2026.

[5] Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung). ABl. L 119 vom 4.5.2016.

[6] McKinsey & Company (2024): The state of AI in early 2024: Gen AI adoption spikes and starts to generate value, 30.05.2024. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-2024

[7] Sienou, A. (2026): MOTIVE Gateway: Architectural Enforcement of AI Governance for Enterprise LLM Integration. In: Proceedings of the 28th International Conference on Enterprise Information Systems (ICEIS 2026), Bd. 2, S. 1633–1640. SCITEPRESS. DOI: 10.5220/0014970100004018.

KONTAKT

Ansprechpartner

Prof. Dr. Amadou Sienou

abamix GmbH, Stuttgart

info@abamix.com · www.abamix.com

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

IMPRESSUM

Herausgeber	abamix GmbH · Lothringerstr. 11 · 70435 Stuttgart
Dokument	Executive Paper — Kurzfassung des Whitepapers „Agentic AI in der Enterprise-Architektur“ (Leseausgabe v3.8) · Agentic AI in der Enterprise-Architektur
Version	1.0 · 06.11.2026 · Status: Freigegeben
Autor	Prof. Dr. Amadou Sienou, abamix GmbH, Stuttgart
Zitiervorschlag	Sienou, A. (2026). *Agentic AI in der Enterprise-Architektur: Was Entscheider über autonome Agenten und die Rolle der Enterprise-Architektur wissen müssen*. Executive Paper, Version 1.0. 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