Holger Reibold

EU AI Act in der Praxis

Der Betreiberleitfaden für IT-Verantwortliche – Einkauf, Betrieb, Monitoring

BRAIN-MEDIA.DE

Holger Reibold

EU AI Act
in der Praxis

Der Betreiberleitfaden für IT-Verantwortliche – Einkauf, Betrieb, Monitoring

BRAIN-MEDIA.DE

ISBN: 978-3-95444-320-8

Cover: Freepik

Brain-Media.de – St. Johanner Str. 41-43 – 66111 Saarbrücken

info@brain-media.de – www.brain-media.de

Inhaltsverzeichnis

Vorwort

Der EU AI Act markiert einen Wendepunkt im Umgang mit Künstlicher Intelligenz in Europa. Er ist das erste umfassende Regelwerk, das nicht nur einzelne Anwendungsfälle adressiert, sondern den gesamten Lebenszyklus von KI-Systemen in den Blick nimmt. Für viele Unternehmen kommt diese Regulierung zu einem Zeitpunkt, an dem KI bereits im Alltag angekommen ist – oft schneller und weniger strukturiert, als ursprünglich geplant.

Dieses Buch ist aus genau dieser Spannung heraus entstanden. In zahlreichen Gesprächen mit IT-Verantwortlichen, Admins und Entscheidern zeigte sich immer wieder dasselbe Bild: KI wird genutzt, getestet, eingekauft und integriert, während gleichzeitig Unsicherheit darüber besteht, welche Verantwortung damit konkret verbunden ist. Nicht aus Nachlässigkeit, sondern weil bisher klare, praxisnahe Leitplanken fehlten.

Der EU AI Act schließt diese Lücke auf regulatorischer Ebene. Gleichzeitig eröffnet er neue Fragen: Was bedeutet „Betreiberverantwortung“ im Alltag? Wie viel Dokumentation ist notwendig – und wie viel ist realistisch? Wie lassen sich Anforderungen erfüllen, ohne Innovationsfähigkeit und operative Effizienz zu verlieren? Dieses Buch versucht, auf diese Fragen praktische und belastbare Antworten zu geben.

Dabei richtet es sich bewusst nicht an Juristen oder KI-Entwickler, sondern an diejenigen, die KI-Systeme im Betrieb verantworten. An Menschen, die entscheiden müssen, ob ein System eingeführt wird, wie es überwacht wird und was im Fehlerfall zu tun ist. Der Anspruch ist nicht, jede rechtliche Feinheit auszuleuchten, sondern Orientierung zu schaffen, wo Unsicherheit herrscht, und Struktur dort anzubieten, wo bislang Improvisation dominierte. Dieses Buch richtet sich an Organisationen, die KI betreiben, nicht an solche, die sie kommentieren.

Der Fokus liegt auf Umsetzbarkeit. Auf Prozessen, die im Alltag funktionieren. Auf Lösungen, die mit bestehenden IT-Tools, begrenzten Ressourcen und realistischen Zeitbudgets vereinbar sind. Der EU AI Act verlangt keinen perfekten Zustand, sondern einen verantwortungsvollen Umgang mit Risiken. Genau hier setzt dieses Buch an.

Wenn es einen roten Faden gibt, der sich durch alle Kapitel zieht, dann ist es dieser: KI ist kein Sonderfall mehr. Sie ist Teil der IT-Landschaft – mit allen Chancen, aber auch mit neuen Formen von Verantwortung. Wer diese Verantwortung frühzeitig strukturiert, gewinnt Sicherheit, Handlungsspielraum und Vertrauen.

Ich hoffe, dieses Buch leistet dazu einen Beitrag.

Herzlichst,

Holger Reibold

Einleitung

Die rasante Entwicklung der KI-Technologie stellt Unternehmen nahezu aller Branchen vor bedeutende Herausforderungen. Die EU hat mit dem AI Act ein mächtiges, aber vielfach missverstandenes Instrument geschaffen, dass eine nachhaltige Technologienutzung etablieren soll. Doch vielfach mangelt es am grundlegenden Verständnis für die Potenziale.

Die größten Irrtümer zum EU AI Act

Der EU AI Act sorgt in vielen Unternehmen weniger für Klarheit als für Reflexe. Besonders auf Managementebene haben sich drei Annahmen etabliert, die nachvollziehbar klingen, in der Praxis aber zu Fehlentscheidungen mit messbaren Kosten führen.

Der erste Irrtum lautet: „Alles ist Hochrisiko."

Diese Annahme führt dazu, dass Unternehmen KI-Projekte unnötig aufblähen, verzögern oder ganz stoppen. Tatsächlich ist Hochrisiko im EU AI Act eine funktionale Ausnahme, keine Grundeinstellung. Wer Art. 6 – insbesondere Absatz 3 – nicht nutzt, produziert Over-Compliance und bindet Ressourcen dort, wo sie keinen Sicherheitsgewinn bringen.

Der zweite Irrtum lautet: „Der Anbieter haftet."

