
KI-Agenten in regulierten Umfeldern

Leitfaden für Entscheider in Gesundheitswesen, Versicherung und KRITIS

Whitepaper | März 2026



Simon Schilling

Geschäftsführer & Principal Consultant

Nexus Management Consulting GmbH | nexuscon.net

Management Summary

KI-Agenten – autonome Software-Einheiten, die Aufgaben planen, ausführen und Entscheidungen treffen – verändern die Art, wie Unternehmen arbeiten. Gartner prognostiziert, dass bis 2028 ein Drittel aller Enterprise-Software agentenbasierte KI-Funktionen enthalten wird. McKinsey schätzt das Marktvolumen für Agentic AI bis 2030 auf über 2 Billionen USD.

Für Unternehmen in regulierten Branchen – Gesundheitswesen, Versicherung, KRITIS, öffentliche Verwaltung – gelten besondere Spielregeln: EU AI Act, NIS2, DSGVO und branchenspezifische Anforderungen schaffen einen Rahmen, der bei der Einführung von KI-Agenten von Tag eins berücksichtigt werden muss. Gleichzeitig bietet genau diese Komplexität eine Chance: Wer KI compliant-by-design einführt, schafft einen nachhaltigen Wettbewerbsvorteil.

Kernfrage

Dieses Whitepaper gibt Entscheidern einen praxisnahen Leitfaden: Was sind KI-Agenten? Wo liegt der konkrete Mehrwert? Welche regulatorischen Anforderungen gelten? Und wie gelingt die Einführung – Schritt für Schritt, compliant-by-design?

1. Was sind KI-Agenten?

Der Begriff „KI-Agent“ beschreibt eine neue Kategorie von Software: Programme, die nicht nur einzelne Aufgaben automatisieren, sondern eigenständig Ziele verfolgen, Pläne erstellen und Werkzeuge nutzen können. Im Gegensatz zu klassischen Chatbots oder RPA-Bots können KI-Agenten mehrstufige Aufgaben orchestrieren, auf unerwartete Situationen reagieren und aus Erfahrung lernen.

Die technologische Grundlage bilden Large Language Models (LLMs) wie GPT-4, Claude oder Gemini, die um Werkzeuge (Tool Use), Speicher (Memory) und Planungsfähigkeiten (Reasoning) ergänzt werden. In Kombination mit Plattformen wie UIPath, LangChain oder Microsoft Semantic Kernel entstehen Agenten, die reale Geschäftsprozesse abbilden können.

1.1 Abgrenzung: Drei Generationen der Automatisierung

Um KI-Agenten einzuordnen, hilft ein Blick auf die Evolution der Prozessautomatisierung. Jede Generation erweitert die Fähigkeiten der vorherigen, ersetzt sie aber nicht vollständig:

Kriterium	Gen 1: RPA	Gen 2: Intelligent Automation	Gen 3: Agentic AI
Daten	Strukturiert	Strukturiert + Dokumente	Unstrukturiert (Freitext, Scans)
Logik	Wenn/Dann-Regeln	Regeln + ML-Klassifikation	Kontextverständnis, Planung
Ausnahmen	Bricht ab	Eskaliert	Löst eigenständig oder eskaliert
Anpassung	Umprogrammierung	Modell-Retraining	Prompt-Anpassung, Feedback

Compliance	Audit-Log	Audit-Log + Modell-Doku	EU AI Act Risikoklassifizierung
------------	-----------	-------------------------	------------------------------------

1.2 Die drei Autonomiegrade

Nicht jeder KI-Agent muss autonom handeln. Gerade in regulierten Umfeldern – wo Fehler direkte Auswirkungen auf Kunden, Patienten oder die öffentliche Sicherheit haben können – ist eine bewusste Abstufung der Autonomie entscheidend:

Autonomiegrad	Rolle Agent	Rolle Mensch	Beispiel
Assistierend	Schlägt vor	Entscheidet immer	Dokumentenklassifizierung mit Vorschlag
Teil-autonom	Handelt in Grenzen	Prüft Ausnahmen	Auto-Nachforderung bei fehlenden Unterlagen
Autonom	Handelt selbstständig	Stichproben	Standardantworten auf Routineanfragen

Praxis-Tipp

Empfehlung: Starten Sie immer mit assistierenden Agenten. Sammeln Sie Vertrauen, Daten und Erfahrung, bevor Sie die Autonomie schrittweise erweitern.

