NADOVO

# EU AI ACT COMPLIANCE FÜR DEN MITTELSTAND

Ein praxisorientierter Leitfaden

**Jochen Stier**

Stand: Juni 2026

# INHALTSVERZEICHNIS


1. Warum AI Compliance jetzt?
2. EU AI Act auf einen Blick
3. Betrifft mich das?
4. Risikoklassifizierung
5. Pflichten nach Rolle und Risikoklasse
6. Zusammenspiel mit der DSGVO
7. NADOVO Framework: Der Einstieg
8. Erste Schritte: Sofort loslegen

# 1. WARUM AI COMPLIANCE JETZT?

Künstliche Intelligenz ist kein Zukunftsthema mehr. Sie ist Gegenwart: in jedem Unternehmen, in jeder Branche, in den Werkzeugen, die Mitarbeiter täglich nutzen. Gleichzeitig hat die Europäische Union mit dem AI Act die weltweit erste umfassende KI-Regulierung verabschiedet. Die Fristen laufen, die Strafen sind empfindlich, und die meisten mittelständischen Unternehmen haben noch nicht angefangen, sich vorzubereiten.

Dieses Kapitel erklärt, warum Abwarten die riskanteste aller Strategien ist.

## KI ist schon da, ob gewollt oder nicht

In Gesprächen mit Geschäftsführern mittelständischer Unternehmen fällt oft der gleiche Satz: "Wir setzen eigentlich keine KI ein." Dieser Satz ist fast immer falsch.

Die Realität sieht anders aus. Die meisten Unternehmen nutzen bereits KI-Systeme, häufig ohne es bewusst entschieden zu haben. Microsoft 365 enthält Copilot-Funktionen, die auf großen Sprachmodellen basieren. CRM-Systeme wie Salesforce oder HubSpot setzen KI für Lead-Scoring und Prognosen ein. Buchhaltungssoftware klassifiziert Belege automatisch. ERP-Systeme optimieren Bestellmengen mit Hilfe maschinellen Lernens. Selbst die Spam-Erkennung im E-Mail-Postfach ist ein KI-System.

Dazu kommt eine zweite Ebene: KI-Funktionen, die in bestehende Software eingebettet werden, ohne dass es groß angekündigt wird. Ein Software-Update, und plötzlich schlägt das System Texte vor, erkennt Muster oder priorisiert Aufgaben. Der Anbieter hat KI integriert. Das Unternehmen, das die Software nutzt, wird zum Betreiber (Deployer) eines KI-Systems, oft ohne es zu wissen.

Die Frage ist also nicht, ob ein Unternehmen KI einsetzt. Die Frage ist, wie viel KI bereits im Einsatz ist und ob die Geschäftsführung darüber den Überblick hat.

> **Praxis:** Ein einfacher Test schafft Klarheit. In einer Abteilungsleiter-Runde die Frage stellen: "Welche unserer Softwaresysteme nutzen KI oder maschinelles Lernen?" Die Antworten mit den tatsächlichen Produktbeschreibungen der eingesetzten Lösungen vergleichen. Die Diskrepanz ist in den meisten Fällen erheblich.

## Schatten-KI: Das unterschätzte Risiko

Neben der "offiziellen" KI-Nutzung gibt es ein Phänomen, das für Unternehmen deutlich gefährlicher ist: Schatten-KI (Shadow AI). Gemeint ist die Nutzung von KI-Werkzeugen durch Mitarbeiter ohne Wissen, Genehmigung oder Kontrolle des Unternehmens.

Die Szenarien sind so alltäglich wie riskant. Ein Mitarbeiter im Vertrieb lässt ChatGPT ein Angebot formulieren und fügt dabei Kundendaten, Preiskonditionen und Vertragsbedingungen in das Eingabefeld ein. Eine Personalsachbearbeiterin nutzt ein KI-Übersetzungstool, um einen Arbeitsvertrag ins Englische zu übertragen, inklusive persönlicher Daten des Mitarbeiters. Ein Entwickler lässt Code-Fragmente von einem KI-Assistenten analysieren und überträgt dabei proprietäre Geschäftslogik an einen externen Dienst.

Was diese Situationen gemeinsam haben: Personenbezogene Daten oder Geschäftsgeheimnisse verlassen das Unternehmen, ohne dass eine Rechtsgrundlage geprüft, ein Auftragsverarbeitungsvertrag geschlossen oder auch nur dokumentiert wurde, dass diese Verarbeitung stattfindet. Das ist kein Kavaliersdelikt, sondern ein handfestes Datenschutzproblem nach DSGVO. Und mit dem EU AI Act kommt eine weitere Compliance-Dimension hinzu.

Wer in den 2010er Jahren die Debatte um Shadow IT miterlebt hat, kennt das Muster: Mitarbeiter umgehen offizielle IT-Wege, weil die offiziellen Lösungen zu langsam, zu umständlich oder schlicht nicht vorhanden sind. Schatten-KI folgt der gleichen Logik, nur mit einem entscheidenden Unterschied. Bei Shadow IT ging es meist um Produktivitätstools oder Cloud-Speicher. Bei Schatten-KI geht es um Systeme, die Inhalte erzeugen, Entscheidungen vorbereiten und Daten an externe Modelle übertragen. Das Risikopotenzial ist deutlich höher.

Die Konsequenz ist klar: Ohne ein Inventar der eingesetzten KI-Systeme, einschließlich der inoffiziellen, und ohne verbindliche Nutzungsrichtlinien kann kein Unternehmen seine KI-Risiken steuern. Der erste Schritt jeder AI-Compliance-Strategie ist deshalb Transparenz über den Status quo.

## Die Uhr tickt: Fristen und Konsequenzen

Der EU AI Act (Verordnung (EU) 2024/1689) ist am 1. August 2024 in Kraft getreten. Seitdem läuft ein gestaffelter Zeitplan, der verschiedene Pflichten zu unterschiedlichen Zeitpunkten aktiviert.

**Was bereits gilt:**

Seit dem 2. Februar 2025 sind die Verbote bestimmter KI-Praktiken wirksam. Dazu gehören unter anderem Social Scoring, manipulative Techniken, die Schwächen von Personen ausnutzen, und bestimmte Formen biometrischer Echtzeit-Fernidentifizierung. Ebenfalls seit dem 2. Februar 2025 gilt die Pflicht zur KI-Kompetenz (Artikel 4): Unternehmen müssen sicherstellen, dass Personal, das KI-Systeme betreibt oder beaufsichtigt, über ausreichende Kenntnisse verfügt.

> **EU AI Act:** Art. 4: Anbieter und Betreiber von KI-Systemen ergreifen Maßnahmen, um nach besten Kräften sicherzustellen, dass ihr Personal und andere Personen, die in ihrem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind, über ein ausreichendes Maß an KI-Kompetenz verfügen.

Mit dem Digital-Omnibus-Paket der EU vom Mai 2026 wurde Artikel 4 abgeschwächt: Statt ein „ausreichendes Maß" an KI-Kompetenz sicherzustellen, müssen Unternehmen nun „Maßnahmen zur Förderung" der KI-Kompetenz ihres Personals ergreifen. Die Pflicht besteht unverändert seit dem 2. Februar 2025 fort und ist nicht abgeschafft.

**Was noch kommt:**

Seit dem 2. August 2025 gelten die Pflichten für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck (General Purpose AI, GPAI), also etwa die Anbieter großer Sprachmodelle. Ab dem **2. Dezember 2027** wird der EU AI Act in seiner vollen Breite anwendbar. Das betrifft insbesondere die umfassenden Pflichten für Hochrisiko-KI-Systeme nach Anhang III: Risikomanagement, Daten-Governance, technische Dokumentation, menschliche Aufsicht, Transparenz und Meldepflichten. Dieser Termin wurde mit dem Digital-Omnibus-Paket der EU vom Mai 2026 vom ursprünglichen 2. August 2026 verschoben (siehe Kapitel 2).

**Die Sanktionen sind empfindlich:**

Der EU AI Act sieht ein dreistufiges Bußgeldsystem vor. Bei Verstößen gegen die verbotenen KI-Praktiken drohen Geldbußen von bis zu 35 Millionen Euro oder 7 Prozent des weltweiten Jahresumsatzes, je nachdem welcher Betrag höher ist. Für andere Verstöße gegen die Verordnung liegt die Obergrenze bei 15 Millionen Euro oder 3 Prozent des Umsatzes. Selbst die Bereitstellung falscher oder unvollständiger Informationen an Behörden kann mit bis zu 7,5 Millionen Euro oder 1 Prozent des Umsatzes geahndet werden.

> **EU AI Act:** Art. 99: Für KMU und Start-ups sieht die Verordnung verhältnismäßige Obergrenzen vor. Das ändert nichts an der Tatsache, dass die Bußgelder auch für mittelständische Unternehmen existenzbedrohend sein können.

Dabei geht es nicht nur um Geld. Die Marktüberwachungsbehörden können die Nutzung nicht-konformer KI-Systeme untersagen oder deren Rücknahme vom Markt anordnen. Für ein Unternehmen, das auf ein bestimmtes KI-System in seinem Geschäftsbetrieb angewiesen ist, kann eine solche Anordnung gravierender sein als eine Geldbuße.

## Compliance als Chance, nicht nur als Pflicht

Bis hierhin mag es klingen, als sei AI Compliance vor allem eine Belastung. Bußgelder, Fristen, Pflichten. Das ist die eine Seite. Die andere Seite wird häufig übersehen.

**Vertrauen als Wettbewerbsvorteil.** Kunden, Geschäftspartner und öffentliche Auftraggeber fragen zunehmend nach: Wie geht das Unternehmen mit KI um? Gibt es Richtlinien? Ist der Einsatz dokumentiert? Unternehmen, die diese Fragen belastbar beantworten können, haben einen Vorteil, sei es bei Ausschreibungen, Lieferantenaudits oder in Kundengesprächen. Nachweisbare KI-Governance wird zum Qualitätsmerkmal, ähnlich wie es ISO-Zertifizierungen oder DSGVO-Compliance bereits sind.

**Bessere Entscheidungen durch Transparenz.** Ein vollständiges KI-Inventar und eine systematische Risikoklassifizierung liefern der Geschäftsführung etwas, das vielen Unternehmen fehlt: einen klaren Überblick über die eigene KI-Landschaft. Welche Systeme sind im Einsatz? Wofür? Mit welchem Risiko? Dieses Wissen verbessert nicht nur die Compliance, sondern auch die strategische Steuerung des KI-Einsatzes insgesamt.

**Vorbereitung auf das, was kommt.** Der EU AI Act ist die erste umfassende KI-Regulierung, aber er steht nicht allein. Die ursprünglich geplante AI Liability Directive wurde 2025 zurückgezogen. Haftungsfragen für KI-Schäden werden stattdessen über die überarbeitete Product Liability Directive geregelt, die ab Dezember 2026 gilt und Software sowie KI-Systeme ausdrücklich einschließt. Branchenspezifische Anforderungen werden folgen. Versicherer werden KI-Risiken in ihre Policen einpreisen. Wer heute eine solide Compliance-Basis aufbaut, muss morgen nicht bei null anfangen, wenn die nächste Regulierungswelle kommt.

**Kein Hexenwerk.** AI Compliance erfordert kein Millionenbudget und kein Team von KI-Spezialisten, sondern Struktur, Überblick und die Bereitschaft, das Thema systematisch

anzugehen. Die meisten mittelständischen Unternehmen haben mit der DSGVO bewiesen, dass sie regulatorische Anforderungen bewältigen können. AI Compliance baut auf vielen dieser Erfahrungen auf.

> **Praxis:** Der wichtigste erste Schritt kostet nichts außer Zeit: ein Inventar der eingesetzten KI-Systeme erstellen. Ohne dieses Inventar ist unklar, was reguliert werden muss. Mit diesem Inventar steht die Grundlage für alles Weitere. Kapitel 8 zeigt, wie sich das in der ersten Woche umsetzen lässt.

Der EU AI Act ist keine Überraschung. Er wurde jahrelang verhandelt, öffentlich diskutiert und im Juni 2024 final verabschiedet. Die Fristen sind bekannt. Die Aufsichtsstrukturen in Deutschland sollen mit dem geplanten KI-MIG etabliert werden. Was jetzt noch fehlt, ist bei vielen Unternehmen die interne Vorbereitung.

Dieser Leitfaden liefert das Fundament dafür. Die folgenden Kapitel erklären, was der EU AI Act konkret regelt, welche Rolle ein Unternehmen einnimmt, wie KI-Systeme zu klassifizieren sind und welche Pflichten sich daraus ergeben. Am Ende steht ein konkreter Fahrplan für die ersten vier Wochen.

# 2. EU AI ACT AUF EINEN BLICK

Der EU AI Act ist die weltweit erste umfassende Regulierung für künstliche Intelligenz. Er betrifft jedes Unternehmen, das KI-Systeme in der Europäischen Union einsetzt, unabhängig davon, wo der Anbieter der Software seinen Sitz hat. Dieses Kapitel gibt einen kompakten Überblick: Was regelt die Verordnung, wie ist sie aufgebaut, welche Fristen gelten, wie sieht die nationale Umsetzung in Deutschland aus, und wie fügt sich der AI Act in die bestehende Regulierungslandschaft ein.

## Was regelt der EU AI Act?

Die Verordnung (EU) 2024/1689 verfolgt ein klares Ziel: den sicheren, vertrauenswürdigen und menschenzentrierten Einsatz von KI in der Europäischen Union. Sie legt fest, unter welchen Bedingungen KI-Systeme entwickelt, bereitgestellt und eingesetzt werden dürfen, und sie definiert Grenzen, die nicht überschritten werden dürfen.

**Der Geltungsbereich ist bewusst weit gefasst.** Der EU AI Act erfasst alle KI-Systeme, die innerhalb der EU auf den Markt gebracht, in Betrieb genommen oder genutzt werden. Das gilt auch dann, wenn der Anbieter seinen Sitz außerhalb der EU hat, solange die Ausgabe des Systems für Personen in der EU bestimmt ist. Diese extraterritoriale Wirkung kennen viele Unternehmen bereits von der DSGVO: Nicht der Standort des Anbieters ist entscheidend, sondern der Wirkungsort des Systems.

**Was nicht unter den AI Act fällt:** Rein militärische KI-Anwendungen sind ausgenommen. Ebenso KI-Systeme, die ausschließlich für persönliche, nicht-berufliche Zwecke genutzt werden. Forschung und Entwicklung genießen unter bestimmten Bedingungen ebenfalls Ausnahmen, allerdings nur solange die Systeme nicht auf den Markt gebracht oder in Betrieb genommen werden.

Für mittelständische Unternehmen im DACH-Raum bedeutet das: Wer KI-Software einsetzt, die in irgendeiner Weise Entscheidungen trifft, Inhalte erzeugt oder Personen betrifft, fällt mit hoher Wahrscheinlichkeit in den Anwendungsbereich dieser Verordnung.