Viele Unternehmen gehen davon aus, dass Compliance mit dem Kauf einer KI-Lösung mitgeliefert wird. Das ist falsch. Der EU AI Act verlagert zentrale Pflichten bewusst auf den Betreiber: Nutzungskontext, Zweckbindung, Monitoring und Human Oversight lassen sich nicht outsourcen. Wer das übersieht, steht im Prüfungsfall ohne belastbare Argumente da – trotz „AI-Act-konformer" Anbieter.

Der dritte Irrtum lautet: „Wir warten erst mal ab."

Diese Haltung wirkt risikoarm, ist es aber nicht. KI wird bereits genutzt – oft inoffiziell. Shadow AI, private Accounts und unkontrollierte Tools schaffen faktische Risiken, während formale Governance fehlt. Abwarten bedeutet nicht Stillstand, sondern Kontrollverlust. Spätestens bei Incidents oder Beschwerden fehlt dann jede Entscheidungsgrundlage.

Dieses Buch setzt genau hier an. Es ersetzt Irrtümer durch belastbare Entscheidungslogik – und zeigt, wie Unternehmen den EU AI Act als Steuerungsinstrument nutzen können, statt ihn als Blockade zu erleben.

Der EU AI Act wird häufig mit der Datenschutz-Grundverordnung verglichen. Diese Parallele liegt nahe – und führt doch in die Irre. Während die DSGVO primär den Umgang mit personenbezogenen Daten regelt, adressiert der EU AI Act den Betrieb technischer Systeme, die Entscheidungen vorbereiten, beeinflussen oder automatisieren. Damit verschiebt sich der Schwerpunkt weg von reiner Rechtskonformität hin zu technischer und organisatorischer Steuerbarkeit.

In der Praxis zeigt sich schnell, dass pauschale Reaktionen wie KI-Stopps oder Verbote keine nachhaltige Lösung darstellen. KI ist bereits Teil moderner IT-Landschaften – oft eingebettet in Standardsoftware, Cloud-Dienste oder interne Workflows. Wer versucht, diese Realität auszublenden, verliert Kontrolle statt sie zu gewinnen.

Der EU AI Act ist daher weniger als Innovationsbremse zu verstehen, sondern als Rahmen für professionellen Betrieb. Er zwingt Unternehmen nicht, KI abzuschalten, sondern Verantwortung dort zu verankern, wo Systeme tatsächlich laufen: in IT-Strukturen, Prozessen und Rollen. Genau deshalb betrifft er nicht nur Anbieter von KI, sondern nahezu jedes Unternehmen, das KI einsetzt – also Betreiber.

Warum KI-Stopps und Verbote scheitern

Die erste Reaktion vieler Unternehmen auf den EU AI Act ist der Versuch, Risiken durch Verzicht zu eliminieren. KI-Projekte werden gestoppt, neue Tools blockiert oder pauschal verboten. Was kurzfristig nach Kontrolle aussieht, führt mittelfristig zu genau dem Gegenteil.

Der zentrale Grund: KI ist längst kein isoliertes Spezialthema mehr. Sie ist in Standardsoftware, Cloud-Diensten und Geschäftsprozessen integriert. Assistenzfunktionen, automatische Priorisierungen, Empfehlungssysteme oder Texterkennung lassen sich nicht einfach „abschalten“, ohne wesentliche Teile der IT-Landschaft zu beeinträchtigen. Ein formales Verbot ändert nichts daran, dass diese Funktionen

technisch weiterhin vorhanden sind – es verschiebt ihre Nutzung lediglich in inoffizielle Kanäle.

In der Praxis entstehen so sogenannte Shadow-AI-Strukturen. Mitarbeitende greifen auf private Accounts, nicht genehmigte Tools oder externe Dienste zurück, um ihre Arbeit effizient zu erledigen. Diese Nutzung entzieht sich jeder Kontrolle: Es gibt keine Protokollierung, keine Transparenz über Datenflüsse und keine Möglichkeit, Risiken zu bewerten oder zu begrenzen. Das eigentliche Ziel – Risikoreduktion – wird verfehlt.

Hinzu kommt ein organisatorisches Problem. KI-Stopps verlagern Verantwortung nicht, sie lösen sie auf. Wenn KI offiziell „nicht genutzt werden darf", fühlt sich niemand zuständig, Systeme zu inventarisieren, Einsatzbereiche zu klassifizieren oder Sicherheitsmaßnahmen zu definieren. Der EU AI Act verlangt jedoch genau das Gegenteil: aktive Steuerung statt passiver Vermeidung.

Auch wirtschaftlich sind Verbotsstrategien kaum tragfähig. Wettbewerber, Dienstleister und Softwareanbieter setzen KI weiter ein. Unternehmen, die sich vollständig entziehen, verlieren Effizienz, Geschwindigkeit und Anschlussfähigkeit – ohne dadurch regulatorisch sicherer zu werden. Der EU AI Act setzt deshalb nicht auf Verbote als Regelfall, sondern auf risikobasierte Steuerung. Er geht davon aus, dass KI genutzt wird, und fordert, dass diese Nutzung nachvollziehbar, überwacht und beherrscht erfolgt. Wer versucht, KI durch Stopps zu umgehen, entzieht sich genau dieser Steuerungslogik – und erhöht am Ende das Risiko statt es zu reduzieren.