2. Praxisbeispiel: KI-Agenten-Netzwerk im Gesundheitswesen

Ein Unternehmen im Gesundheitswesen (GKV/KRITIS) hat fünf spezialisierte KI-Agenten eingeführt, um den End-to-End-Prozess der Kundenanliegenbearbeitung zu automatisieren. Das Projekt wurde von Nexus als neutralem Programm-Manager gesteuert, die Implementierung erfolgte durch einen spezialisierten Technologiepartner.

Die zentrale Erkenntnis: Nicht ein einzelner „Super-Agent“ automatisiert den Prozess, sondern ein Netzwerk aus spezialisierten Agenten, die jeweils einen klar abgegrenzten Teilprozess übernehmen.

Agent	Aufgabe	Autonomie	Technologie
1. Klassifikator	Eingehende Anliegen verstehen und routen	Teil-autonom	LLM + UIPath Maestro
2. Vollständigkeitsprüfer	Unterlagen auf Vollständigkeit prüfen	Teil-autonom	DocumentUnderstanding
3. Bestandsabgleicher	Daten mit Kernsystemen abgleichen	Autonom	API-Integration
4. Antwortgenerator	Individuelle Antwortvorschläge formulieren	Assistierend	LLM mit Fachvorlagen
5. SLA-Monitor	Fristen überwachen und eskalieren	Autonom	Regelbasiert + KI-Prognose



Ergebnisse nach 3 Monaten

- Bearbeitungszeit um 60 % reduziert (von Ø 12 Tagen auf Ø 5 Tage)
- Fehlerquote um 40 % gesenkt (insbesondere bei der Vollständigkeitsprüfung)
- Mitarbeitende fokussieren sich auf komplexe Einzelfälle statt auf Routinevorgänge
- Compliance-Framework (Sozialdaten-Governance, EU AI Act) von Tag eins integriert
- Keine Datenschutzvorfälle seit Go-Live

Lessons Learned

Drei zentrale Erkenntnisse aus dem Projekt, die sich auf andere regulierte Umfeldern übertragen lassen:

- **1. Datenschutz als Enabler:** Die frühzeitige Einbindung des Datenschutzbeauftragten hat die DSFA-Durchlaufzeit von 8 auf 3 Wochen reduziert. In regulierten Umfeldern ist der Datenschutz kein Blocker, sondern ein Beschleuniger – wenn er früh eingebunden wird.
- **2. Spezialisierung schlägt Generalisierung:** Ein einzelner „Super-Agent“ wäre nicht beherrschbar gewesen. Fünf spezialisierte, einfache Agenten sind leichter zu testen, zu dokumentieren und bei Bedarf einzeln anzupassen. Die Orchestrierung über die UIPath-Plattform liefert zudem ein zentrales Monitoring.
- **3. Autonomiegrad ist verhandelbar:** Die initiale Planung sah vor, dass Agent 4 (Antwortgenerator) autonom arbeitet. Nach dem PoC wurde der Autonomiegrad auf „assistierend“ reduziert, weil die Sachbearbeiter die generierten Antworten fachlich validieren wollten. Flexibilität im Autonomiegrad ist entscheidend.

3. Regulatorischer Rahmen

Unternehmen in regulierten Branchen müssen bei der Einführung von KI-Agenten drei zentrale Regelwerke beachten. Diese sind kein Hindernis, sondern ein Qualitätsrahmen: Wer sie von Anfang an berücksichtigt, vermeidet kostspielige Nacharbeit.

3.1 EU AI Act (vollständig ab 02.08.2026)

Der EU AI Act klassifiziert KI-Systeme nach Risiko. Für KI-Agenten in regulierten Umfeldern ist vor allem die Hochrisiko-Kategorie relevant:

- **Risikoklassifizierung** nach Annex I–III (4 Klassen)
- **8 Pflichten** für Hochrisiko-KI: Risikomanagement, Datenqualität, Dokumentation, Logging, Transparenz, Human Oversight, Genauigkeit, Cybersecurity
- **Transparenzpflichten** für alle KI-Systeme (Chatbot-Kennzeichnung, KI-generierte Inhalte)
- **Bußgelder:** Bis 35 Mio. EUR oder 7 % des weltweiten Jahresumsatzes