## Struktur der Verordnung

Der EU AI Act umfasst 13 Kapitel mit 113 Artikeln und 13 Anhängen. Das klingt nach viel, und das ist es auch. Die gute Nachricht: Für die Praxis sind nicht alle Teile gleich relevant. Die folgende Übersicht zeigt, wo die wichtigsten Inhalte zu finden sind.

| Kapitel | Inhalt | Relevanz für KMU |
|---|---|---|
| **Kapitel I** (Art. 1-4) | Allgemeine Bestimmungen, Definitionen, Geltungsbereich, KI-Kompetenz | Hoch: Hier werden die Grundbegriffe definiert |
| **Kapitel II** (Art. 5) | Verbotene KI-Praktiken | Hoch: Gilt seit dem 2. Februar 2025 |
| **Kapitel III** (Art. 6-49) | Hochrisiko-KI-Systeme: Klassifizierung, Anforderungen, Pflichten für Anbieter und Betreiber | Kernstück: Entscheidend für alle, die Hochrisiko-Systeme einsetzen |
| **Kapitel IV** (Art. 50) | Transparenzpflichten für bestimmte KI-Systeme | Relevant für Chatbots, generative KI, Emotionserkennung |
| **Kapitel V** (Art. 51-56) | KI-Modelle mit allgemeinem Verwendungszweck (General Purpose AI) | Primär für GPAI-Anbieter, KMU als Nutzer indirekt betroffen |
| **Kapitel VII** (Art. 64-68) | Governance: AI Office, AI Board, nationale Behörden | Relevant für Aufsichtsstruktur |
| **Kapitel IX** (Art. 72-94) | Überwachung nach Inverkehrbringen, Marktüberwachung | Relevant für Meldepflichten und Post-Market-Monitoring |
| **Kapitel X-XII** (Art. 95-101) | Verhaltenskodizes, Sanktionen | Relevant für Bußgeldrahmen |

Zwei Anhänge verdienen besondere Aufmerksamkeit.

**Anhang I** listet die harmonisierten EU-Produktvorschriften auf. Wenn ein Produkt bereits einer EU-Konformitätsbewertung unterliegt, etwa als Maschine, Medizinprodukt oder Spielzeug, und eine KI-Komponente als Sicherheitselement enthält, gilt das KI-System automatisch als Hochrisiko.

**Anhang III** definiert acht Anwendungsbereiche, in denen KI-Systeme als Hochrisiko eingestuft werden: von biometrischer Identifizierung über Personalmanagement bis zur Rechtspflege. Dieser Anhang ist für KMU die zentrale Prüfgrundlage und wird in Kapitel 4 ausführlich behandelt.

> **Praxis:** Es ist nicht nötig, alle 113 Artikel zu lesen. Der pragmatische Einstieg: Artikel 5 (Verbote), Artikel 6 (Hochrisiko-Klassifizierung), Artikel 26 (Deployer-Pflichten) und Artikel 50 (Transparenzpflichten). Zusammen mit Anhang III decken diese Stellen den größten Teil dessen ab, was für KMU operativ relevant ist.

## Zeitstrahl: Was gilt ab wann?

Der EU AI Act wird nicht auf einen Schlag wirksam, sondern in Stufen. Das gibt Unternehmen Zeit zur Vorbereitung, aber nur wenn sie diese Zeit auch nutzen.

| Datum | Was gilt? | Status |
|---|---|---|
| **1. August 2024** | Verordnung in Kraft getreten | Abgeschlossen |
| **2. Februar 2025** | Verbotene KI-Praktiken (Art. 5); Pflicht zur KI-Kompetenz (Art. 4) | **Bereits wirksam** |
| **2. August 2025** | Pflichten für GPAI-Modelle (Art. 51-56); Governance-Strukturen (AI Office, AI Board) | **Bereits wirksam** |
| **2. August 2026** | Transparenzpflichten für bestimmte KI-Systeme (Art. 50) | Wirksam ab |
| **2. Dezember 2026** | Neues Verbot KI-generierter nicht-einvernehmlicher intimer Darstellungen und von CSAM (Art. 5); Schonfrist für die Wasserzeichen-Kennzeichnung nach Art. 50 Abs. 2 bei Bestandssystemen | Ausstehend |
| **2. Dezember 2027** | Vollständige Anwendung: Hochrisiko-KI-Systeme nach Anhang III, Deployer-Pflichten, Sanktionen | Verschoben (vormals 2. August 2026) |
| **2. August 2028** | Hochrisiko-Systeme als Sicherheitskomponente in regulierten Produkten (Anhang I) | Verschoben (vormals 2. August 2027) |

> **Hinweis zum Stand:** Die hier genannten verschobenen Fristen (Hochrisiko nach Anhang III ab 2. Dezember 2027, nach Anhang I ab 2. August 2028) beruhen auf dem Digital-Omnibus-Paket der EU. Das Europäische Parlament hat die Reform am 16. Juni 2026 angenommen; die formale Annahme durch den Rat und die Veröffentlichung im EU-Amtsblatt standen zu Redaktionsschluss noch aus. Bis zur Veröffentlichung bleibt formal der ursprüngliche Stichtag 2. August 2026 in Kraft.

Für die meisten KMU ist der **2. Dezember 2027** der entscheidende Stichtag. Ab diesem Datum gelten die umfassenden Pflichten für Hochrisiko-Systeme in vollem Umfang: Risikomanagement, Dokumentation, menschliche Aufsicht, Meldepflichten und die Möglichkeit behördlicher Sanktionen.

Zwei Pflichten gelten allerdings bereits jetzt. Die Verbote bestimmter KI-Praktiken sind seit dem 2. Februar 2025 wirksam. Wer Social Scoring betreibt oder manipulative KI-Techniken einsetzt, handelt bereits heute rechtswidrig. Und die Pflicht zur KI-Kompetenz nach Artikel 4 verlangt schon jetzt, dass Mitarbeiter, die KI-Systeme bedienen oder beaufsichtigen, über ausreichende Kenntnisse verfügen.

> **Praxis:** Als erstes sollte geprüft werden, ob die bereits geltenden Pflichten erfüllt sind. Gibt es im Unternehmen KI-Anwendungen, die unter die Verbotsliste fallen könnten? Verfügen die Mitarbeiter über ausreichende KI-Kompetenz? Diese beiden Punkte sind keine Zukunftsmusik, sie gelten jetzt.

## Nationale Umsetzung: Das KI-MIG

Der EU AI Act gilt als EU-Verordnung unmittelbar in allen Mitgliedstaaten. Anders als bei einer Richtlinie muss er nicht erst in nationales Recht umgesetzt werden. Was jedoch national geregelt werden muss, ist die Frage, welche Behörden für die Aufsicht zuständig sind, wie Bußgelder durchgesetzt werden und wie die Zusammenarbeit der Behörden organisiert wird.

In Deutschland soll das **KI-Marktüberwachungs- und Innovationsförderungsgesetz (KI-MIG)** diese Lücke schließen. Das Bundeskabinett hat den Regierungsentwurf am 11. Februar 2026 beschlossen, der Bundestag hat das Gesetz am 11. Juni 2026 verabschiedet. Die Zustimmung des Bundesrates stand zu Redaktionsschluss noch aus. Eigentlich hätten die nationalen Aufsichtsstrukturen bereits bis zum 2. August 2025 stehen

müssen; die vorgezogene Bundestagswahl hatte den Prozess verzögert. Das Gesetz sieht ein nicht-öffentliches Register für Hochrisiko-KI-Systeme vor.

**Zuständige Behörden: Ein hybrider Ansatz**

Deutschland setzt auf eine verteilte Aufsichtsstruktur, die bestehende Zuständigkeiten respektiert.

Die **Bundesnetzagentur (BNetzA)** wird zur zentralen Marktüberwachungsbehörde für die private Wirtschaft. Sie ist der Hauptansprechpartner für Unternehmen, die nicht bereits einer sektorspezifischen Aufsicht unterliegen. Für den Finanzsektor bleibt die **BaFin** zuständig, insbesondere für Hochrisiko-KI-Systeme in Banken, Versicherungen und Finanzdienstleistungen. Ebenso behalten die bestehenden **Produktaufsichtsbehörden** ihre Zuständigkeit. Wer bisher mit der zuständigen Stelle für Medizinprodukte oder Maschinensicherheit zusammengearbeitet hat, behält diesen Ansprechpartner.

Für KMU bedeutet dieser hybride Ansatz: In den meisten Fällen ist die BNetzA die richtige Adresse. Nur wenn das Unternehmen in einem regulierten Sektor mit eigener Aufsichtsbehörde tätig ist, bleibt die bestehende Zuständigkeit bestehen.

**KoKIVO und Unterstützungsangebote der BNetzA**

Bei der BNetzA ist die Einrichtung des **Koordinierungs- und Kompetenzzentrums für die KI-Verordnung (KoKIVO)** vorgesehen. Es soll KI-Expertise bündeln und anderen Behörden zur Verfügung stellen. Für Unternehmen bietet die BNetzA bereits jetzt einen **KI-Service-Desk**, der sich gezielt an kleine und mittlere Unternehmen sowie Start-ups richtet. Ergänzt wird das Angebot durch den **KI-Compliance Kompass**, ein interaktives Tool zur Ersteinschätzung der eigenen Betroffenheit.

**KI-Reallabore: Testen mit behördlicher Begleitung**

Der EU AI Act (Art. 57) verpflichtet jeden Mitgliedstaat, bis zum 2. August 2027 mindestens ein **KI-Reallabor** (Regulatory Sandbox) einzurichten; das Digital-Omnibus-Paket hat diese Frist vom ursprünglichen 2. August 2026 verschoben. In Deutschland soll die BNetzA diese Aufgabe übernehmen. In diesen kontrollierten Testumgebungen können Unternehmen innovative KI-Anwendungen unter behördlicher Begleitung entwickeln und auf Konformität prüfen. Die regulatorischen Anforderungen gelten dabei uneingeschränkt; der Vorteil liegt in der fachlichen Beratung und erhöhten Rechtssicherheit. KMU und Start-ups mit Sitz in der EU erhalten vorrangigen und kostenlosen Zugang (Art. 62).

**Kein deutscher Sonderweg**

Ein Detail des Gesetzentwurfs verdient besondere Betonung: **Das KI-MIG verzichtet auf zusätzliche nationale Anforderungen über den EU AI Act hinaus.** Das Bundesministerium für Digitales und Staatsmodernisierung (BMDS) betont ausdrücklich die innovationsoffene Umsetzung. Wer die EU-Verordnung erfüllt, soll damit auch die deutschen Anforderungen erfüllen. Der Entwurf sieht keinen nationalen Aufschlag und keine verschärften Sonderregeln vor, wenngleich der EU AI Act den Mitgliedstaaten in einzelnen Bereichen wie der biometrischen Echtzeit-Identifizierung strengere nationale Regelungen erlaubt.

Das unterscheidet den KI-Bereich von manchen anderen Regulierungsfeldern, in denen deutsche Umsetzungsgesetze zusätzliche Hürden aufgebaut haben. Für KMU ist das eine wichtige Entlastungsbotschaft: Die Compliance-Anforderungen sollen sich auf das europäisch Vorgeschriebene beschränken.

> **EU AI Act / KI-MIG:** Für die Praxis heißt das: Der EU AI Act ist der Maßstab. Wer dessen Anforderungen erfüllt, ist in Deutschland compliant. Der KI-Service-Desk der BNetzA steht als Anlaufstelle für Fragen bereit.

## Abgrenzung zu anderen Regelwerken

Der EU AI Act steht nicht allein. Er ist Teil eines wachsenden regulatorischen Ökosystems, in dem sich verschiedene Regelwerke gegenseitig ergänzen.

**EU AI Act und DSGVO** sind komplementär. Die DSGVO regelt den Schutz personenbezogener Daten, der EU AI Act reguliert den Einsatz von KI-Systemen. Beide greifen häufig gleichzeitig, weil die meisten KI-Systeme personenbezogene Daten verarbeiten. Der AI Act stellt in Artikel 2 ausdrücklich klar, dass die Rechte der Betroffenen aus der DSGVO unberührt bleiben. Wie Unternehmen beide Verordnungen zusammen umsetzen können, behandelt Kapitel 6 im Detail.

**EU AI Act und Produktsicherheitsrecht** überschneiden sich bei KI-Systemen, die als Sicherheitskomponente in regulierten Produkten eingesetzt werden. Wenn ein Produkt, etwa eine Maschine, ein Medizinprodukt oder ein Aufzug, unter eine EU-Harmonisierungsvorschrift aus Anhang I fällt und die Konformitätsbewertung eine benannte Stelle (Notified Body) erfordert, gilt die KI-Sicherheitskomponente als Hochrisiko-KI-System (Art. 6 Abs. 1). Die bestehende CE-Kennzeichnung deckt dann auch die AI-Act-Anforderungen ab: Eine einzige Konformitätsbewertung umfasst beide Regelwerke (Art. 43 Abs. 3).

**Die AI Liability Directive** war ursprünglich als Ergänzung zum AI Act geplant, um die zivilrechtliche Haftung bei KI-Schäden zu regeln. Die EU-Kommission hat den Entwurf jedoch 2025 zurückgezogen. Haftungsfragen für KI-Schäden werden stattdessen über die überarbeitete Product Liability Directive geregelt, die ab Dezember 2026 gilt und Software sowie KI-Systeme ausdrücklich einschließt. Der AI Act selbst verfolgt mit seinen Bußgeldern und Marktüberwachungsbefugnissen einen öffentlich-rechtlichen Ansatz. Die Product Liability Directive ergänzt ihn um den privatrechtlichen Schadensersatz.

**Internationale Frameworks** wie die OECD AI Principles, das NIST AI Risk Management Framework (AI RMF) und der Standard ISO/IEC 42001 für KI-Managementsysteme setzen ergänzende Impulse. Sie sind nicht rechtsverbindlich, bieten aber bewährte Methoden für Risikomanagement und Governance, die bei der Umsetzung des EU AI Act helfen können. Unternehmen, die international tätig sind, profitieren davon, ihre Compliance-Strategie an diesen anerkannten Rahmenwerken auszurichten.

> **Praxis:** Die wichtigste Erkenntnis für die Praxis: Der EU AI Act ersetzt keine bestehenden Regelwerke, sondern ergänzt sie. Unternehmen, die bereits DSGVO-Prozesse, ein Datenschutz-Management-System oder eine CE-Konformitätsbewertung haben, starten nicht bei null. Das sind Bausteine, auf denen AI Compliance aufbauen kann.

# 3. BETRIFFT MICH DAS?

Der EU AI Act reguliert nicht KI-Technologie als solche, sondern die Rollen, die Organisationen im KI-Ökosystem einnehmen. Die zentrale Frage lautet daher nicht: „Nutzen wir KI?" Sondern: „In welcher Rolle nutzen wir KI?" Die Antwort bestimmt, welche Pflichten gelten. Dieses Kapitel erklärt die drei Hauptrollen, zeigt, wie sich die eigene Rolle bestimmen lässt, und macht deutlich, warum die meisten KMU als Betreiber einzustufen sind, aber nicht alle.