Regulierung als Betriebshygiene

Regulierung wird im Kontext von Künstlicher Intelligenz häufig als Gegensatz zu Innovation verstanden. Die Sorge ist, dass neue Vorgaben Entwicklung verlangsamen, Experimente verhindern und Unternehmen gegenüber weniger regulierten Märkten ins Hintertreffen geraten. Diese Sichtweise greift zu kurz – insbesondere aus der Perspektive des Betriebs. Der EU AI Act setzt nicht bei der Innovationsidee an, sondern bei deren Umsetzung im Alltag. Er reguliert nicht, *ob* KI eingesetzt werden darf, sondern *wie* sie betrieben wird. Damit ähnelt er anderen etablierten Rahmenwerken in der IT: Sicherheitsstandards, Datenschutz oder Verfügbarkeitsanforderungen haben Innovation nicht verhindert, sondern strukturiert. Systeme werden nicht langsamer, weil sie überwacht werden, sondern stabiler.

In der Praxis bedeutet Betriebshygiene, dass Systeme dokumentiert, überwacht und regelmäßig überprüft werden. Diese Maßnahmen sind kein Selbstzweck. Sie reduzieren Abhängigkeiten von Einzelpersonen, verhindern Wissensverlust und ermöglichen es, Änderungen kontrolliert vorzunehmen. Gerade bei KI-Systemen, deren Verhalten sich durch neue Daten oder Modellupdates verändern kann, ist diese Form der Steuerung Voraussetzung für nachhaltigen Einsatz.

Unternehmen, die Regulierung als Hygienefaktor begreifen, gewinnen Handlungsspielraum. Sie können KI schneller einführen, weil Verantwortlichkeiten geklärt sind, Risiken bewertet wurden und klare Prozesse existieren. Ohne diese Grundlagen entstehen

Reibungsverluste: Freigaben verzögern sich, Entscheidungen werden vertagt oder Innovationen werden aus Angst vor Haftung blockiert. Der EU AI Act zwingt Organisationen dazu, diese Grundlagen explizit zu machen. Er fordert kein perfektes Risikomanagement, sondern ein funktionsfähiges. Wer diese Anforderungen pragmatisch umsetzt, schafft eine stabile Betriebsumgebung, in der KI kontrolliert weiterentwickelt werden kann. Regulierung wird damit nicht zur Innovationsbremse, sondern zur Voraussetzung dafür, dass Innovation wiederholbar, skalierbar und verantwortbar wird.

Warum fast alle Unternehmen Betreiber sind

Viele Unternehmen gehen zunächst davon aus, vom EU AI Act nur am Rande betroffen zu sein. Die häufigste Begründung lautet: „Wir entwickeln keine KI, wir nutzen sie nur." Genau hier liegt das zentrale Missverständnis. Der EU AI Act knüpft Verantwortung nicht primär an die Entwicklung von Modellen, sondern an deren Einsatz im eigenen Verantwortungsbereich.

Wer KI-Systeme einkauft, integriert, konfiguriert oder im eigenen Prozesskontext nutzt, übernimmt die Rolle des Betreibers. Das gilt unabhängig davon, ob das Modell intern trainiert wurde oder als SaaS, API oder Cloud-Dienst bezogen wird. In der betrieblichen Realität betrifft das nahezu jedes Unternehmen, das moderne Software einsetzt: von HR-Tools über Support-Systeme bis hin zu Assistenzfunktionen in Standardanwendungen.

Entscheidend ist nicht, wo das Modell entstanden ist, sondern wer über Zweck, Einsatz und Rahmenbedingungen entscheidet. Betreiber bestimmen, wofür ein System genutzt wird, welche Daten einfließen, wer Ergebnisse sieht und wie mit Fehlern umgegangen wird. Genau an dieser Stelle setzt der EU AI Act an. Er adressiert Verantwortung dort, wo Risiken wirksam gesteuert werden können – im Betrieb.

Diese Einordnung ist unbequem, aber realistisch. Sie erklärt, warum sich Betreiberpflichten nicht delegieren lassen und warum sich nahezu jedes Unternehmen mit dem EU AI Act auseinandersetzen muss, sobald KI produktiv eingesetzt wird.

Was dieses Buch bewusst nicht ist

Dieses Buch ist kein juristischer Kommentar zum EU AI Act. Es ersetzt keine Rechtsberatung und erhebt nicht den Anspruch, jede Auslegungsfrage abschließend zu klären. Paragrafen, Erwägungsgründe und Definitionen werden nur dort aufgegriffen, wo sie konkrete Auswirkungen auf Betrieb, Organisation oder Technik haben.