3.2 NIS2 (seit 12/2025 in Kraft)

NIS2 reguliert die Cybersicherheit und betrifft rund 29.500 Unternehmen in Deutschland:

- **Meldepflichten:** 24h-Frühwarnung, 72h-Vorfallbericht, 1-Monat-Abschluss
- **Persönliche Haftung:** Geschäftsleitung haftet persönlich und nicht delegierbar
- **Bußgelder:** Bis 10 Mio. EUR oder 2 % des Jahresumsatzes

3.3 DSGVO & Branchenspezifisches

- **DSGVO:** Datenschutz-Folgeabschätzung (DSFA) bei personenbezogenen Daten
- **SGB V (GKV):** Sozialdaten-Governance, Auftragsverarbeitung
- **VAG (Versicherung):** Aufsichtsrechtliche Anforderungen
- **BSI-Standards (KRITIS):** IT-Grundschutz, C5-Testat

3.4 Synergien zwischen den Regelwerken

Die gute Nachricht: Viele Anforderungen überlappen sich. Ein integrierter Compliance-Ansatz spart erheblich Zeit und Geld:

Anforderung	EU AI Act	NIS2	DSGVO	Synergie
Risikomanagement	Art. 9	Art. 21	Art. 35	Gemeinsames Framework
Dokumentation	Art. 11	ISMS-Doku	Art. 30	Einheitliches DMS
Incident Response	Monitoring	24h/72h	72h	Integrierter Prozess
Schulungen	Transparenz	GF-Pflicht	Awareness	Kombiniertes Programm

4. Fünf Erfolgsfaktoren aus der Praxis

Basierend auf unserer Erfahrung mit KI-Agenten-Projekten in regulierten Umfeldern haben wir fünf Erfolgsfaktoren identifiziert:

4.1 Compliance-by-Design, nicht Compliance-by-Audit

Der häufigste und teuerste Fehler: Erst den KI-Agenten bauen, dann die Compliance-Abteilung fragen. Compliance muss von Tag eins im Design verankert sein.

- EU AI Act-Risikoklassifizierung vor dem ersten Prototyp
- DSFA als fester Bestandteil des PoC-Scopes
- Entscheidungslogik von Anfang an dokumentieren (Auditierbarkeit)
- Compliance-Steckbrief pro Agent erstellen, bevor die Implementierung beginnt

4.2 Agenten-Netzwerke statt Einzel-Agenten

KI-Agenten entfalten ihren vollen Wert erst als Netzwerk, in dem spezialisierte Agenten zusammenarbeiten. Laut einer Studie von Deloitte (2024) erzielen Unternehmen, die KI-Agenten als vernetzte Systeme statt als isolierte Projekte einführen, einen um 3,5x höheren ROI. Planen Sie von Anfang an die Orchestrierung mehrerer Agenten – auch wenn Sie mit einem starten.

Die Vorteile eines Netzwerk-Ansatzes sind erheblich: Jeder Agent bleibt einfach, testbar und dokumentierbar. Das Gesamtsystem ist modular erweiterbar. Und bei regulatorischen Änderungen muss nur der betroffene Agent angepasst werden, nicht das gesamte System.

4.3 Neutrale Partner-Steuerung

Die technische Implementierung wird oft ausgelagert. Die strategische Steuerung darf es nicht. Ohne neutrale Steuerung drohen:

- **Scope-Creep:** Partner baut, was technisch spannend ist, nicht was Geschäftswert hat
- **Compliance-Lücken:** Partner kennt die regulatorischen Anforderungen oft nicht
- **Vendor Lock-in:** Architektur wird vom Tool-Hersteller getrieben

4.4 PoC-Überführung von Anfang an planen

Die Überführung in die Produktion ist der Punkt, an dem die meisten Projekte scheitern:

Hürde	Im PoC	In Produktion	Präventive Maßnahme
Daten	Testdaten	Echte Kundendaten	Datenfreigabe in Phase 1 klären
Infrastruktur	Sandbox	Produktionsumgebung	Security-Anforderungen mitdenken
Change Mgmt	Nur IT-Team	Gesamte Organisation	Stakeholder früh einbinden
Betriebsmodell	Einmaliger Test	Dauerbetrieb	Monitoring in Phase 1 planen

4.5 Bewusste Autonomiegrade definieren

Erstellen Sie für jeden KI-Agenten einen Compliance-Steckbrief:

- EU AI Act Risikoklasse
- Datenklassifizierung (personenbezogen, Sozialdaten, öffentlich)
- Autonomiegrad (assistierend / teil-autonom / autonom)
- Verantwortlichkeiten (fachlich, technisch, compliance)
- Eskalationspfade (wann greift der Mensch ein?)