## Die drei Rollen im EU AI Act

Der EU AI Act unterscheidet drei zentrale Rollen, die jeweils unterschiedliche Pflichten nach sich ziehen. Die Definitionen finden sich in Artikel 3 der Verordnung.

**Anbieter (Provider)** ist, wer ein KI-System entwickelt oder entwickeln lässt und es unter eigenem Namen oder eigener Marke auf den Markt bringt oder in Betrieb nimmt. Die Provider-Rolle ist die pflichtintensivste: Anbieter tragen die Verantwortung für Konformitätsbewertung, CE-Kennzeichnung, technische Dokumentation und das gesamte Risikomanagement ihres Systems. In einfacher Sprache: Wer das System baut, trägt die Hauptverantwortung.

**Betreiber (Deployer)** ist, wer ein KI-System unter eigener Verantwortung einsetzt. Der Betreiber hat das System nicht selbst entwickelt, sondern von einem Anbieter bezogen und nutzt es im eigenen Geschäftsbetrieb. Die Pflichten sind weniger umfangreich als beim Anbieter, aber keineswegs vernachlässigbar: menschliche Aufsicht, Transparenz gegenüber betroffenen Personen, Überwachung des Systems im Betrieb und bei Hochrisiko-Systemen eine Grundrechte-Folgenabschätzung. In einfacher Sprache: Wer das System nutzt, trägt die Verantwortung für den sachgemäßen Einsatz.

**Händler (Distributor)** ist, wer ein KI-System eines Anbieters auf dem EU-Markt verfügbar macht, ohne es wesentlich zu verändern. Typische Händler sind Softwarereseller oder Systemhäuser, die KI-Lösungen anderer Hersteller vertreiben. Die Pflichten beschränken sich im Wesentlichen darauf, sicherzustellen, dass das System die CE-Kennzeichnung trägt und die erforderliche Dokumentation beigefügt ist. In einfacher Sprache: Wer das System weiterverkauft, muss prüfen, dass alles in Ordnung ist.

Daneben kennt der EU AI Act weitere Rollen wie den Importeur (bringt ein System aus einem Drittland in die EU) und den Bevollmächtigten (vertritt einen Nicht-EU-Anbieter

in der EU). Für die meisten KMU sind diese Rollen nicht relevant, da sie typischerweise als Betreiber agieren.

> **EU AI Act:** Art. 3 Nr. 3: „Anbieter" ist eine natürliche oder juristische Person, die ein KI-System entwickelt oder ein KI-System entwickeln lässt und es unter ihrem eigenen Namen oder ihrer eigenen Marke in Verkehr bringt oder das KI-System unter ihrem eigenen Namen oder ihrer eigenen Marke in Betrieb nimmt.

| Rolle | Kurzbeschreibung | Pflichtumfang | Typisches KMU-Szenario |
|---|---|---|---|
| **Anbieter (Provider)** | Entwickelt oder lässt entwickeln, bringt unter eigenem Namen auf den Markt | Hoch: Konformität, CE, Dokumentation, Risikomanagement | Eher untypisch, aber möglich bei eigener KI-Entwicklung |
| **Betreiber (Deployer)** | Setzt KI-System unter eigener Verantwortung ein | Mittel: Aufsicht, Transparenz, Monitoring | Der Regelfall für KMU |
| **Händler (Distributor)** | Macht KI-System auf dem EU-Markt verfügbar | Gering: Prüfung der Konformität und Dokumentation | IT-Dienstleister, Systemhäuser |

## Entscheidungsbaum: Welche Rolle habe ich?

Die eigene Rolle lässt sich mit wenigen Fragen bestimmen. Der folgende Entscheidungsbaum führt systematisch zum Ergebnis.

**Frage 1: Wird im Unternehmen ein KI-System selbst entwickelt oder dessen Entwicklung beauftragt, und wird es unter eigenem Namen bereitgestellt?** Wenn ja: Anbieter (Provider). Die vollen Provider-Pflichten gelten, einschließlich Konformitätsbewertung und technischer Dokumentation.

**Frage 2: Wird ein KI-System eines externen Anbieters im eigenen Geschäftsbetrieb eingesetzt?** Wenn ja: Betreiber (Deployer). Die Deployer-Pflichten aus Artikel 26 gelten, deren Umfang von der Risikoklasse des Systems abhängt.

**Frage 3: Werden KI-Systeme anderer Anbieter vertrieben oder weiterverkauft, ohne sie wesentlich zu verändern?** Wenn ja: Händler (Distributor). Die Pflichten beschränken sich auf Konformitätsprüfung und korrekte Weitergabe der Dokumentation.

**Frage 4: Treffen mehrere dieser Beschreibungen zu?** Dann liegen Mehrfachrollen vor. Ein Unternehmen kann gleichzeitig Anbieter eines eigenen KI-Systems und Betreiber eingekaufter KI-Lösungen sein. In diesem Fall gelten für jedes System die Pflichten der jeweiligen Rolle.

Ein Beispiel verdeutlicht die Mehrfachrolle: Ein mittelständischer IT-Dienstleister hat ein eigenes KI-gestütztes Ticketing-System entwickelt und vertreibt es an Kunden. Für dieses System ist das Unternehmen Anbieter. Gleichzeitig nutzt es Microsoft Copilot für interne Zwecke und eine KI-basierte Buchhaltungssoftware. Für diese Systeme ist es Betreiber. Beide Rollen bestehen nebeneinander, und für jedes System gelten die jeweiligen Pflichten.

> **Praxis:** Als ersten Schritt empfiehlt es sich, eine Liste aller im Unternehmen genutzten KI-Systeme zu erstellen und bei jedem System die Frage zu beantworten: Haben wir dieses System selbst entwickelt oder wesentlich verändert? In den meisten Fällen wird die Antwort „Nein" lauten. Damit ist die Rolle klar: Betreiber.

## Die typische KMU-Situation: Meist Betreiber

Die Realität in den meisten kleinen und mittleren Unternehmen ist eindeutig: KI-Systeme werden eingekauft und eingesetzt, nicht selbst entwickelt. Ein Handwerksbetrieb, der eine KI-gestützte Angebotskalkulation nutzt, ist Betreiber. Eine Steuerkanzlei, die KI-basierte Dokumentenanalyse einsetzt, ist Betreiber. Ein Logistikunternehmen, das KI-optimierte Routenplanung verwendet, ist Betreiber. Ein Maschinenbauer, der KI-basierte Qualitätskontrolle in seiner Fertigung einsetzt, ist Betreiber.

Betreiber zu sein bedeutet nicht, dass keine Pflichten bestehen. Die Betreiber-Pflichten aus Artikel 26 sind überschaubar, aber real. Die Intensität der Pflichten hängt maßgeblich von der Risikoklasse des eingesetzten Systems ab.

**Pflichten nach Risikoklasse: Der Anwendungsfall entscheidet**

Ein zentrales Prinzip des EU AI Act wird in der Praxis häufig missverstanden: Nicht das KI-System selbst bestimmt die Risikoklasse, sondern der konkrete Anwendungsfall. Dasselbe System kann je nach Einsatzkontext in unterschiedliche Risikoklassen fallen. Die entscheidende Größe ist daher der KI-Prozess, also die Kombination aus KI-System und Anwendungsbereich.

Ein Beispiel macht das greifbar: Ein Unternehmen setzt ein KI-gestütztes Textanalyse-Tool ein. Im Marketing generiert es Produktbeschreibungen und Social-Media-Beiträge.

Das ist minimales Risiko, es bestehen keine spezifischen Pflichten über die KI-Kompetenz nach Artikel 4 hinaus. Dasselbe Tool wird in der Personalabteilung eingesetzt, um Bewerbungen vorzusortieren und Kandidaten zu bewerten. Dieser Anwendungsfall fällt unter Anhang III Nr. 4 (Beschäftigung und Personalmanagement) und ist damit ein Hochrisiko-KI-Prozess. Ein System, zwei Anwendungsbereiche, zwei völlig unterschiedliche Compliance-Anforderungen.

Für Hochrisiko-KI-Prozesse müssen Betreiber unter anderem sicherstellen, dass das System gemäß der Gebrauchsanweisung des Anbieters eingesetzt wird, dass eine angemessene menschliche Aufsicht gewährleistet ist, dass die Eingabedaten dem Verwendungszweck entsprechen und dass relevante Vorfälle gemeldet werden. Bestimmte Betreiber, etwa öffentliche Einrichtungen, müssen zusätzlich eine Grundrechte-Folgenabschätzung (Fundamental Rights Impact Assessment) durchführen.

Für KI-Prozesse mit begrenztem Risiko gelten vor allem Transparenzpflichten: Personen, die mit einem Chatbot interagieren, müssen darüber informiert werden, und KI-generierte Inhalte müssen als solche gekennzeichnet sein.

Für KI-Prozesse mit minimalem Risiko bestehen keine spezifischen Pflichten aus dem EU AI Act. Die Pflicht zur KI-Kompetenz nach Artikel 4 gilt jedoch für alle Risikoklassen.

Diese prozessbasierte Betrachtung hat eine unmittelbare praktische Konsequenz: Ein vollständiges KI-Inventar allein reicht nicht aus. Erst wenn jedes KI-System seinen konkreten Anwendungsbereichen zugeordnet ist, lässt sich die Risikoklasse bestimmen und der tatsächliche Compliance-Aufwand ermitteln. Genau diesen Schritt bildet das NADOVO Framework in der DEFINE-Phase systematisch ab.

> **Praxis:** Betreiber zu sein ist kein Freifahrtschein. Entscheidend ist nicht die Rolle allein, sondern die Kombination aus Rolle und Risikoklasse. Ein Betreiber eines Hochrisiko-Systems hat deutlich mehr Pflichten als ein Betreiber eines Systems mit minimalem Risiko. Die Risikoklassifizierung ist daher der nächste logische Schritt nach der Rollenbestimmung und wird in Kapitel 4 ausführlich behandelt.

## Wann wird ein Betreiber zum Anbieter?

Artikel 25 des EU AI Act enthält eine Regelung, die besondere Beachtung verdient: die Rollenverschiebung (Role Shift). Unter bestimmten Umständen kann ein Betreiber zum Anbieter werden, mit allen Pflichten, die damit verbunden sind.

**Drei Szenarien lösen die Rollenverschiebung aus:**

**Szenario 1: Wesentliche Veränderung des Systems.** Wer ein KI-System so verändert, dass es nicht mehr dem ursprünglichen System des Anbieters entspricht, wird selbst zum Anbieter. Ein Beispiel: Ein Unternehmen kauft ein vortrainiertes Sprachmodell und trainiert es mit eigenen Branchendaten nach (Fine-Tuning), um es für spezifische Aufgaben wie die automatisierte Kreditwürdigkeitsprüfung einzusetzen. Durch das Fine-Tuning verändert sich das Verhalten des Modells wesentlich. Das Unternehmen wird zum Anbieter dieses veränderten Systems.

**Szenario 2: Bereitstellung unter eigenem Namen.** Wer ein KI-System eines anderen Anbieters nimmt und es unter eigenem Namen oder eigener Marke auf den Markt bringt, wird zum Anbieter, auch ohne technische Veränderung. Das klassische White-Label-Modell: Die Technologie stammt von einem Dritten, aber nach außen erscheint das Unternehmen als Anbieter.

**Szenario 3: Änderung des Verwendungszwecks.** Wer ein KI-System für einen anderen Zweck einsetzt als den vom ursprünglichen Anbieter vorgesehenen, wird zum Anbieter. Das gilt insbesondere dann, wenn durch die Zweckänderung eine andere Risikoklasse entsteht. Ein Beispiel: Ein KI-System, das für die Kundenanalyse im Marketing entwickelt wurde (minimales Risiko), wird stattdessen für die Bewertung von Kreditanträgen eingesetzt (Hochrisiko). Die Zweckänderung macht das Unternehmen zum Anbieter des Systems in diesem neuen Anwendungskontext.

**Die Konsequenzen sind erheblich.** Wer zum Anbieter wird, übernimmt die vollen Provider-Pflichten: Konformitätsbewertung, technische Dokumentation, CE-Kennzeichnung, Risikomanagement, Post-Market-Monitoring. Das sind Pflichten, die erhebliche Ressourcen und Expertise erfordern.

> **EU AI Act:** Art. 25 Abs. 1: Jede natürliche oder juristische Person gilt als Anbieter eines Hochrisiko-KI-Systems und unterliegt den Pflichten des Anbieters, wenn sie ein bereits in Verkehr gebrachtes oder in Betrieb genommenes Hochrisiko-KI-System wesentlich verändert.

Die gute Nachricht: Normale Konfiguration und Parametrierung im Rahmen der vom Anbieter vorgesehenen Einstellungen lösen keine Rollenverschiebung aus. Wer ein CRM-System mit integrierten KI-Funktionen nutzt und die Standard-Einstellungen anpasst, bleibt Betreiber. Die Schwelle zur „wesentlichen Veränderung" ist absichtlich hoch angesetzt.

**Praxis:** Eine einfache Schutzmaßnahme hilft, die unbeabsichtigte Rollenverschiebung zu vermeiden: Vor jeder Anpassung einer KI-Lösung, die über die Standard-Konfiguration hinausgeht, sollte geprüft werden, ob die Schwelle zur wesentlichen Veränderung überschritten wird. Besonders bei Fine-Tuning, eigenem Training mit Unternehmensdaten oder der Nutzung für nicht vorgesehene Zwecke ist Vorsicht geboten. Im Zweifel lohnt sich die Rücksprache mit dem Anbieter des Systems, der dokumentiert haben sollte, welche Anpassungen innerhalb des vorgesehenen Rahmens liegen.

# 4. RISIKOKLASSIFIZIERUNG

Der EU AI Act verfolgt einen risikobasierten Ansatz. Das bedeutet: Nicht jedes KI-System wird gleich behandelt. Die Regulierungsintensität richtet sich nach dem Risiko, das ein KI-System für die Gesundheit, Sicherheit und Grundrechte von Personen darstellt. Dieses Kapitel erklärt die vier Risikostufen, zeigt, wie der Anwendungsfall die Risikoklasse bestimmt, und liefert eine praktische Methode, um die eigenen KI-Systeme einzuordnen.

## Die vier Risikostufen

Der EU AI Act teilt KI-Systeme in vier Risikostufen ein. Je höher das Risiko, desto strenger die Anforderungen.