Der Fokus liegt bewusst auf die Umsetzbarkeit. Das Ziel ist es nicht, rechtliche Vollständigkeit zu erreichen, sondern handlungsfähig zu machen. Wer eine akademische Analyse oder eine systematische Kommentierung des Gesetzestextes sucht, wird andere Werke finden. Dieses Buch richtet sich an diejenigen, die Entscheidungen treffen, Systeme betreiben und im Zweifel erklären müssen, wie KI im Alltag kontrolliert wird.

Lesepfade: Admin – IT-Leitung – Management

Dieses Buch ist so aufgebaut, dass es je nach Rolle unterschiedlich gelesen werden kann. Nicht jede Zielgruppe muss jedes Kapitel im Detail durcharbeiten, um Nutzen daraus zu ziehen. Admins und operative IT-Rollen finden den größten Mehrwert in den Kapiteln zu Inventur, Betrieb, Monitoring, Logging, Testing und Incident Response. Hier geht es um konkrete Maßnahmen, technische Umsetzung und pragmatische Mindeststandards.

IT-Leitung und CISO-Rollen profitieren insbesondere von den Kapiteln zu Rollenklärung, Einkauf, Vendor Management, Risikoklassifizierung und Governance. Sie liefern Entscheidungsgrundlagen, Priorisierungshilfen und Argumente gegenüber Management und Prüfern.

Management und Entscheider können sich auf die Einordnungskapitel, den Kosten- und Proportionalitätsteil sowie den 90-Tage-Umsetzungsplan konzentrieren. Diese Abschnitte zeigen, wie Verantwortung organisiert werden kann, ohne operative Teams zu blockieren oder Innovation zu ersticken.

Alle Kapitel sind modular aufgebaut. Das Buch kann vollständig gelesen oder gezielt als Referenz genutzt werden – je nach Rolle, Zeitbudget und Fragestellung.

1 Inventur, Shadow AI und Rollenrealität

Bevor über Risikoklassen, Pflichten oder technische Maßnahmen gesprochen werden kann, muss eine grundlegende Frage geklärt werden: Welche KI-Systeme sind überhaupt im Einsatz – und in welcher Rolle? In der Praxis wird dieser Schritt häufig übersprungen oder stark unterschätzt. Stattdessen wird direkt über Klassifizierung, Dokumentation oder Verbote diskutiert, ohne eine belastbare Übersicht zu haben. Das führt zwangsläufig zu Fehlentscheidungen.

Die Realität in Unternehmen ist selten eindeutig. KI wird nicht nur über große, offiziell eingeführte Systeme genutzt, sondern auch über Funktionen in Standardsoftware, Cloud-Dienste, Plugins oder private Accounts. Hinzu kommen interne Experimente, Proofs of Concept und „nur mal getestete" Anwendungen, die technisch existieren, organisatorisch aber niemandem zugeordnet sind. Genau hier entstehen die größten Risiken – nicht durch böse Absicht, sondern durch fehlende Transparenz.

Der EU AI Act setzt deshalb sehr früh an der Rollenklärung an. Er unterscheidet zwischen Anbietern, Betreibern und Nutzern von KI-Systemen. Diese Trennung ist keine formale Spielerei, sondern haftungsrelevant. Sie entscheidet darüber, welche Pflichten ein Unternehmen hat, was delegierbar ist und wo Verantwortung verbleibt. Wer diese Rollen falsch einordnet, riskiert entweder Über-Compliance oder gefährliche Lücken.

Kapitel 1 schafft die notwendige Grundlage für alles Weitere. Es erklärt, warum fast jedes Unternehmen Betreiber ist, weshalb Shadow AI kein Randphänomen, sondern Normalfall ist, und warum auch interne Tests und PoCs rechtlich zählen können. Zudem wird aufgezeigt, wann scheinbar harmlose Anpassungen – etwa durch Fine-Tuning – die eigene Rolle verändern.

Abschließend führt das Kapitel in eine pragmatische Minimal-Inventur ein. Ziel ist keine perfekte Erfassung, sondern eine arbeitsfähige Übersicht, die in kurzer Zeit erstellt werden kann und als Basis für alle weiteren Schritte dient. Gerade für kleine und mittlere Unternehmen ist dieser Einstieg entscheidend: Wer hier pragmatisch beginnt, vermeidet später unnötige Komplexität und Fehlsteuerung.

1.1 Anbieter, Betreiber, Nutzer

Der EU AI Act unterscheidet konsequent zwischen drei Rollen: Anbieter, Betreiber und Nutzer von KI-Systemen. Auf den ersten Blick wirkt diese Einteilung formal und abstrakt. In der betrieblichen Praxis entscheidet sie jedoch darüber, wer welche Pflichten trägt, wer haftet und wer sich nicht auf Unwissen berufen kann.

Ein Anbieter ist nach dem EU AI Act diejenige Organisation, die ein KI-System entwickelt oder es unter eigenem Namen oder eigener Marke in Verkehr bringt. Dazu zählen klassische KI-Hersteller ebenso wie Softwareanbieter, die KI-Funktionalitäten als Produktbestandteil ausliefern. Anbieter tragen die umfangreichsten Pflichten,

insbesondere im Hinblick auf Konformitätsbewertung, technische Dokumentation und Systemdesign.