5. Der Weg zum KI-Agenten: Phasenmodell

Die Einführung von KI-Agenten folgt einem bewährten 4-Phasen-Modell. Jede Phase endet mit einer Go/No-Go-Entscheidung:

Phase	Dauer	Ziel	Zentrale Deliverables
-------	-------	------	-----------------------

Assessment	5–7 Tage	Reifegrad & Priorisierung	KI-Reifegrad-Report (20–30 S.), Use-Case-Matrix, Compliance-Quickcheck, Roadmap
Strategie & Design	4–6 Wochen	Architektur & Spezifikation	Agenten-Steckbriefe, Compliance-Framework, PoC-Spec, Partner-Empfehlung
PoC & Validierung	6–10 Wochen	Funktionsnachweis	Funktionierender PoC, Testing-Protokoll, Go/No-Go, Lessons Learned
Rollout & Betrieb	2–6 Monate	Produktivbetrieb	Produktive Agenten, Betriebsmodell, Governance-Framework, Wissenstransfer

6. KI-Readiness: Wo steht Ihr Unternehmen?

Unser KI-Readiness Assessment bewertet Ihre Organisation über fünf Dimensionen:

Dimension	Was wird geprüft	Typische Lücken
Strategie & Use Cases	KI-Vision, Use-Case-Pipeline, Roadmap	Keine priorisierte Use-Case-Liste
Daten & Infrastruktur	Datenqualität, Cloud-Readiness, APIs	Datensilos, fehlende APIs
Compliance & Regulatorik	EU AI Act, NIS2, DSGVO, Branche	Keine Risikoklassifizierung
Organisation & Governance	Rollen, Prozesse, Entscheidungswege	Kein AI Officer, keine KI-Policy
Technologie & Partner	Tools, Plattformen, Implementierungspartner	Shadow AI, kein Gesamtbild

Selbstcheck

Kostenloser Schnelltest: Prüfen Sie Ihren KI-Reifegrad in 10 Minuten unter nexuscon.net/ki-readiness-schnelltest

7. Fazit & Handlungsempfehlung

KI-Agenten in regulierten Umfeldern sind kein rein technisches, sondern vor allem ein organisatorisches Projekt. Die Wahl der Technologie ist zweitrangig. Entscheidend sind: Compliance-by-Design, bewusste Autonomiegrade, Netzwerk-Denken, neutrale Partner-Steuerung und eine von Anfang an geplante Überführungsstrategie.

Drei konkrete nächste Schritte

1. KI-Readiness Assessment durchführen (5–7 Tage) → [Mehr erfahren](#)
2. Ersten Agenten designen im Design Sprint (3–4 Tage) → [Mehr erfahren](#)
3. Erstgespräch vereinbaren → nexuscon.net/kontakt

KI-Readiness: Wo steht Ihr Unternehmen?

Unser KI-Readiness Assessment bewertet Ihre Organisation über fünf Dimensionen. Die folgende Grafik zeigt ein typisches Ergebnis:

KI-Reifegrad - Beispiel eines typischen Unternehmens



Typisches Bild: Technologie und Daten sind vorhanden, aber Compliance und Governance hinken hinterher. Die schwächste Dimension bestimmt den Startpunkt.

Kostenloser Schnelltest

Prüfen Sie Ihren KI-Reifegrad in 10 Minuten unter nexuscon.net/ki-readiness-schnelltest

8. Glossar

Begriff	Definition
Agentic AI	KI-Systeme, die eigenständig Ziele verfolgen, planen und Werkzeuge nutzen – im Gegensatz zu passiven Chatbots oder regelbasierten Bots.
LLM	Large Language Model – Sprachmodelle wie GPT-4, Claude oder Gemini, die natürliche Sprache verstehen und generieren.
RPA	Robotic Process Automation – Software-Roboter, die strukturierte, repetitive Aufgaben nach festen Regeln automatisieren.
PoC	Proof of Concept – Machbarkeitsnachweis, in dem ein KI-Agent in einem begrenzten Scope getestet wird.
Human-in-the-Loop	Der Mensch prüft und genehmigt jede Entscheidung des KI-

	Agenten, bevor sie ausgeführt wird.
Compliance-by-Design	Regulatorische Anforderungen werden von Anfang an in das System-Design integriert, nicht nachträglich geprüft.
Shadow AI	KI-Tools, die von Mitarbeitenden ohne IT-Freigabe genutzt werden (z. B. ChatGPT für Geschäftsdaten).
DSFA	Datenschutz-Folgeabschätzung gemäß Art. 35 DSGVO – Pflicht bei hohem Risiko für personenbezogene Daten.