**Unannehmbares Risiko: Verboten.** Bestimmte KI-Anwendungen sind vollständig untersagt. Artikel 5 definiert die verbotenen Praktiken, die seit dem 2. Februar 2025 gelten. Dazu gehören unter anderem:

- Social Scoring durch Behörden: Die Bewertung von Personen auf Basis ihres Sozialverhaltens mit nachteiligen Konsequenzen.
- Manipulation durch unterschwellige Techniken: KI-Systeme, die das Verhalten von Personen auf eine Weise beeinflussen, die diese nicht erkennen können und die ihnen Schaden zufügt.
- Ausnutzung von Vulnerabilitäten: KI-Systeme, die gezielt Schwächen bestimmter Gruppen ausnutzen, etwa aufgrund von Alter, Behinderung oder sozialer Lage.
- Biometrische Echtzeit-Fernidentifizierung in öffentlichen Räumen: Mit eng definierten Ausnahmen für die Strafverfolgung.
- Emotionserkennung am Arbeitsplatz und in Bildungseinrichtungen: Mit Ausnahmen für medizinische oder sicherheitsrelevante Zwecke.
- Erzeugung nicht-einvernehmlicher intimer Darstellungen sowie von Darstellungen sexuellen Kindesmissbrauchs (CSAM): KI-Systeme, deren Zweck oder vernünftigerweise vorhersehbares Ergebnis die Erstellung solcher Inhalte ist. Dieses durch das Digital-Omnibus-Paket (Mai 2026) ergänzte Verbot wird nach einer Übergangsfrist ab dem 2. Dezember 2026 wirksam.

Für KMU ist die Verbotsliste eine klare rote Linie. Die meisten Unternehmen werden keines dieser Systeme einsetzen. Dennoch lohnt sich die Prüfung, denn manche Verbo-

en von Mitarbeitern im Homeoffice analysiert, um deren Produktivität zu messen, fällt beispielsweise unter das Verbot der Emotionserkennung am Arbeitsplatz.

**Hohes Risiko: Strenge Regulierung.** Hochrisiko-KI-Systeme unterliegen den umfassendsten Anforderungen des EU AI Act. Es gibt zwei Wege, auf denen ein KI-System als Hochrisiko eingestuft wird.

Der erste Weg führt über **Anhang I**: Wenn ein Produkt bereits einer EU-Konformitätsbewertung unterliegt (etwa als Maschine, Medizinprodukt oder Aufzug) und eine KI-Komponente als Sicherheitselement enthält, gilt das KI-System automatisch als Hochrisiko. Die Pflichten aus dem AI Act ergänzen dann die bestehenden Produktsicherheitsanforderungen.

Der zweite Weg führt über **Anhang III**: Dieser definiert acht Anwendungsbereiche, in denen KI-Systeme als Hochrisiko gelten. Er ist für die meisten KMU der relevantere Prüfmaßstab und wird im Abschnitt „Anhang I und Anhang III" ausführlich behandelt.

Die Pflichten für Hochrisiko-Systeme umfassen unter anderem Risikomanagement, Daten-Governance, technische Dokumentation, Transparenz, menschliche Aufsicht und Post-Market-Monitoring. Für Anbieter gelten zusätzlich Konformitätsbewertung und CE-Kennzeichnung. Kapitel 5 behandelt die Pflichten im Detail.

**Begrenztes Risiko: Transparenzpflichten.** KI-Systeme mit begrenztem Risiko unterliegen spezifischen Transparenzpflichten nach Artikel 50. Drei Kategorien fallen darunter:

- KI-Systeme, die direkt mit Personen interagieren (etwa Chatbots): Die betroffenen Personen müssen darüber informiert werden, dass sie mit einem KI-System kommunizieren.
- KI-Systeme, die synthetische Inhalte erzeugen (Text, Bild, Audio, Video): Die Anbieter dieser Systeme müssen die Ausgaben maschinenlesbar als KI-generiert kennzeichnen (Art. 50 Abs. 2). Für Systeme, die bereits vor dem 2. August 2026 auf dem Markt waren, gilt für diese Kennzeichnung eine Schonfrist bis zum 2. Dezember 2026 (Digital-Omnibus-Paket).
- Emotionserkennungs- und biometrische Kategorisierungssysteme (soweit nicht verboten): Die betroffenen Personen müssen über den Einsatz informiert werden.

Die Transparenzpflichten nach Art. 50 sind differenzierter als oft dargestellt. Die Kennzeichnungspflicht nach Art. 50 Abs. 2 trifft die Anbieter der KI-Systeme, nicht die Unternehmen, die diese Systeme als Werkzeug nutzen. Für Unternehmen relevant ist vor allem Art. 50 Abs. 4: Wer KI-generierte Texte zu Themen von öffentlichem Interesse veröffentlicht, muss die KI-Beteiligung offenlegen. Allerdings gilt eine praxisrelevante Ausnahme: Wurde der Inhalt einer menschlichen Überprüfung mit redaktioneller Verantw-

ortung unterzogen, entfällt diese Pflicht. Ein Unternehmen, das KI-gestützt einen Fachbericht erstellt, diesen inhaltlich prüft und unter eigenem Namen veröffentlicht, unterliegt also nicht der Kennzeichnungspflicht nach Art. 50 Abs. 4.

Deepfakes und synthetische Medien (Bild, Audio, Video), die reale Personen oder Ereignisse darstellen, müssen dagegen immer als KI-generiert gekennzeichnet werden (Art. 50 Abs. 4).

> **Praxis:** Unabhängig von der rechtlichen Pflicht kann eine freiwillige Transparenz über den Einsatz von KI-Werkzeugen ein Zeichen verantwortungsvoller Praxis sein, gerade für Unternehmen, die sich im Bereich AI Compliance positionieren.

**Minimales Risiko: Keine spezifischen Pflichten.** Die große Mehrheit der KI-Systeme fällt in diese Kategorie. Spamfilter, Rechtschreibprüfungen, einfache Empfehlungssysteme oder KI-gestützte Suchfunktionen unterliegen keinen spezifischen Pflichten aus dem EU AI Act. Der Gesetzgeber empfiehlt zwar freiwillige Verhaltenskodizes, schreibt aber nichts vor.

Zwei Einschränkungen gelten dennoch. Erstens: Die Pflicht zur KI-Kompetenz nach Artikel 4 gilt für alle KI-Systeme, unabhängig von der Risikoklasse. Zweitens: Die DSGVO und andere bestehende Regelwerke greifen unabhängig vom AI Act weiterhin.

## Das Kernprinzip: Der Anwendungsfall bestimmt die Risikoklasse

Dies ist die wichtigste Erkenntnis des gesamten Leitfadens: Nicht die Technologie bestimmt die Risikoklasse, sondern der Anwendungsfall. Dasselbe KI-Modell kann je nach Einsatzzweck in unterschiedliche Risikoklassen fallen. Die entscheidende Größe ist der **KI-Prozess**: die Kombination aus KI-System (Asset) und konkretem Anwendungsbereich.

Ein großes Sprachmodell (Large Language Model, LLM) verdeutlicht das Prinzip. Wird es für die Erstellung von Marketing-Texten eingesetzt, handelt es sich um ein System mit minimalem Risiko. Wird dasselbe Modell für eine automatisierte Vorauswahl von Bewerbungen genutzt, fällt es unter Anhang III Nr. 4 (Beschäftigung und Personalmanagement) und wird zum Hochrisiko-System. Wird es so konfiguriert, dass es das Verhalten von Personen auf unterschwellige Weise manipuliert, ist der Einsatz verboten.

Ein weiteres Beispiel: Bilderkennung. Die gleiche Technologie zur Klassifizierung von Produktfotos im E-Commerce ist minimales Risiko. Dieselbe Technologie zur biometrischen Identifizierung von Personen ist Hochrisiko oder je nach Kontext sogar verboten.

Und noch ein Beispiel aus dem KMU-Alltag: Ein KI-Chatbot. Im Kundenservice eingesetzt, unterliegt er den Transparenzpflichten (begrenztes Risiko). Wird derselbe Chatbot für die medizinische Erstberatung in einer Arztpraxis genutzt, kann er als Hochrisiko-System einzustufen sein.

> **Praxis:** Pauschale Einordnungen wie „unser KI-System ist kein Hochrisiko" greifen zu kurz. Jeder einzelne Anwendungsfall muss separat bewertet werden. Ein Unternehmen, das dasselbe KI-Tool in drei verschiedenen Abteilungen für drei verschiedene Zwecke einsetzt, hat möglicherweise drei verschiedene Risikoklassen zu berücksichtigen.

## Anhang I und Anhang III: Was steht drin?

**Anhang I** listet die harmonisierten EU-Produktvorschriften auf, die eine Konformitätsbewertung durch Dritte erfordern. Die Logik ist einfach: Wenn ein Produkt bereits reguliert ist (als Maschine, Aufzug, Medizinprodukt, Spielzeug, Sportboot, Seilbahn und weitere) und eine KI-Komponente als Sicherheitselement enthält, dann gilt die KI-Komponente automatisch als Hochrisiko. Für KMU, die regulierte Produkte mit KI-Komponenten herstellen, ist Anhang I der relevante Prüfpunkt. Die vollständige Anwendung der Pflichten für Anhang-I-Systeme beginnt am 2. August 2028 (mit dem Digital-Omnibus-Paket vom ursprünglichen 2. August 2027 verschoben). Das Digital-Omnibus-Paket engt zugleich die automatische Hochrisiko-Einstufung von Sicherheitskomponenten ein: KI, die ausschließlich unterstützende oder optimierende Funktionen erfüllt (Performance, Effizienz, Komfort oder Qualitätskontrolle) und deren Ausfall kein Gesundheits- oder Sicherheitsrisiko begründet, gilt nicht mehr automatisch als Hochrisiko. Für Maschinen- und Produkthersteller lohnt sich daher eine erneute Prüfung bestehender Einstufungen.

**Anhang III** ist für die meisten KMU die zentrale Prüfgrundlage. Er definiert acht Anwendungsbereiche, in denen KI-Systeme als Hochrisiko eingestuft werden. Die folgende Übersicht zeigt die Bereiche mit typischen Anwendungsbeispielen.

| Nr. | Bereich | Typische Anwendungen | KMU-Relevanz |
|---|---|---|---|
| 1 | Biometrische Identifizierung und Kategorisierung | Gesichtserkennung, biometrische Zugangskontrollen | Mittel: Relevant bei biometrischen Zeiterfassungssystemen |
| 2 | Kritische Infrastruktur | KI-Steuerung von Strom-, Gas-, Wassernetzen, Verkehrsleitsysteme | Gering für die meisten KMU |
| 3 | Bildung und Berufsausbildung | Automatisierte Prüfungsbewertung, Zugangsentscheidungen zu Bildungseinrichtungen | Gering bis mittel: Relevant für Bildungsanbieter |
| 4 | Beschäftigung und Personalmanagement | KI-gestütztes Bewerber-Screening, automatisierte Leistungsbewertung, Kündigungsentscheidungen | **Hoch**: Betrifft viele KMU |
| 5 | Zugang zu wesentlichen Dienstleistungen | KI-basierte Kreditwürdigkeitsprüfung, Versicherungsbewertung, Priorisierung von Notdiensten | Hoch: Relevant für Finanzdienstleister und Versicherer |
| 6 | Strafverfolgung | Risikoeinschätzung, Lügendetektoren, prädiktive Polizeiarbeit | Gering für privatwirtschaftliche KMU |
| 7 | Migration, Asyl und Grenzkontrolle | Risikobewertung, Dokumentenprüfung | Gering für die meisten KMU |
| 8 | Rechtspflege und demokratische Prozesse | KI-gestützte Rechtsrecherche mit Entscheidungsvorschlägen, Wahlbeeinflussung | Gering bis mittel |

Für die meisten KMU im DACH-Raum sind vor allem die Bereiche 4 (Beschäftigung) und 5 (wesentliche Dienstleistungen) relevant. Wer KI-Systeme im Personalwesen oder bei der Kreditvergabe einsetzt, sollte genau prüfen, ob der konkrete Anwendungsfall unter Anhang III fällt.

### Art. 6 Abs. 3: Die Ausnahme von der Hochrisiko-Einstufung

Ein KI-System, das in einen Anhang-III-Bereich fällt, gilt dann nicht als Hochrisiko, wenn es kein erhebliches Risiko für Gesundheit, Sicherheit oder Grundrechte birgt und

ondere das Ergebnis der Entscheidungsfindung nicht wesentlich beeinflusst. Voraussetzung ist, dass mindestens eine der folgenden vier Bedingungen erfüllt ist:

(a) Das KI-System ist dazu bestimmt, eine eng begrenzte Verfahrensaufgabe auszuführen.

(b) Das KI-System ist dazu bestimmt, das Ergebnis einer zuvor abgeschlossenen menschlichen Tätigkeit zu verbessern.

(c) Das KI-System ist dazu bestimmt, Entscheidungsmuster oder Abweichungen von früheren Entscheidungsmustern zu erkennen, ohne die menschliche Bewertung zu ersetzen oder wesentlich zu beeinflussen.

(d) Das KI-System ist dazu bestimmt, eine vorbereitende Aufgabe für eine Bewertung auszuführen, die für die Zwecke der in Anhang III aufgeführten Anwendungsfälle relevant ist.

Ein Beispiel: Ein KI-gestütztes Tool, das in der Personalabteilung eingehende Bewerbungen nach formalen Kriterien vorsortiert (vollständige Unterlagen, Mindestqualifikation), ohne eine inhaltliche Bewertung oder Rangfolge der Kandidaten vorzunehmen, könnte unter Bedingung (d) als vorbereitende Aufgabe eingestuft werden und damit von der Hochrisiko-Einstufung ausgenommen sein.

Die Ausnahme hat jedoch eine klare Grenze: Wenn ein KI-System Profiling natürlicher Personen vornimmt, gilt es immer als Hochrisiko, unabhängig davon, ob eine der vier Bedingungen erfüllt ist. Sobald also ein System Persönlichkeitsmerkmale, Verhaltensmuster oder persönliche Vorlieben systematisch auswertet, greift die Ausnahme nicht.

Wichtig für Anbieter: Wer sich auf die Ausnahme beruft, muss die Bewertung dokumentieren, bevor das System in Verkehr gebracht oder in Betrieb genommen wird (Art. 6 Abs. 4). Auf Verlangen der zuständigen Behörde ist diese Dokumentation vorzulegen. Zudem bleibt die Registrierungspflicht bestehen: Anbieter, die ihr System nach Artikel 6 Absatz 3 als nicht hochriskant einstufen, müssen es dennoch in der EU-Datenbank registrieren (Artikel 49). Eine im Digital-Omnibus-Entwurf zunächst vorgesehene Befreiung von dieser Registrierung wurde in der finalen Einigung nicht übernommen.

## Praxis-Check: Die eigenen Anwendungen einordnen

Die Einordnung der eigenen KI-Systeme in die Risikostufen ist keine Raketenwissenschaft, erfordert aber Systematik. Die folgende Schritt-für-Schritt-Methode führt zum Ergebnis.

**Schritt 1: Anwendungsfall beschreiben.** Was tut die KI konkret? Für welche Personen hat das Ergebnis Konsequenzen? Welche Art von Entscheidungen werden vorbereitet oder getroffen? Eine präzise Beschreibung des Anwendungsfalls ist die Grundlage für alles Weitere.