Ein Betreiber hingegen ist jede natürliche oder juristische Person, die ein KI-System in eigener Verantwortung einsetzt. Entscheidend ist nicht, wer das System gebaut hat, sondern wer bestimmt, wofür und wie es genutzt wird. Betreiber konfigurieren Systeme, integrieren sie in Prozesse, entscheiden über Einsatzkontexte und verantworten den Umgang mit Ergebnissen. Genau deshalb richtet sich ein Großteil der praktischen Pflichten des EU AI Act an Betreiber – nicht an Anbieter.

Die Rolle des Nutzers schließlich ist deutlich enger gefasst. Nutzer bedienen ein KI-System im Rahmen vorgegebener Prozesse, ohne Einfluss auf Zweck, Konfiguration oder Integration zu haben. In vielen Organisationen sind Mitarbeitende Nutzer, während das Unternehmen selbst als Betreiber fungiert. Diese Differenzierung ist wichtig, weil Pflichten und Haftungsrisiken nicht auf einzelne Personen, sondern auf die verantwortliche Organisation zielen.

In der Praxis verschwimmen diese Rollen häufig. Unternehmen sprechen von „wir nutzen nur ein Tool“, obwohl sie es in Wirklichkeit betreiben. Sie konfigurieren Modelle, legen Schwellenwerte fest, bestimmen Datenquellen oder bauen KI-Ausgaben in Entscheidungsprozesse ein. Spätestens an diesem Punkt liegt keine reine Nutzung mehr vor. Der EU AI Act zieht hier eine klare Linie: Wer Einsatz und Zweck bestimmt, ist Betreiber – unabhängig vom technischen Eigentum am Modell.

Diese Rollenklärung ist haftungsrelevant aus zwei Gründen. Erstens lassen sich Betreiberpflichten nur sehr eingeschränkt delegieren. Auch wenn Anbieter Konformität zusichern oder Zertifikate vorlegen, bleibt der Betreiber verantwortlich für den konkreten Einsatz im eigenen Kontext. Zweitens entscheidet die Rolle darüber, welche Anforderungen verhältnismäßig sind. Betreiber müssen nicht entwickeln, aber sie müssen überwachen, dokumentieren und eingreifen können.

Ein häufiger Fehler besteht darin, Anbieterpflichten zu fürchten und Betreiberpflichten zu ignorieren. Unternehmen investieren viel Energie in Vertragsklauseln, Haftungsausschlüsse oder Zertifikate, vernachlässigen aber Inventur, Monitoring oder Incident-Prozesse. Der EU AI Act ist hier eindeutig: Haftung folgt Verantwortung im Betrieb, nicht technischer Herkunft.

Die klare Trennung zwischen Anbieter, Betreiber und Nutzer ist daher kein theoretisches Konstrukt, sondern die Grundlage für jede sinnvolle Umsetzung. Wer seine Rolle korrekt bestimmt, kann Anforderungen realistisch priorisieren, Verantwortlichkeiten sauber zuordnen und regulatorische Risiken kontrollierbar machen. Wer sie falsch einordnet, läuft Gefahr, entweder unnötig zu blockieren – oder unbemerkt Pflichten zu verletzen.

1.2 Warum jedes Unternehmen Betreiber ist

Viele Unternehmen gehen zunächst davon aus, vom EU AI Act nur am Rand betroffen zu sein. Die häufigste Begründung lautet: „Wir

entwickeln keine KI, wir kaufen nur Software ein." Genau diese Annahme führt in der Praxis zu Fehlentscheidungen. Denn der EU AI Act knüpft Verantwortung nicht an die Entwicklung eines Modells, sondern an dessen Einsatz im eigenen organisatorischen und fachlichen Kontext.

In der betrieblichen Realität wird KI heute überwiegend nicht selbst entwickelt, sondern als Bestandteil von Standardsoftware, Cloud-Diensten oder spezialisierten SaaS-Lösungen genutzt. HR-Systeme priorisieren Bewerbungen, Support-Tools schlagen Antworten vor, CRM-Systeme bewerten Leads, Office-Anwendungen generieren Texte oder Zusammenfassungen. Technisch mag das alles „eingekaufte KI" sein – regulatorisch entsteht dadurch dennoch eine Betreiberrolle.

Der entscheidende Punkt ist die Zweckbestimmung. Unternehmen legen fest, wofür ein KI-System eingesetzt wird, in welchem Prozess es wirkt und welche Folgen seine Ergebnisse haben. Sie entscheiden, ob ein Vorschlag nur informativen Charakter hat oder Grundlage für weitere Schritte ist. Sie bestimmen, welche Daten einfließen, welche Nutzer Zugriff haben und wie mit Fehlentscheidungen umgegangen wird. Genau diese Entscheidungen machen ein Unternehmen zum Betreiber.