Quellen & Referenzen

Die folgenden Quellen wurden für dieses Whitepaper herangezogen:

- Gartner (2024): „By 2028, 33% of enterprise software applications will include agentic AI.“ – Gartner Press Release, Oktober 2024. [→ Quelle](#)
- McKinsey & Company (2024): „Why agents are the next frontier of generative AI.“ – McKinsey Digital, Juli 2024. [→ Quelle](#)
- Europäisches Parlament (2024): Verordnung (EU) 2024/1689 – EU AI Act, Amtsblatt der EU, 12. Juli 2024. [→ Quelle](#)
- Europäisches Parlament (2022): Richtlinie (EU) 2022/2555 – NIS2-Richtlinie, Dezember 2022. [→ Quelle](#)
- BSI (2025): NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – Bundesamt für Sicherheit in der Informationstechnik. [→ Quelle](#)
- UiPath (2025): „Agentic Automation with Maestro“ – UiPath Platform Documentation. [→ Quelle](#)
- Deloitte (2024): „State of Generative AI in the Enterprise“ – Deloitte AI Institute. [→ Quelle](#)
- DSGVO: Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung. [→ Quelle](#)
- ISO/IEC 27001:2022 – Informationssicherheitsmanagementsysteme – Anforderungen. [→ Quelle](#)

Stand: März 2026. Alle Angaben ohne Gewähr. Dieses Whitepaper stellt keine Rechtsberatung dar.

Über den Autor



Simon Schilling

Geschäftsführer & Principal Consultant

Nexus Management Consulting GmbH | Stuttgart
AWS Solutions Architect | PRINCE2 | Azure Architect | TOGAF 9 | ITIL v3

Mit über 13 Jahren Erfahrung in der IT-Beratung hat Simon komplexe Transformationsprojekte bei T-Systems, Wipro und Q_PERIOR begleitet, bevor er 2023 Nexus gründete. Sein Fokus liegt auf der Integration von KI-Agenten in regulierte Geschäftsprozesse – von der Strategie über den PoC bis zum compliant-by-design Rollout.

Er verbindet technische Tiefe mit strategischer Beratung und Compliance-Expertise (EU AI Act, NIS2, DSGVO). Aktuelle Referenzprojekte: KI-Agenten für Anliegenmanagement (GKV/KRITIS), Workplace Architecture (Versicherung), SW-Lifecycle-Management (IT-Dienstleister), Sovereign Cloud Vergabe (öffentliche Verwaltung).

Über Nexus Management Consulting

„Nexus integriert KI-Agenten in regulierte Geschäftsprozesse – von der Strategie über den PoC bis zum compliant-by-design Rollout.“

Nexus Management Consulting ist eine spezialisierte Unternehmensberatung für regulierte Umfelder mit Sitz in Stuttgart. Wir unterstützen Unternehmen in den Bereichen Gesundheitswesen, Versicherung, KRITIS und öffentliche Verwaltung bei der Einführung von KI-Agenten und der Umsetzung regulatorischer Anforderungen.

Leistungsportfolio

- **KI-Readiness Assessment** (5–7 Tage) – Reifegrad, Use Cases, Compliance-Check
- **Agentic AI Design Sprint** (3–4 Tage) – Agenten-Architektur und PoC-Spezifikation
- **KI-Agenten-Programm** (3–12 Monate) – End-to-End Steuerung
- **NIS2 / EU AI Act Compliance** – Vom Assessment bis zur Audit-Readiness
- **Fractional AI Officer / Virtual CISO** – Laufende Steuerung auf Abruf

Kontakt aufnehmen

E-Mail simon.schilling@nexuscon.net
Telefon +49 151 5472 6609
Web nexuscon.net

Im Kaisemer 11 | 70191 Stuttgart | Nexus Management Consulting GmbH

→ Jetzt Erstgespräch buchen