**Schritt 2: Gegen die Verbotsliste prüfen.** Fällt der Anwendungsfall unter eine der verbotenen Praktiken aus Artikel 5? Wenn ja: sofort einstellen. Die Verbote gelten bereits seit dem 2. Februar 2025.

**Schritt 3: Gegen Anhang III prüfen.** Fällt der Anwendungsfall in einen der acht Hochrisiko-Bereiche? Wenn ja: Liegt möglicherweise die Ausnahme nach Artikel 6 Absatz 3 vor? Wenn keine Ausnahme greift, handelt es sich um ein Hochrisiko-System.

**Schritt 4: Gegen Anhang I prüfen.** Ist das KI-System eine Sicherheitskomponente in einem regulierten Produkt? Wenn ja: Hochrisiko.

**Schritt 5: Transparenzpflichten prüfen.** Interagiert das System direkt mit Personen? Erzeugt es synthetische Inhalte? Wenn ja: Es gelten die Transparenzpflichten nach Artikel 50 (begrenztes Risiko).

**Schritt 6: Wenn kein Treffer.** Fällt der Anwendungsfall in keine der genannten Kategorien, handelt es sich um ein System mit minimalem Risiko. Es gelten keine spezifischen Pflichten aus dem AI Act, aber die allgemeine KI-Kompetenzpflicht nach Artikel 4.

Die folgende Tabelle zeigt die Einordnung typischer KMU-Anwendungsfälle.

| Anwendungsfall | Risikoklasse | Begründung |
|---|---|---|
| KI-gestützte Buchhaltungssoftware (Belegklassifizierung) | Minimal | Keine Anhang-III-Kategorie, keine direkte Personenbetroffenheit |
| Chatbot im Kundenservice | Begrenzt | Transparenzpflicht: Kunden müssen wissen, dass sie mit KI interagieren |
| KI-basiertes Bewerber-Screening | **Hoch** | Anhang III Nr. 4: Beschäftigung und Personalmanagement |
| KI-gestützte Kreditwürdigkeitsprüfung | **Hoch** | Anhang III Nr. 5: Zugang zu wesentlichen Dienstleistungen |
| KI-optimierte Routenplanung (Logistik) | Minimal | Keine Anhang-III-Kategorie, keine sicherheitskritische Funktion |
| Generative KI für Marketing-Texte | Begrenzt | Transparenzpflicht: KI-generierte Inhalte müssen kennzeichenbar sein |
| KI-Qualitätskontrolle als Sicherheitselement in Maschinen | **Hoch** | Anhang I: KI als Sicherheitskomponente in reguliertem Produkt |

**Praxis:** Die NADOVO-Kernformel fasst das Prinzip zusammen: **Asset + Anwendungsbereich = KI-Prozess, daraus ergibt sich die Risikoklasse.** Zuerst das KI-System identifizieren (Asset), dann den konkreten Anwendungsbereich beschreiben, daraus den KI-Prozess ableiten und schließlich die Risikoklasse bestimmen. Kapitel 7 zeigt, wie die DISCOVER-Phase des NADOVO Frameworks diese systematische Inventarisierung und Klassifizierung unterstützt. Kapitel 8 liefert den konkreten Fahrplan für die ersten vier Wochen.

# 5. PFLICHTEN NACH ROLLE UND RISIKOKLASSE

Kapitel 3 hat die Rollen geklärt, Kapitel 4 die Risikoklassen. Jetzt kommt beides zusammen: Welche konkreten Pflichten ergeben sich aus der Kombination von Rolle und Risikoklasse? Der Schwerpunkt liegt auf den Deployer-Pflichten, da die meisten KMU in dieser Rolle agieren. Die Provider-Pflichten werden im Überblick behandelt, denn auch Betreiber sollten wissen, was sie von ihren KI-Lieferanten erwarten können und müssen.

## Provider-Pflichten im Überblick

Anbieter (Provider) tragen die Hauptlast der Regulierung. Sie sind verantwortlich dafür, dass ein Hochrisiko-KI-System von der Entwicklung über die Markteinführung bis zur laufenden Überwachung den Anforderungen des EU AI Act entspricht.

Die wichtigsten Provider-Pflichten bei Hochrisiko-Systemen im Überblick:

**Risikomanagement (Art. 9):** Der Anbieter muss ein Risikomanagementsystem einrichten, das den gesamten Lebenszyklus des KI-Systems abdeckt. Risiken müssen identifiziert, bewertet und durch geeignete Maßnahmen gemindert werden.

**Daten-Governance (Art. 10):** Die Trainingsdaten müssen qualitativ hochwertig, repräsentativ und auf systematische Verzerrungen (Bias) geprüft sein. Die Anforderungen an die Datenqualität gelten auch für Test- und Validierungsdaten.

**Technische Dokumentation (Art. 11):** Eine umfassende technische Dokumentation muss erstellt und aktuell gehalten werden. Diese Dokumentation ist die Grundlage für die Konformitätsbewertung und muss den Behörden auf Anfrage zugänglich sein.

**Automatische Protokollierung (Art. 12):** Das KI-System muss so gestaltet sein, dass relevante Vorgänge automatisch aufgezeichnet werden (Logging). Die Protokolle ermöglichen die Nachvollziehbarkeit von Entscheidungen und die Erkennung von Risiken im Betrieb.

**Transparenz und Gebrauchsanweisungen (Art. 13):** Der Anbieter muss klare, verständliche Informationen über das System bereitstellen, insbesondere Gebrauchsanweisungen für den Betreiber. Diese müssen unter anderem den Verwendungszweck, die Leistungsgrenzen und die Anforderungen an die menschliche Aufsicht beschreiben.

**Menschliche Aufsicht (Art. 14):** Das System muss so konzipiert sein, dass eine wirksame menschliche Aufsicht möglich ist. Der Anbieter definiert, welche Aufsichtsmaßnahmen erforderlich sind, und stellt sicher, dass die technischen Voraussetzungen dafür gegeben sind.

**Genauigkeit, Robustheit und Cybersicherheit (Art. 15):** Das System muss ein angemessenes Maß an Genauigkeit, Robustheit und Cybersicherheit aufweisen und diese über den gesamten Lebenszyklus aufrechterhalten.

**Konformitätsbewertung und CE-Kennzeichnung (Art. 43):** Vor der Markteinführung muss der Anbieter eine Konformitätsbewertung durchführen. Je nach System kann das eine interne Prüfung oder eine Bewertung durch eine benannte Stelle (Notified Body) erfordern. Bei positivem Ergebnis wird die CE-Kennzeichnung angebracht.

**Post-Market Monitoring (Art. 72):** Nach der Markteinführung muss der Anbieter das System systematisch überwachen, Leistungsdaten sammeln und bei Bedarf Korrekturmaßnahmen ergreifen.

> **Praxis:** Auch wenn KMU meist nicht selbst Provider sind, lohnt es sich, diese Pflichten zu kennen. Sie bilden den Maßstab für die Lieferantenauswahl. Bei der Beschaffung von KI-Systemen, insbesondere Hochrisiko-Systemen, sollten folgende Fragen an den Anbieter gestellt werden: Liegt eine Konformitätsbewertung vor? Gibt es eine technische Dokumentation? Sind Gebrauchsanweisungen für den Deployer-Betrieb verfügbar? Welche Angaben macht der Anbieter zu Datenqualität und Bias-Prüfung? Ein Anbieter, der diese Fragen nicht beantworten kann, sollte nicht die erste Wahl sein.

## Deployer-Pflichten: Was KMU wirklich tun müssen

Die Pflichten für Betreiber (Deployer) sind weniger umfangreich als die der Anbieter, aber sie sind verbindlich und erfordern organisatorische Vorbereitung. Der Umfang hängt maßgeblich von der Risikoklasse des eingesetzten Systems ab.

**Bei Hochrisiko-Systemen (Art. 26):**

Die Deployer-Pflichten bei Hochrisiko-KI-Systemen lassen sich in sieben Kernbereiche gliedern.

**1. Bestimmungsgemäßer Einsatz.** Das KI-System muss gemäß der Gebrauchsanweisung des Anbieters eingesetzt werden. Das klingt selbstverständlich, hat aber regulatorische Bedeutung: Wer ein System außerhalb des vorgesehenen Verwendungszwecks

nutzt, riskiert nicht nur Fehlfunktionen, sondern auch eine Rollenverschiebung zum Provider (wie in Kapitel 3 beschrieben).

**2. Menschliche Aufsicht.** Der Betreiber muss sicherstellen, dass kompetentes Personal die Funktion des KI-Systems überwacht. Die betreffenden Personen müssen in der Lage sein, die Ausgaben des Systems zu verstehen, Anzeichen für Anomalien zu erkennen und das System bei Bedarf zu stoppen oder zu übersteuern. Das setzt voraus, dass die Mitarbeiter entsprechend geschult sind, was wiederum mit der KI-Kompetenzpflicht nach Artikel 4 zusammenhängt.

**3. Eingabedaten.** Soweit der Betreiber Kontrolle über die Eingabedaten hat, muss er sicherstellen, dass diese dem Verwendungszweck des Systems angemessen und hinreichend repräsentativ sind.

**4. Überwachung und Meldung.** Der Betreiber muss die Funktion des Systems im laufenden Betrieb überwachen. Bei Fehlfunktionen, Risiken oder schwerwiegenden Vorfällen besteht eine Meldepflicht gegenüber dem Anbieter und den zuständigen Marktüberwachungsbehörden.

**5. Protokollaufbewahrung.** Die vom System automatisch erzeugten Protokolle müssen mindestens sechs Monate aufbewahrt werden, sofern keine abweichenden Vorschriften gelten.

**6. Datenschutz-Folgenabschätzung.** Wenn der Einsatz des Hochrisiko-Systems eine Datenschutz-Folgenabschätzung (Data Protection Impact Assessment, DPIA) nach DSGVO erfordert, muss der Betreiber diese durchführen. Der EU AI Act verweist in Artikel 26 Absatz 9 ausdrücklich auf diese Pflicht. Kapitel 6 behandelt das Zusammenspiel von AI Act und DSGVO im Detail.

**7. Grundrechte-Folgenabschätzung.** Die FRIA-Pflicht nach Artikel 27 hat einen eng begrenzten Adressatenkreis: Einrichtungen des öffentlichen Rechts, private Einrichtungen, die öffentliche Dienste erbringen, sowie alle Betreiber von KI-Systemen zur Kreditwürdigkeitsprüfung (Anhang III Nr. 5 lit. b) und Risikobewertung bei Lebens- und Krankenversicherungen (Anhang III Nr. 5 lit. c). Für die meisten privaten KMU greift diese Pflicht nicht. Die FRIA bewertet die Auswirkungen des KI-Einsatzes auf die Grundrechte der betroffenen Personen.

> **EU AI Act:** Art. 26 Abs. 1: Die Betreiber von Hochrisiko-KI-Systemen treffen geeignete technische und organisatorische Maßnahmen, um sicherzustellen, dass sie solche Systeme gemäß den dem System beigefügten Betriebsanleitungen verwenden.

**Bei KI-Systemen mit begrenztem Risiko:**

Die Pflichten beschränken sich auf Transparenz. Personen, die mit einem KI-System interagieren (etwa einem Chatbot), müssen darüber informiert werden, dass sie mit einer KI kommunizieren. KI-generierte oder manipulierte Inhalte wie synthetische Bilder, Videos oder Texte müssen als solche kennzeichenbar und bei der Veröffentlichung auch gekennzeichnet sein.

**Bei KI-Systemen mit minimalem Risiko:**

Es bestehen keine spezifischen Pflichten aus dem EU AI Act. Dennoch empfiehlt es sich, auch diese Systeme im KI-Inventar zu führen und interne Nutzungsrichtlinien aufzustellen. Das schafft Transparenz und erleichtert die Anpassung, falls sich die Regulierung weiterentwickelt oder ein System für einen neuen Anwendungsfall mit höherer Risikoklasse eingesetzt werden soll.

> **Praxis:** Die Deployer-Pflichten bei Hochrisiko-Systemen sind anspruchsvoll, aber sie erfordern vor allem Organisation, nicht Technik. Das Rückgrat bilden drei Elemente: geschultes Personal (KI-Kompetenz), dokumentierte Prozesse (wer überwacht was, wie werden Vorfälle gemeldet) und eine funktionierende Kommunikation mit dem Anbieter des Systems. Wer diese drei Elemente aufbaut, hat die wesentlichen Grundlagen gelegt.

## Übersichtstabelle: Rolle mal Risikoklasse

Die folgende Matrix fasst die wichtigsten Pflichten nach Rolle und Risikoklasse zusammen. Sie dient als zentrale Referenz für den eigenen Handlungsbedarf.

| Risikoklasse | Provider (Anbieter) | Deployer (Betreiber) | Distributor (Händler) |
|---|---|---|---|
| **Unannehmbar** | Verboten | Verboten | Verboten |
| **Hoch** | Risikomanagement, Daten-Governance, technische Dokumentation, Logging, Transparenz, menschliche Aufsicht, Genauigkeit/Robustheit/Cybersicherheit, Konformitätsbewertung, CE-Kennzeichnung, Post-Market Monitoring | Bestimmungsgemäßer Einsatz, menschliche Aufsicht, Eingabedaten-Qualität, Überwachung und Meldepflicht, Protokollaufbewahrung, DPIA (wenn DSGVO-pflichtig), ggf. FRIA | CE-Kennzeichnung ur Dokumentation prüfe Konformität in der Lieferkette sicherstelle |
| **Begrenzt** | Transparenz sicherstellen, Kennzeichnung KI-generierter Inhalte ermöglichen | Nutzer über KI-Interaktion informieren, KI-generierte Inhalte kennzeichnen | Kennzeichnungspflich in Lieferkette weitergeben |
| **Minimal** | Keine spezifischen Pflichten (freiwillige Verhaltenskodizes empfohlen) | Keine spezifischen Pflichten (freiwillige Verhaltenskodizes empfohlen) | Keine spezifischen Pflichten |

**Für alle Risikoklassen gilt:** Die Pflicht zur KI-Kompetenz nach Artikel 4 betrifft jeden, der KI-Systeme betreibt oder beaufsichtigt, unabhängig von Rolle oder Risikoklasse. Das Digital-Omnibus-Paket (Mai 2026) hat den Wortlaut von Artikel 4 abgeschwächt (Förderung statt Sicherstellung der KI-Kompetenz), die Pflicht besteht jedoch unverändert fort.

## GPAI-Modelle: Was KMU als Nutzer wissen müssen

Neben den Pflichten für KI-Systeme regelt der EU AI Act in den Artikeln 51 bis 56 auch die Pflichten für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck (General Purpose AI, GPAI). Damit sind Modelle gemeint, die ein breites Spektrum unterschiedlicher Aufgaben kompetent erfüllen können, in der Praxis oft als Foundation Models bezeichnet: GPT, Claude, Gemini, Llama oder Mistral.