Hinzu kommt, dass KI-Systeme in der Praxis selten unverändert genutzt werden. Konfigurationen, Schwellenwerte, Workflow-Anbindungen oder ergänzende Datenquellen verändern das Verhalten eines Systems erheblich. Selbst ohne eigenes Modelltraining entsteht

so ein kontextualisiertes KI-System, dessen Risiken nicht mehr allein beim Anbieter liegen. Der EU AI Act trägt dieser Realität Rechnung, indem er Betreiberpflichten dort verankert, wo diese Kontextentscheidungen getroffen werden.

Besonders trügerisch ist die Annahme, nur Hochrisiko-Systeme würden Betreiberpflichten auslösen. Auch KI-Anwendungen mit begrenztem oder minimalem Risiko unterliegen bestimmten Anforderungen, etwa an Transparenz oder Überwachung. Betreiber zu sein bedeutet nicht automatisch, Hochrisiko-Pflichten erfüllen zu müssen – wohl aber, Verantwortung für den eigenen Einsatz zu übernehmen.

Ein weiterer Grund, warum fast alle Unternehmen Betreiber sind, liegt in der zunehmenden Verschränkung von KI-Funktionen mit bestehenden IT-Systemen. KI ist nicht mehr klar als separates Produkt erkennbar. Sie ist Feature, Option oder Hintergrundfunktion. Wer diese Funktionen aktiviert, integriert oder duldet, übernimmt faktisch die Betreiberrolle – auch wenn sie organisatorisch nie explizit benannt wurde.

Diese Erkenntnis ist unbequem, aber notwendig. Sie bedeutet nicht, dass jedes Unternehmen sofort umfangreiche Compliance-Strukturen aufbauen muss. Sie bedeutet jedoch, dass sich Verantwortung nicht wegverhandeln lässt. Der EU AI Act geht davon aus, dass Risiken dort gesteuert werden, wo Systeme tatsächlich eingesetzt werden – nicht dort, wo sie entwickelt wurden.

Wer akzeptiert, Betreiber zu sein, gewinnt Handlungsspielraum. Pflichten lassen sich priorisieren, Anforderungen proportional umsetzen und Risiken realistisch managen. Wer diese Rolle dagegen ablehnt oder ignoriert, verliert genau das: Kontrolle über den eigenen KI-Einsatz. Deshalb ist die Feststellung, dass fast jedes Unternehmen Betreiber ist, kein Alarmismus. Sie ist der notwendige Ausgangspunkt für eine pragmatische, realitätsnahe Umsetzung des EU AI Act.

1.3 Shadow AI

In kaum einem Unternehmen wird KI heute ausschließlich über offiziell eingeführte Systeme genutzt. Parallel dazu existiert fast immer eine zweite Ebene: Shadow AI. Gemeint sind KI-Anwendungen, die außerhalb formaler Freigabe- und Betriebsprozesse eingesetzt werden – häufig gut gemeint, selten kontrolliert.

Typische Beispiele sind private ChatGPT-Accounts, Browser-Plugins mit KI-Funktionen, KI-Features in Office-Tools oder eigenständig genutzte Assistenzdienste wie Copilot-Varianten. Aus Sicht der Mitarbeitenden sind diese Werkzeuge schlicht produktiv. Aus Sicht des Unternehmens entstehen jedoch blinde Flecken: Es ist unklar, welche Daten verarbeitet werden, wohin Informationen fließen und welche Ergebnisse in Entscheidungen einfließen.

Shadow AI ist kein Randphänomen und kein Zeichen von Regelverstößen einzelner Mitarbeitender. Sie entsteht dort, wo der Bedarf schneller ist als formale Prozesse. Wenn KI offiziell nicht verfügbar ist

oder nur eingeschränkt genutzt werden darf, weichen Mitarbeitende auf private oder inoffizielle Lösungen aus. Der Versuch, KI durch Verbote zu kontrollieren, verstärkt diesen Effekt häufig.

Für den EU AI Act ist Shadow AI besonders relevant, weil Verantwortung nicht an formale Genehmigungen geknüpft ist, sondern an faktische Nutzung im Unternehmenskontext. Wenn Mitarbeitende KI-Ergebnisse in Arbeitsprozesse einbringen – etwa bei Texten, Bewertungen, Priorisierungen oder Entscheidungs-vorbereitungen – wirkt das System mittelbar im Unternehmen. Die Risiken entstehen unabhängig davon, ob der Einsatz offiziell genehmigt war.

Aus regulatorischer Sicht ergeben sich daraus mehrere Probleme. Erstens fehlt Transparenz. Ohne Kenntnis über eingesetzte Tools ist keine Inventur möglich, keine Risikobewertung und kein Monitoring. Zweitens fehlt Steuerbarkeit. Unternehmen können weder eingreifen noch reagieren, wenn Ergebnisse fehlerhaft, verzerrt oder sicherheitsrelevant sind. Drittens entsteht ein Governance-Bruch: Offizielle Prozesse gelten nur für einen Teil der Realität.

Besonders kritisch wird Shadow AI dort, wo personenbezogene oder sensible Unternehmensdaten verarbeitet werden. Private Accounts unterliegen anderen Nutzungsbedingungen, Logging-Mechanismen oder Trainingsregeln als Unternehmenslösungen. Daten können unbemerkt in externe Systeme gelangen oder für Trainingszwecke verwendet werden, ohne dass das Unternehmen dies nachvollziehen oder steuern kann.

Der EU AI Act adressiert dieses Problem nicht explizit unter dem Begriff „Shadow AI“, setzt aber implizit voraus, dass Unternehmen wissen, welche KI-Systeme in ihrem Einflussbereich genutzt werden. Ohne diese Kenntnis lassen sich Betreiberpflichten weder erfüllen noch glaubhaft vertreten. In Prüf- oder Incident-Situationen ist „das war privat“ keine tragfähige Argumentation.

Schicht	Typ	Beispiele	Governance-Status
Offiziell	Offizielle KI-Systeme	HR-Recruiting-Tool CRM-KI Support-Chatbot	Gesteuert (Einkauf, Compliance, Monitoring)
Geduldet	Geduldete SaaS-KI	MS Copilot GitHub Copilot Analytics-Tools (z. B. Tableau u. KI)	Teilweise gesteuert (Nutzungsbedingungen, aber limitiertes Monitoring)
Inoffiziell	Shadow AI	Private ChatGPT-Accounts Browser-Plugins PoCs ohne Freigabe Excel u. Copilot	Ungesteuert (kein Inventur, kein Risikomanagement)

Die Übersicht zeigt die typische Verteilung von KI-Nutzung im Unternehmen: offiziell eingeführte Systeme, geduldete Tools und inoffizielle Shadow-AI-Nutzung. Sie macht sichtbar, wo Governance greift – und wo Haftungs- und Sicherheitsrisiken entstehen.

Literatur- und Quellenverzeichnis

Amazon Web Services (2024). AWS Bedrock documentation. https://docs.aws.amazon.com.

European Commission (2021). Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

European Commission (2023). Impact assessment accompanying the proposal for an Artificial Intelligence Act.

European Commission (2024). AI Act explained. https://digital-strategy.ec.europa.eu.

European Data Protection Board (2020). Guidelines on automated individual decision-making and profiling.

European Parliament & Council of the European Union (2016). Regulation (EU) 2016/679 (General Data Protection Regulation). Official Journal of the European Union.

European Parliament & Council of the European Union (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity (NIS2 Directive).

European Parliament & Council of the European Union (2022). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA).

European Parliament & Council of the European Union (2024). Regulation (EU) 2024/… laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union.

Floridi, L., Cowls, J., Beltrametti, M., et al. (2018). AI4People—An ethical framework for a good AI society. Minds and Machines, 28(4), 689–707.

International Organization for Standardization (2019). ISO/IEC 27001: Information security management systems.

International Organization for Standardization (2023). ISO/IEC 42001: Artificial intelligence — Management system.

Microsoft (2024). Azure OpenAI Service documentation. https://learn.microsoft.com.

Microsoft (2024). Microsoft Copilot documentation. https://learn.microsoft.com.

Mitchell, M., Wu, S., Zaldivar, A., et al. (2019). Model cards for model reporting. Proceedings of the Conference on Fairness, Accountability, and Transparency.

National Institute of Standards and Technology (2023). AI Risk Management Framework (AI RMF 1.0). https://www.nist.gov.

OpenAI. (2023). GPT-4 Technical Report. https://openai.com.

Raji, I. D., Smart, A., White, R. N., et al. (2020). Closing the AI accountability gap. Proceedings of the ACM Conference on Fairness, Accountability, and Transparency.

Stichwortverzeichnis

E

F

G

H

I

K

L

M

N

O

P

R

S

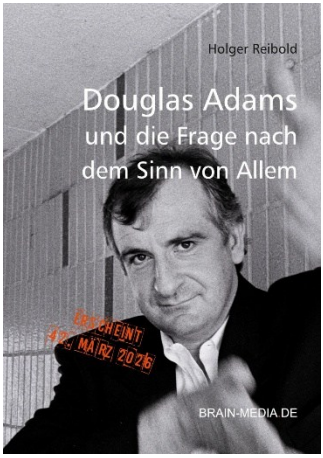
T

U

V

Z

Mehr von Brain-Media.de



42 – Douglas Adams und die Frage nach dem Sinn von Allem

Am 11. Mai 2026 ist Douglas Adams 25 Jahre tot. Der Kultautor hat der Welt wunderbar, skurrile Werke geschenkt. Jetzt ist es an der Zeit, den Autor kennenzulernen.