### Die vier Kernpflichten für alle GPAI-Anbieter (Art. 53)

Anbieter von GPAI-Modellen müssen seit dem 2. August 2025 folgende Pflichten erfüllen:

(a) Technische Dokumentation des Modells erstellen und aktuell halten (Anhang XI).

(b) Informationen und Dokumentation für nachgelagerte Anbieter bereitstellen, die das Modell in ihre KI-Systeme integrieren (Anhang XII).

(c) Eine Strategie zur Einhaltung des EU-Urheberrechts umsetzen, insbesondere zur Beachtung von Rechtsvorbehalten nach der Urheberrechtsrichtlinie (EU) 2019/790.

(d) Eine Zusammenfassung der für das Training verwendeten Inhalte erstellen und veröffentlichen, nach einer Vorlage des KI-Büros.

Open-Source-Ausnahme: Modelle, die unter einer freien und quelloffenen Lizenz bereitgestellt werden und deren Gewichte, Architektur und Nutzungsinformationen öffentlich zugänglich sind, sind von den Pflichten (a) und (b) befreit. Die Urheberrechtsstrategie (c) und die Trainingsdaten-Zusammenfassung (d) gelten auch für Open-Source-Modelle. Bei systemischem Risiko greift diese Ausnahme nicht.

**Zusätzliche Pflichten bei systemischem Risiko (Art. 55)**

GPAI-Modelle mit systemischem Risiko, also Modelle mit besonders hoher Leistungsfähigkeit oder Reichweite (Art. 51), unterliegen verschärften Anforderungen: Modellbewertung und Angriffstests (adversarial testing) zur Identifikation systemischer Risiken, Beobachtung und Meldung schwerwiegender Vorfälle an das KI-Büro sowie Gewährleistung eines angemessenen Cybersicherheitsniveaus.

**Was bedeutet das für KMU?**

Die Compliance-Last für GPAI-Modelle liegt bei deren Anbietern, nicht bei den Unternehmen, die darauf aufbauende KI-Systeme nutzen. Die GPAI-spezifischen Pflichten der Art. 53 bis 55 treffen Unternehmen wie OpenAI (als Anbieter des GPAI-Modells GPT), nicht das nutzende Unternehmen.

Dabei ist eine Rollenunterscheidung wichtig: OpenAI ist GPAI-Modellanbieter. Microsoft integriert GPT in ein eigenes Produkt (Copilot) und ist damit Anbieter eines KI-Systems mit eigenen Pflichten nach Art. 16 ff., aber nicht Anbieter des zugrunde liegenden GPAI-Modells.

Für Unternehmen stellt sich die Frage, ob sie durch den Einsatz solcher KI-Systeme zum Betreiber im Sinne des EU AI Act werden. Art. 3 Nr. 4 definiert einen Betreiber als jemand, der ein KI-System "unter eigener Verantwortung" verwendet. Ein Unternehmen, das Microsoft Copilot lizenziert und in seine Geschäftsprozesse integriert, ist Betreiber und unterliegt den Pflichten nach Art. 26. Die gelegentliche Nutzung von ChatGPT über den Browser durch einzelne Mitarbeiter begründet dagegen nicht ohne Weiteres eine Betreiberrolle. Entscheidend ist, ob das Unternehmen den Einsatz des KI-Systems organisatorisch verantwortet.

Praxisleitfäden als Compliance-Nachweis: Bis zur Veröffentlichung harmonisierter Normen können GPAI-Anbieter ihre Pflichterfüllung durch Einhaltung der Praxisleitfäden (Codes of Practice) nach Art. 56 nachweisen. Das KI-Büro der EU-Kommission hat den finalen Code of Practice am 10. Juli 2025 veröffentlicht, die Kommission und das KI-Gremium haben ihn am 2. August 2025 als angemessenes Compliance-Instrument bestätigt. Die Einhaltung ist freiwillig, begründet aber eine Konformitätsvermutung. Die aktive Durchsetzung durch das KI-Büro (Auskunftsersuchen, Modellzugang) beginnt ab dem 2. August 2026.

Bei Verstößen gegen die GPAI-Pflichten drohen Bußgelder von bis zu 15 Mio. Euro oder 3 % des weltweiten Jahresumsatzes (Art. 101 Abs. 1).

> **Praxis:** Der rote Faden bleibt unverändert: Der Anwendungsfall bestimmt die Risikoklasse. Das gilt auch und gerade für GPAI-basierte Systeme. Die GPAI-Modellanbieter tragen ihre eigenen Pflichten, nachgelagerte KI-Systemanbieter wie Microsoft ihre. Aber welche Pflichten für das einsetzende Unternehmen gelten, hängt davon ab, wofür das System konkret genutzt wird und ob das Unternehmen als Betreiber agiert.

# 6. ZUSAMMENSPIEL MIT DER DSGVO

Der EU AI Act steht nicht allein. Er tritt in ein regulatorisches Umfeld ein, das bereits seit 2018 von der Datenschutz-Grundverordnung (DSGVO) geprägt ist. Da die meisten KI-Systeme personenbezogene Daten verarbeiten, greifen beide Verordnungen häufig gleichzeitig. Die gute Nachricht: Bestehende DSGVO-Prozesse bilden eine solide Grundlage für AI Compliance. Dieses Kapitel zeigt, wo sich die beiden Regelwerke überschneiden, wo sie sich ergänzen und wie KMU Synergien nutzen können, ohne doppelte Strukturen aufzubauen.

## Was regelt die DSGVO, was der EU AI Act?

Die beiden Verordnungen haben unterschiedliche Regelungsgegenstände, aber einen breiten gemeinsamen Anwendungsbereich.

**Die DSGVO** regelt den Schutz personenbezogener Daten. Sie definiert, unter welchen Bedingungen personenbezogene Daten erhoben, verarbeitet und gespeichert werden dürfen, welche Rechte betroffene Personen haben und welche organisatorischen und technischen Maßnahmen zum Datenschutz erforderlich sind. Die DSGVO ist seit Mai 2018 in Kraft, und die meisten Unternehmen haben inzwischen Prozesse etabliert: Verzeichnis der Verarbeitungstätigkeiten, Datenschutz-Folgenabschätzungen, Auftragsverarbeitungsverträge, Datenschutzbeauftragter.

**Der EU AI Act** reguliert den Einsatz von KI-Systemen. Er definiert, unter welchen Bedingungen KI-Systeme entwickelt, bereitgestellt und betrieben werden dürfen, welche Risikostufen existieren und welche Pflichten sich daraus ergeben. Der Fokus liegt nicht auf den Daten allein, sondern auf dem System und seinem Anwendungsfall: Wie trifft die KI Entscheidungen? Welche Risiken entstehen daraus für betroffene Personen? Ist menschliche Aufsicht gewährleistet?

**Beide Verordnungen gelten parallel.** Der EU AI Act stellt in Artikel 2 Absatz 7 ausdrücklich klar, dass die Rechte der Betroffenen aus der DSGVO unberührt bleiben. DSGVO-Compliance ersetzt keine AI-Act-Compliance und umgekehrt. Wer ein KI-System einsetzt, das personenbezogene Daten verarbeitet, muss beide Verordnungen erfüllen.

Ein Beispiel verdeutlicht das Zusammenspiel: Ein KI-gestütztes Bewerber-Screening verarbeitet Lebensläufe mit personenbezogenen Daten (Name, Berufserfahrung, Qualifikationen). Die DSGVO verlangt eine Rechtsgrundlage für die Verarbeitung, Transparenz gegenüber den Bewerbern und das Recht auf nicht ausschließlich automatisierte

Entscheidungen. Der EU AI Act klassifiziert das System als Hochrisiko (Anhang III Nr. 4) und verlangt zusätzlich menschliche Aufsicht, Risikomanagement, Dokumentation und Überwachung. Beide Anforderungssets müssen erfüllt werden.

## Überschneidungen und Synergien

Die DSGVO und der EU AI Act verfolgen verwandte Ziele: den Schutz natürlicher Personen vor Risiken durch automatisierte Verarbeitung und Entscheidungsfindung. An mehreren Stellen überschneiden sich die Anforderungen.

**Transparenz.** Die DSGVO verlangt Transparenz bei der Verarbeitung personenbezogener Daten (Artikel 13 und 14 DSGVO): Betroffene müssen wissen, welche Daten zu welchem Zweck verarbeitet werden. Der EU AI Act verlangt Transparenz beim Einsatz von KI-Systemen: Personen müssen wissen, dass sie mit einer KI interagieren (Artikel 50), und Betreiber von Hochrisiko-Systemen müssen betroffene Personen über den KI-Einsatz informieren (Artikel 26 Absatz 11).

**Automatisierte Entscheidungen.** Artikel 22 DSGVO gibt betroffenen Personen das Recht, nicht einer ausschließlich auf automatisierter Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihnen gegenüber rechtliche Wirkung entfaltet. Artikel 14 EU AI Act verlangt menschliche Aufsicht bei Hochrisiko-KI-Systemen. Beide Regelungen zielen in dieselbe Richtung: Menschen sollen nicht vollständig automatisierten Entscheidungen ausgeliefert sein.

**Rechenschaftspflicht.** Beide Verordnungen verlangen Dokumentation und Nachweisbarkeit. Die DSGVO nennt es Rechenschaftspflicht (Accountability, Artikel 5 Absatz 2 DSGVO): Der Verantwortliche muss nachweisen können, dass die Datenschutzgrundsätze eingehalten werden. Der EU AI Act verlangt technische Dokumentation, Protokollierung und die Fähigkeit, die Compliance gegenüber Behörden zu belegen.

**Datenqualität.** Das DSGVO-Prinzip der Richtigkeit (Artikel 5 Absatz 1 lit. d) verlangt, dass personenbezogene Daten sachlich richtig und auf dem neuesten Stand sind. Der EU AI Act stellt in Artikel 10 Anforderungen an die Qualität und Repräsentativität der Trainings-, Validierungs- und Testdaten. Beide Anforderungen können in einem gemeinsamen Datenqualitätsprozess adressiert werden.

Die folgende Tabelle zeigt die wichtigsten Parallelen.

| DSGVO-Prinzip | Parallele im EU AI Act | Synergiepotenzial |
|---|---|---|
| Transparenz (Art. 13/14) | Transparenzpflichten (Art. 50), Informationspflichten (Art. 26) | Gemeinsame Informationsprozesse für Betroffene |
| Automatisierte Entscheidungen (Art. 22) | Menschliche Aufsicht (Art. 14) | Integriertes Konzept für Human Oversight |
| Datenrichtigkeit (Art. 5(1)(d)) | Daten-Governance (Art. 10) | Gemeinsames Datenqualitätsmanagement |
| Rechenschaftspflicht (Art. 5(2)) | Dokumentation, Logging, Konformität | Erweiterte Compliance-Dokumentation |
| Datenschutz-Folgenabschätzung (Art. 35) | Grundrechte-Folgenabschätzung (Art. 27), Risikomanagement (Art. 9) | Integriertes Assessment-Verfahren |
| Auftragsverarbeitung (Art. 28) | Lieferanten-Due-Diligence, Provider-Pflichten | Erweiterte Vendor-Prüfung |

> **Praxis:** Unternehmen, die ihre DSGVO-Prozesse sauber aufgesetzt haben, starten nicht bei null. Die bestehende Infrastruktur aus Datenschutz-Management-System, Verarbeitungsverzeichnis, DPIA-Methodik und Vendor-Management bildet ein Fundament, auf dem AI Compliance aufbauen kann.

## DPIA und AI Risk Assessment: Synergien nutzen

Eine der größten Synergien liegt im Bereich der Risikobewertung. Die DSGVO kennt die Datenschutz-Folgenabschätzung (Data Protection Impact Assessment, DPIA), der EU AI Act die Grundrechte-Folgenabschätzung (Fundamental Rights Impact Assessment, FRIA) und das Risikomanagementsystem nach Artikel 9. Die Methodik aller drei Instrumente ist verwandt: Risiken identifizieren, bewerten, Maßnahmen definieren und dokumentieren.

**Die DPIA (Artikel 35 DSGVO)** ist Pflicht, wenn eine Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringt. Bei KI-Systemen, die personenbezogene Daten verarbeiten, ist das regelmäßig der Fall.

**Die Grundrechte-Folgenabschätzung (Fundamental Rights Impact Assessment, FRIA) nach Artikel 27 EU AI Act** hat einen eng begrenzten Adressatenkreis. Verpflichtet sind Einrichtungen des öffentlichen Rechts und private Einrichtungen, die öffentliche Dienste erbringen, wenn sie Anhang-III-Hochrisiko-KI-Systeme einsetzen. Darüber hinaus gilt die Pflicht für alle Betreiber, also auch rein private Unternehmen, von KI-Systemen zur Kreditwürdigkeitsprüfung natürlicher Personen (Anhang III Nr. 5 lit. b) und zur Risikobewertung bei Lebens- und Krankenversicherungen (Anhang III Nr. 5 lit. c).

Für die meisten privaten KMU bedeutet das: Die FRIA ist keine unmittelbare Pflicht, sofern sie keine öffentlichen Dienstleistungen erbringen und nicht in den Bereichen Kreditbewertung oder Versicherung tätig sind. Die FRIA bewertet die Auswirkungen des KI-Einsatzes auf Grundrechte und geht damit über den reinen Datenschutz hinaus: Nichtdiskriminierung, Gleichbehandlung, Zugang zu wesentlichen Dienstleistungen und menschliche Aufsicht gehören zum Bewertungsumfang.

**Das Risikomanagementsystem (Artikel 9 EU AI Act)** ist primär eine Provider-Pflicht. Es muss den gesamten Lebenszyklus des KI-Systems abdecken und Risiken systematisch identifizieren, bewerten und mindern.

Die Unterschiede liegen im Fokus: Die DPIA blickt auf Datenschutzrisiken, die FRIA auf Grundrechte im weiteren Sinne, das Risikomanagementsystem auf systemische KI-Risiken. Aber die Methodik überschneidet sich erheblich.

Die pragmatische Empfehlung lautet: Ein integriertes Assessment-Verfahren aufbauen, das alle relevanten Perspektiven in einem modularen Prozess abdeckt. Statt drei separate Dokumente zu erstellen, kann die DPIA als Ausgangspunkt dienen und um KI-spezifische Fragen erweitert werden: Welche Grundrechte sind betroffen? Wie ist die menschliche Aufsicht organisiert? Welche KI-spezifischen Risiken bestehen, etwa systematische Verzerrungen (Bias), fehlerhafte Ausgaben (Halluzinationen) oder schleichende Leistungsveränderungen (Drift)?

Ein solcher integrierter Ansatz spart Ressourcen und liefert zugleich bessere Ergebnisse, weil Wechselwirkungen zwischen Datenschutz- und KI-Risiken nicht isoliert, sondern im Zusammenhang betrachtet werden.

Der EU AI Act unterstützt diesen integrierten Ansatz ausdrücklich: Art. 27 Abs. 4 bestimmt, dass die FRIA eine bereits durchgeführte DPIA nach Art. 35 DSGVO ergänzt, nicht ersetzt. Ebenso verweist Art. 26 Abs. 9 Betreiber von Hochrisiko-KI-Systemen explizit auf die DPIA-Pflicht. Die Verknüpfung beider Instrumente ist also nicht nur pragmatisch sinnvoll, sondern vom Gesetzgeber vorgesehen.

## Praktische Empfehlungen für KMU

Fünf konkrete Schritte helfen KMU, die Synergien zwischen DSGVO und EU AI Act zu nutzen.

**1. Verarbeitungsverzeichnis als Ausgangspunkt für das KI-Inventar.** Das Verzeichnis der Verarbeitungstätigkeiten nach Artikel 30 DSGVO dokumentiert bereits, welche personenbezogenen Daten im Unternehmen verarbeitet werden und mit welchen Systemen. Dieses Verzeichnis lässt sich als Ausgangspunkt für das KI-Inventar nutzen: Welche der dokumentierten Verarbeitungen nutzen KI-Komponenten? Welche zusätzlichen KI-Systeme sind im Einsatz, die bisher nicht im Verarbeitungsverzeichnis erfasst sind, weil sie keine personenbezogenen Daten verarbeiten?

**2. Datenschutzbeauftragten einbinden.** Der Datenschutzbeauftragte (DSB) kennt die DSGVO-Prozesse, hat Erfahrung mit Risikobewertungen und ist mit den relevanten Abteilungen vernetzt. Es ist sinnvoll, AI-Compliance-Themen beim DSB anzusiedeln oder zumindest eng mit ihm abzustimmen, statt eine parallele Compliance-Struktur aufzubauen.

**3. Bestehende Prozesse erweitern, nicht ersetzen.** Das Datenschutz-Management-System (DSMS) um KI-spezifische Aspekte ergänzen, statt ein separates AI-Compliance-System zu schaffen. Das betrifft insbesondere die Risikobewertungsmethodik, die Vendor-Prüfung und die Dokumentation.

**4. Auftragsverarbeitung bei KI-as-a-Service prüfen.** Viele KMU nutzen KI als Cloud-Dienst (KI-as-a-Service). In diesen Fällen werden personenbezogene Daten in der Regel an den KI-Anbieter übermittelt. Das erfordert einen Auftragsverarbeitungsvertrag nach Artikel 28 DSGVO. Gleichzeitig verlangt der EU AI Act eine Prüfung, ob der Provider seine Pflichten erfüllt (CE-Kennzeichnung, technische Dokumentation, Gebrauchsanweisung). Beide Prüfungen lassen sich in einem integrierten Vendor-Assessment zusammenfassen.

**5. Rechtsgrundlagen für KI-bezogene Datenverarbeitung klären.** Wenn Unternehmensdaten für KI-Training oder Fine-Tuning verwendet werden, müssen die DSGVO-Rechtsgrundlagen geprüft werden. Das gilt insbesondere, wenn personenbezogene Daten betroffen sind. Die üblichen Rechtsgrundlagen (Einwilligung, berechtigtes Interesse, Vertragserfüllung) sind auch hier anwendbar, erfordern aber eine spezifische Prüfung im KI-Kontext.

**Praxis:** Der Zusatzaufwand für AI Compliance ist für Unternehmen mit etablierten DSGVO-Prozessen überschaubar. Das Muster ist dasselbe: Inventar, Risikobewertung, Dokumentation, laufende Überwachung. Wer die DSGVO-Einführung bewältigt hat, verfügt über die organisatorische Reife, auch den EU AI Act umzusetzen. Der entscheidende Schritt ist, die bestehende Infrastruktur bewusst als Sprungbrett zu nutzen, statt parallel von vorne anzufangen.

# 7. NADOVO FRAMEWORK: DER EINSTIEG

Die bisherigen Kapitel haben gezeigt, was der EU AI Act regelt, welche Rollen und Risikoklassen existieren, welche Pflichten daraus entstehen und wie das Zusammenspiel mit der DSGVO funktioniert. Die entscheidende Frage lautet jetzt: Wo anfangen? Dieses Kapitel stellt das NADOVO AI Compliance Framework als strukturierten Ansatz vor, der die Komplexität handhabbar macht.

## Das Problem: Wo anfangen?

113 Artikel, 13 Anhänge, multiple Rollen, vier Risikoklassen, gestaffelte Fristen und ein wachsendes Ökosystem aus ergänzenden Regelwerken. Die Informationsfülle zum EU AI Act ist beträchtlich, und die Überforderung, die daraus entsteht, ist nachvollziehbar. In der Praxis zeigen sich vier typische Reaktionsmuster, die alle in eine Sackgasse führen.

**„Wir warten ab und schauen, was passiert."** Abwarten klingt nach einer risikoarmen Strategie, ist aber das Gegenteil. Die Verbote und die KI-Kompetenzpflicht gelten bereits seit dem 2. Februar 2025. Die umfassenden Hochrisiko-Pflichten greifen ab dem 2. Dezember 2027 (mit dem Digital-Omnibus-Paket vom ursprünglichen 2. August 2026 verschoben). Wer erst dann anfängt, hat keine Zeit mehr für eine sorgfältige Umsetzung.

**„Wir machen alles auf einmal."** Der Versuch, die gesamte AI Compliance in einem einzigen Großprojekt zu bewältigen, führt regelmäßig zur Überforderung. Das Projekt wird zu komplex, die Beteiligten verlieren den Überblick, und am Ende versandet es.

**„Der Datenschutzbeauftragte macht das nebenbei."** AI Compliance berührt zwar den Datenschutz (wie Kapitel 6 gezeigt hat), geht aber deutlich darüber hinaus. Risikomanagement, technische Bewertung, Lieferantenprüfung und organisatorische Maßnahmen erfordern ein eigenes Vorgehen, auch wenn der DSB ein wichtiger Partner ist.

**„Wir kaufen ein Tool."** Compliance-Software kann Prozesse unterstützen, aber sie ersetzt kein Verständnis der eigenen KI-Landschaft. Wer nicht weiß, welche KI-Systeme im Einsatz sind und wofür, kann auch mit dem besten Tool keine sinnvolle Compliance aufbauen.

Was fehlt, ist ein strukturierter, schrittweiser Ansatz, der die Komplexität in handhabbare Abschnitte zerlegt und einen klaren Anfangspunkt definiert.

## NADOVO als Compliance Lifecycle

Das NADOVO AI Compliance Framework ist ein praxisorientierter Lifecycle-Ansatz, der genau diese Struktur liefert.

Die Grundidee: AI Compliance ist kein einmaliges Projekt mit einem definierten Endpunkt. Es ist ein kontinuierlicher Kreislauf, der sich an Veränderungen anpasst. Neue KI-Systeme kommen hinzu, bestehende werden verändert, regulatorische Anforderungen entwickeln sich weiter. Ein statischer Compliance-Zustand existiert nicht.

Das Framework besteht aus fünf Phasen, die als Kreislauf organisiert sind. Vier Kernphasen bilden den operativen Zyklus: DISCOVER, DEFINE, ASSESS und IMPLEMENT. Sie repräsentieren die zwei Seiten der Compliance-Arbeit: Verstehen (DISCOVER und DEFINE) und Umsetzen (ASSESS und IMPLEMENT). Die fünfte Phase, MONITOR, umrahmt den gesamten Zyklus als kontinuierliche Überwachung und stellt sicher, dass die Compliance aktuell bleibt.

Der Lifecycle stellt sicher, dass nichts vergessen wird, dass jede Phase auf der vorherigen aufbaut und dass die Ergebnisse regelmäßig überprüft und aktualisiert werden.


Der NADOVO Continuous Compliance Cycle

## Die fünf Phasen im Überblick

### Phase 1: DISCOVER (Asset Management)

**Was wird getan:** Inventarisierung aller KI-Systeme im Unternehmen, einschließlich eingebetteter KI-Funktionen in bestehender Software und nicht genehmigter Schatten-KI.

**Kernfrage:** Welche KI-Systeme sind im Einsatz, auch diejenigen, von denen bisher niemand wusste?

**Ergebnis:** Ein vollständiges KI-Register (AI Inventory), das alle KI-Assets mit ihren grundlegenden Eigenschaften erfasst: Name, Anbieter, Einsatzbereich, Art der KI-Funktion, betroffene Daten.

Die DISCOVER-Phase ist der Startpunkt jeder AI-Compliance-Initiative. Ohne ein vollständiges Inventar fehlt die Grundlage für alles Weitere. Die Erfahrung zeigt: In den meisten Unternehmen sind deutlich mehr KI-Systeme im Einsatz, als zunächst angenommen. Das liegt an eingebetteten KI-Funktionen in Standardsoftware und an der unkontrollierten Nutzung externer KI-Dienste durch einzelne Mitarbeiter.

> **Praxis:** Mit den Top 10 starten, nicht mit dem Anspruch auf Vollständigkeit. Die wichtigsten und offensichtlichsten KI-Systeme zuerst erfassen, dann systematisch erweitern. Ein Inventar, das 80 Prozent abdeckt, ist unendlich wertvoller als ein Perfektionsanspruch, der nie umgesetzt wird.

### Phase 2: DEFINE (Process Management)

**Was wird getan:** Für jedes erfasste KI-Asset den konkreten Anwendungsfall definieren, die Rolle im Sinne des EU AI Act zuweisen (Provider, Deployer, Distributor) und den zugehörigen Geschäftsprozess beschreiben.

**Kernfrage:** Wofür wird jedes System eingesetzt, und wer ist verantwortlich?

**Ergebnis:** Dokumentierte Anwendungsfälle mit klarer Rollenzuordnung. Jedes KI-Asset ist einem oder mehreren Geschäftsprozessen zugeordnet, und für jeden Prozess ist die Rolle des Unternehmens dokumentiert.

Die DEFINE-Phase wendet die NADOVO-Kernformel an: **Asset + Anwendungsbereich = KI-Prozess.** Das KI-System allein sagt noch nichts über die Risikoklasse aus. Erst der konkrete Anwendungsfall, also das „Wofür", ermöglicht die Einordnung. Deshalb muss jeder Anwendungsfall einzeln definiert und dokumentiert werden.

### Phase 3: ASSESS (Risk Management)

**Was wird getan:** Jeden definierten Prozess einer Risikoklasse zuordnen, die Risiken bewerten und den Handlungsbedarf priorisieren.

**Kernfrage:** Welche Risikoklasse ergibt sich aus dem Anwendungsfall?

**Ergebnis:** Eine vollständige Risikoklassifizierung aller KI-Prozesse und eine priorisierte Handlungsliste. Systeme mit unannehmabrem Risiko müssen sofort eingestellt werden. Hochrisiko-Systeme erfordern umfassende Maßnahmen. Systeme mit begrenztem

Risiko benötigen Transparenzmaßnahmen. Systeme mit minimalem Risiko brauchen keine spezifischen Maßnahmen.

Die ASSESS-Phase nutzt die in Kapitel 4 beschriebene Methode: Prüfung gegen die Verbotsliste (Artikel 5), gegen Anhang III (Hochrisiko-Bereiche), gegen Anhang I (regulierte Produkte) und gegen die Transparenzpflichten (Artikel 50).

### Phase 4: IMPLEMENT (Compliance Execution)

**Was wird getan:** Die erforderlichen Maßnahmen umsetzen, abgestuft nach Risikoklasse und Rolle.

**Kernfrage:** Was muss konkret getan werden, um compliant zu sein?

**Ergebnis:** Umgesetzte Compliance-Maßnahmen. Das umfasst je nach Bedarf: Dokumentation, menschliche Aufsicht, Schulungen, Lieferantenverträge, Prozessanpassungen, Transparenzmaßnahmen und Meldeprozesse.

Die IMPLEMENT-Phase setzt die Erkenntnisse aus den ersten drei Phasen in konkrete Maßnahmen um. Der Umfang variiert erheblich: Für ein Hochrisiko-System als Deployer sind deutlich mehr Maßnahmen erforderlich als für ein System mit minimalem Risiko. Kapitel 5 hat die Pflichten nach Rolle und Risikoklasse im Detail beschrieben. Die IMPLEMENT-Phase macht daraus Arbeitspakete.

> **Praxis:** Bei Hochrisiko-Systemen mit dem Wichtigsten beginnen: menschliche Aufsicht organisieren und die Dokumentation aufsetzen. Diese beiden Maßnahmen sind sowohl regulatorisch als auch operativ am wirkungsvollsten.

### Phase 5: MONITOR (Continuous Compliance)

**Was wird getan:** Laufende Überwachung der implementierten Maßnahmen, Aktualisierung des KI-Inventars bei Veränderungen und regelmäßige Überprüfung der Compliance.

**Kernfrage:** Funktionieren die Maßnahmen noch? Gibt es neue KI-Systeme, veränderte Anwendungsfälle oder regulatorische Entwicklungen?

**Ergebnis:** Ein lebendiges Compliance-System, das sich an Veränderungen anpasst, statt zu veralten.

MONITOR ist keine einmalige Phase, sondern ein dauerhafter Prozess. Er stellt sicher, dass das KI-Inventar aktuell bleibt, dass neue KI-Systeme den Lifecycle durchlaufen, bev-

or sie in Betrieb genommen werden, und dass bestehende Bewertungen bei Änderungen aktualisiert werden.

> **Praxis:** Quartalsweise Reviews einplanen. Bei jeder wesentlichen Softwareänderung, jedem neuen KI-Tool und jedem veränderten Anwendungsfall den Zyklus erneut durchlaufen. Das KI-Inventar sollte ein lebendes Dokument sein, kein einmal erstellter und dann vergessener Bericht.

## Die Kernformel

Die NADOVO-Kernformel verdichtet das Grundprinzip des EU AI Act in eine operative Handlungsanweisung:

**Asset + Anwendungsbereich = KI-Prozess, daraus ergibt sich die Risikoklasse.**

Ein durchgängiges Beispiel zeigt die Formel in der Anwendung.

**Das Asset:** Microsoft Azure OpenAI Service (GPT-4), eingesetzt in einem mittelständischen Dienstleistungsunternehmen.

**Anwendungsfall 1:** Das Modell wird für die interne FAQ-Beantwortung genutzt. Mitarbeiter stellen Fragen zu internen Prozessen, das System liefert Antworten auf Basis der Unternehmensdokumentation. Der Prozess: Wissensmanagement. Die Risikoklasse: Minimal. Es sind keine personenbezogenen Entscheidungen betroffen, keine Anhang-III-Kategorie einschlägig.

**Anwendungsfall 2:** Dasselbe Modell wird in der Personalabteilung für die automatisierte Vorauswahl von Bewerbungen eingesetzt. Es analysiert Lebensläufe und erstellt eine Rangliste der Kandidaten. Der Prozess: Recruiting-Screening. Die Risikoklasse: Hoch. Anhang III Nr. 4 (Beschäftigung und Personalmanagement) ist einschlägig. Die vollen Deployer-Pflichten für Hochrisiko-Systeme greifen.