Umfang: 140 Seiten

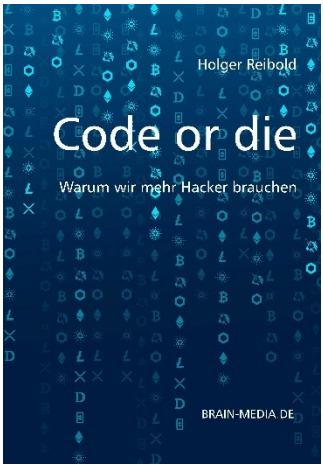
Preis: 14,99 EUR

Erscheint: 42. März 2026

Towelday, das ultimative Handtuch für alle Fans

An seinem Todestag, dem Towelday, erinnern sich Fans an Douglas Adams und huldigen dem Kultautor.

100 % intergalaktisch geprüfte Baumwolle, nachhaltig Produktion zum Preis von 42 EUR.



Code or die – Warum wir mehr Hacker brauchen

Ein Manifest für mehr digitale Selbstbestimmung, Neugierde und Eigenverantwortung. Medienkompetenzen alleine genügen nicht; die Gesellschaft von morgen braucht Digitalkompetenzen.

Umfang: 120 Seiten

Preis: 14,99 EUR

Erscheint Frühjahr 2026

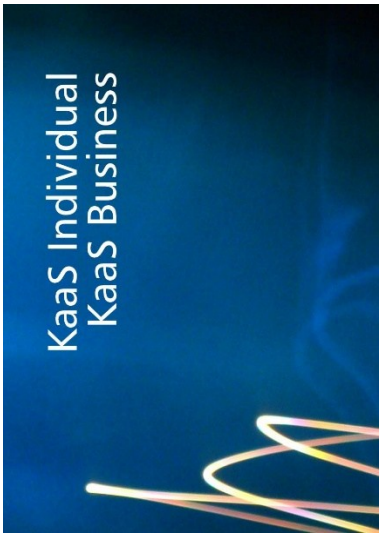
KI Incident Response – Wie man Sicherheitsvorfälle in KI-Systemen erkennt, eindämmt und verantwortet

Ziel- und punktgenaue Reaktionen für kritischen KI-Vorfälle.

Umfang: 140 Seiten

Preis: 16,99 EUR

Erscheint: Frühjahr 2026



Knowledge as a Service

Individual

Business

Brain-Media.de ist ein **Pionier** in Sachen E-Book-Flatrates. Bereits 2014 wurden mit Plus+ E-Books als attraktives und preisgünstiges Abo angeboten. Im April 2026 erlebt sie mit KaaS eine Renaissance.

Abonnementen erhalten **1 Jahr Zugriff auf alle E-Books**, die bereits erschienen sind, und auf alle Neuerscheinungen des Abozeitraums. Sie können alle verfügbaren E-Books herunterladen – dazu exklusives Download (Checklisten, Vorlagen, Beispiele etc.). Sie können die E-Books ausdrucken und auf mehreren Lesegeräten verwenden. Die E-Books verwenden kein DRM!

Und das alles zum **Sonderpreis** von 99 Euro!

Mehr von Brain-Media.de | LI

IT-Texter.one

100+ IT-Fachbücher

1500+ Fachartikel

30+ Erfahrung

KOMPLEXE INHALTE PUNKTGENAU AUFZUBEREITEN, IST EINE KUNST. ICH BEHERRSCHE SIE. BEI MIR ERHALTEN SIE FACHTEXTE, DIE KOMPLEXES VERSTÄNDLICH MACHEN.

Seit über 30 Jahren unterstütze ich Unternehmen aus der IT-, Software- und Digitalbranche dabei, ihre technischen Inhalte klar, präzise und zielgruppenorientiert zu kommunizieren. Als promovierter Informatiker und erfahrener IT-Journalist verbinde ich fundiertes Fachwissen mit journalistischem Storytelling. Als Key Account Manager eines IT-Dienstleisters verfüge ich obendrein über konkrete Erfahrungen mit allen gängigen Technologien.

WARUM SIE MIT MIR ARBEITEN SOLLTEN

35 Jahre Erfahrung mit Internet-, Netzwerk- und Webtechnologien

Kooperation mit führenden Akteuren der IT- und Medienbranche

Strategisches Denken: Texte, die nicht nur informieren, sondern auch verkaufen

THEMENSCHWERPUNKTE	WIE KANN ICH SIE UNTERSTÜTZEN?
Open-Source	Content Creation
Enterprise IT	Dokumentationen
IT-Consulting	Case Studies
SaaS	Suchmaschinenoptimierung
Künstliche Intelligenz	Tech-Marketing

MEIN VERSPRECHEN

Ich übernehme die inhaltliche und sprachliche Brücke zwischen Technologie und Anwendung. Selbst komplexe Sachverhalte kommen beim Publikum an – fachlich korrekt, prägnant und SEO-wirksam.

PREISMODELLE

Professionelle Leistungen, die ihresgleichen suchen, gibt es nicht umsonst. Sprechen Sie mit an. Gerne vereinbaren wir einen Fixpreis; das vereinfacht Ihre Kalkulation.

KONTAKT AUFNEHMEN

Sprechen wir über Ihr Projekt. Schreiben Sie mir eine Mail (info@it-texter.one). Oder besser noch: Rufen Sie mich an (+49 681 91005698).