Gleiches Asset, unterschiedliche Risikoklassen. Die Technologie ist identisch. Was sich ändert, ist der Anwendungsfall. Und der Anwendungsfall bestimmt die Risikoklasse. Diese Erkenntnis ist das operative Herzstück von NADOVO und zugleich das Grundprinzip des EU AI Act.

## Weiterführend

NADOVO ist bewusst als Framework konzipiert, nicht als starres Regelwerk. Es lässt sich an verschiedene Unternehmensgrößen und Reifegrade anpassen. Ein Start-up mit drei

KI-Tools durchläuft den Zyklus schneller als ein mittelständisches Unternehmen mit 50 KI-Anwendungen, aber die Methodik bleibt dieselbe.

Dieser Leitfaden gibt den Überblick über die fünf Phasen und ihre Zusammenhänge. Für die vertiefte Umsetzung bietet das NADOVO Framework detaillierte Templates, Checklisten und Methodiken, die den Lifecycle Schritt für Schritt operationalisieren.

NADOVO versteht sich als pragmatischer Ansatz, nicht als einziger. Das Framework ist kompatibel mit etablierten Standards wie ISO/IEC 42001 (KI-Managementsysteme), dem NIST AI Risk Management Framework und den OECD AI Principles. Unternehmen, die bereits mit einem dieser Rahmenwerke arbeiten, können NADOVO als Ergänzung nutzen, die den EU-AI-Act-spezifischen Compliance-Fokus liefert.

> **Praxis:** Die Tiefe der Umsetzung bestimmt jedes Unternehmen selbst, je nach Risikolage und Ambition. Manche Unternehmen benötigen ein umfassendes KI-Governance-System. Andere kommen mit einem sauberen Inventar und dokumentierten Risikoklassifizierungen aus. NADOVO gibt die Richtung vor. Das nächste Kapitel liefert den konkreten Fahrplan für die ersten vier Wochen.

# 8. ERSTE SCHRITTE: SOFORT LOSLEGEN

Theorie ist wichtig. Aber Theorie ohne Umsetzung ist wertlos. Dieses Kapitel liefert einen konkreten 4-Wochen-Plan, mit dem jedes KMU sofort starten kann. Der Plan folgt den ersten drei Phasen des NADOVO Frameworks (DISCOVER, DEFINE, ASSESS) in einer verdichteten Form, die für den Einstieg ausreicht.

## Die ersten vier Wochen: Der Fahrplan

Zunächst ein realistisches Erwartungsmanagement: In vier Wochen wird kein Unternehmen vollständig AI-Act-compliant sein. Das ist auch nicht das Ziel. Das Ziel ist eine solide Basis: Überblick über die eigene KI-Landschaft, Klarheit über Rollen und Risikoklassen, eine priorisierte Handlungsliste. Das ist mehr, als die meisten Unternehmen heute haben.

Der Plan erfordert keinen Vollzeiteinsatz. Pro Woche sind realistisch vier bis acht Stunden Arbeit einzuplanen, verteilt auf die verantwortliche Person und kurze Abstimmungen mit Fachabteilungen. Die Ressourcen sind überschaubar. Was es braucht, ist die Entscheidung, anzufangen.

## Woche 1: KI-Inventar starten (DISCOVER)

**Ziel:** Die fünf bis zehn wichtigsten KI-Systeme im Unternehmen identifizieren und dokumentieren.

**Vorgehen:**

**1. IT-Landschaft durchgehen.** Welche Software ist im Unternehmen im Einsatz? Welche dieser Systeme hat KI-Funktionen? Viele Standardanwendungen enthalten inzwischen KI-Komponenten: Microsoft 365 mit Copilot, CRM-Systeme mit KI-gestütztem Lead-Scoring, Buchhaltungssoftware mit automatischer Belegklassifizierung, ERP-Systeme mit KI-basierter Bestelloptimierung.

**2. Fachabteilungen befragen.** Eine gezielte Frage an die Abteilungsleiter: Welche KI-Tools oder KI-Funktionen werden in der Abteilung genutzt? Hier zeigt sich häufig die in Kapitel 1 beschriebene Schatten-KI: Mitarbeiter, die eigenständig ChatGPT, Midjourney, DeepL oder andere KI-Dienste nutzen, ohne dass die IT-Abteilung davon weiß.

**3. Cloud-Dienste prüfen.** Welche SaaS-Lösungen sind im Einsatz, und welche davon verwenden KI im Hintergrund? Ein Blick auf die aktuellen Produktbeschreibungen der

eingesetzten Cloud-Dienste zeigt oft KI-Funktionen, die bei der ursprünglichen Beschaffung noch nicht existierten.

**4. Ergebnis dokumentieren.** Eine einfache Tabelle reicht für den Anfang:

| Systemname | Anbieter | Art (Cloud/On-Premise/intern) | Einsatzbereich | Nutzerkreis | Personenbezo Daten? |
|---|---|---|---|---|---|
| Microsoft 365 Copilot | Microsoft | Cloud | Unternehmensweit | Alle Mitarbeiter | Ja |
| HubSpot (KI-Scoring) | HubSpot | Cloud | Vertrieb | Vertriebsteam | Ja |
| ChatGPT (Team) | OpenAI | Cloud | Diverse | Einzelne Mitarbeiter | Potenziell |
| DATEV (KI-Belegerfassung) | DATEV | Cloud | Buchhaltung | Finanzbuchhaltung | Ja |
| … | … | … | … | … | … |

> **Praxis:** Perfektion ist nicht nötig. Mit dem starten, was bekannt ist, und sukzessive ergänzen. Ein Inventar, das 80 Prozent der KI-Systeme erfasst, ist die Grundlage für alles Weitere. Ohne dieses Inventar bleibt AI Compliance ein abstraktes Vorhaben.

## Woche 2: Rollen bestimmen (DEFINE, Teil 1)

**Ziel:** Für jedes identifizierte KI-System die eigene Rolle im Sinne des EU AI Act klären.

**Vorgehen:**

Für jedes System im Inventar zwei Fragen stellen:

**Frage 1: Wurde das System im Unternehmen selbst entwickelt oder wesentlich verändert?** Wenn nein (was bei den meisten KMU der Fall sein wird): Die Rolle ist Betreiber (Deployer).

**Frage 2: Wird das System unter eigenem Namen oder eigener Marke bereitgestellt?** Wenn ja: Die Rolle ist potenziell Anbieter (Provider), und die deutlich umfangreicheren Provider-Pflichten müssen geprüft werden.

In der Praxis werden etwa 90 Prozent der KMU bei allen ihren KI-Systemen als Deployer einzustufen sein. Das ist eine entlastende Erkenntnis, denn die Deployer-Pflichten sind überschaubarer als die Provider-Pflichten (wie Kapitel 5 gezeigt hat).

Das Inventar wird um eine Spalte ergänzt:

| Systemname | ... | Rolle |
|---|---|---|
| Microsoft 365 Copilot | ... | Deployer |
| HubSpot (KI-Scoring) | ... | Deployer |
| ChatGPT (Team) | ... | Deployer |
| Eigenes Ticketing-System mit KI | ... | Provider |

Besondere Aufmerksamkeit verdienen Fälle, in denen KI-Systeme nachtrainiert, per Fine-Tuning angepasst oder für einen anderen Zweck eingesetzt werden als vom Anbieter vorgesehen. Hier kann die in Kapitel 3 beschriebene Rollenverschiebung greifen.

## Woche 3: Anwendungsfälle definieren und klassifizieren (DEFINE/ASSESS)

**Ziel:** Für jedes KI-System den konkreten Anwendungsfall dokumentieren und die Risikoklasse bestimmen.

**Vorgehen:**

**Schritt 1: Anwendungsfall beschreiben.** Was tut die KI im Unternehmen? Welche Entscheidungen werden getroffen oder vorbereitet? Welche Personen sind betroffen?

**Schritt 2: Gegen Artikel 5 prüfen (Verbote).** Fällt der Anwendungsfall unter eine verbotene Praktik? Wenn ja: sofort einstellen.

**Schritt 3: Gegen Anhang III prüfen (Hochrisiko).** Fällt der Anwendungsfall in einen der acht Hochrisiko-Bereiche? Besonders die Bereiche 4 (Beschäftigung) und 5 (wesentliche Dienstleistungen) sind für KMU relevant. Wenn ja, sollte zusätzlich geprüft werden, ob die Ausnahme nach Artikel 6 Absatz 3 greift (siehe Kapitel 4).

**Schritt 4: Transparenzpflichten prüfen (Artikel 50).** Interagiert das System direkt mit Personen? Werden synthetische Inhalte erzeugt?

**Schritt 5: Risikoklasse zuordnen.** Unannehmbar, Hoch, Begrenzt oder Minimal.

Die NADOVO-Kernformel kommt hier zur Anwendung: **Asset + Anwendungsbereich = KI-Prozess, daraus ergibt sich die Risikoklasse.**

Das Inventar wird erneut erweitert:

| Systemname | Rolle | Anwendungsfall | Risikoklasse |
|---|---|---|---|
| Microsoft 365 Copilot | Deployer | Textunterstützung, E-Mail-Zusammenfassungen | Minimal |
| HubSpot (KI-Scoring) | Deployer | Lead-Priorisierung im Vertrieb | Minimal |
| ChatGPT (Team) | Deployer | Interne Recherche, Texterstellung | Begrenzt (Transparenz) |
| KI-Bewerber-Screening | Deployer | Vorauswahl von Bewerbungen | **Hoch** (Anhang III Nr. 4) |

> **Praxis:** Nach Woche 3 liegt ein klares Bild vor: welche KI-Systeme im Einsatz sind, in welcher Rolle das Unternehmen agiert und welche Risikoklasse jeweils gilt. Das ist die Grundlage für alle weiteren Entscheidungen.

## Woche 4: Ergebnisse dokumentieren und nächste Schritte planen

**Ziel:** Bisherige Ergebnisse konsolidieren, Handlungsbedarf priorisieren und das weitere Vorgehen planen.

**Vorgehen:**

**1. Inventar-Dokument finalisieren.** Die Ergebnisse der Wochen 1 bis 3 in einem sauberen Dokument zusammenfassen und mit der Geschäftsführung abstimmen. Dieses Dokument ist das KI-Register des Unternehmens und die Basis aller weiteren Compliance-Maßnahmen.

**2. Hochrisiko-Systeme priorisieren.** Gibt es KI-Systeme, die als Hochrisiko eingestuft wurden? Diese erfordern die umfangreichsten Maßnahmen und sollten zuerst angegangen werden. Für jedes Hochrisiko-System eine erste Maßnahmenliste erstellen: menschliche Aufsicht, Dokumentation, Meldeprozesse, Lieferantenprüfung.

**3. Quick Wins umsetzen.** Manche Maßnahmen lassen sich sofort umsetzen: einen Chatbot-Hinweis ergänzen, der Kunden darauf aufmerksam macht, dass sie mit einer

KI interagieren. Eine interne KI-Nutzungsrichtlinie für Mitarbeiter erstellen, die regelt, welche KI-Tools genutzt werden dürfen und welche Daten nicht in externe KI-Systeme eingegeben werden dürfen.

**4. Verantwortlichkeiten klären.** Wer im Unternehmen ist für AI Compliance zuständig? Idealerweise eine Person, die die Themen koordiniert und als zentrale Anlaufstelle fungiert. Das kann der Datenschutzbeauftragte sein (mit erweitertem Mandat), ein IT-Leiter oder eine eigens benannte Person.

**5. Zeitplan bis zum 2. Dezember 2027 erstellen.** Welche Maßnahmen müssen bis zum Stichtag umgesetzt sein? Welche Ressourcen werden dafür benötigt? Ein realistischer Meilensteinplan hilft, den Überblick zu behalten.

## Wie es weitergeht

Nach vier Wochen steht die Basis. Die nächsten Schritte führen in die IMPLEMENT- und MONITOR-Phasen des NADOVO Frameworks.

**Hochrisiko-Systeme:** Für jedes identifizierte Hochrisiko-System die detaillierten Deployer-Pflichten aus Kapitel 5 umsetzen. Menschliche Aufsicht organisieren, Dokumentation aufbauen, Meldeprozesse definieren, Lieferantenverträge prüfen.

**Monitoring aufsetzen:** Einen Prozess etablieren, der sicherstellt, dass das KI-Inventar bei jeder wesentlichen Änderung aktualisiert wird. Quartalsweise Reviews einplanen.

**KI-Richtlinie für Mitarbeiter:** Eine verbindliche Richtlinie entwickeln, die die Nutzung von KI-Tools im Unternehmen regelt. Das adressiert sowohl die Schatten-KI-Problematik als auch die KI-Kompetenzpflicht nach Artikel 4.

**Lieferanten-Management:** Compliance-Anforderungen an KI-Provider definieren. Bei der Beschaffung neuer KI-Systeme die Fragen aus Kapitel 5 (Konformitätsbewertung, technische Dokumentation, Gebrauchsanweisungen) standardmäßig stellen.

Das NADOVO AI Compliance Framework bietet für jede dieser Aufgaben detaillierte Templates, Checklisten und Methodiken. Der KI-Service-Desk der Bundesnetzagentur steht als Anlaufstelle für spezifische Fragen zur Verfügung.

**Praxis:** AI Compliance ist kein Sprint, sondern ein kontinuierlicher Prozess. Aber der wichtigste Schritt ist getan: Der Überblick steht, die Risikoklassen sind bekannt, und der Handlungsbedarf ist priorisiert. Das ist die Grundlage, auf der alles Weitere aufbaut. Die Fristen laufen, aber wer jetzt startet, hat ausreichend Zeit für eine sorgfältige Umsetzung.

## Wie geht es weiter?

Du weißt jetzt, worauf es beim EU AI Act ankommt. Die entscheidende Frage ist: Wo steht dein Unternehmen konkret, und welche Schritte sind für dich die richtigen?

In einem kostenlosen, unverbindlichen Erstgespräch ordnen wir deine Situation gemeinsam ein, und du nimmst einen klaren nächsten Schritt mit.

**Termin direkt buchen: cal.com/contoro.solutions**

## Hinweis zur Erstellung dieses Leitfadens

Dieser Leitfaden wurde unter Einsatz KI-gestützter Schreibwerkzeuge erstellt. Die fachliche Konzeption, inhaltliche Strukturierung, Qualitätssicherung und redaktionelle Verantwortung liegen vollständig beim Autor. Sämtliche Inhalte wurden geprüft und entsprechen dem Stand der Regulierung zum Zeitpunkt der Veröffentlichung.

Diese Kennzeichnung erfolgt freiwillig im Sinne der Transparenzpflichten des EU AI Act (Art. 50) und entspricht der Überzeugung, dass der verantwortungsvolle Einsatz von KI mit Offenheit beginnt.

## Rechtlicher Hinweis

Dieser Leitfaden dient ausschließlich der allgemeinen Information und stellt keine Rechtsberatung dar. Trotz sorgfältiger Erstellung kann keine Gewähr für Vollständigkeit, Richtigkeit und Aktualität übernommen werden. Für die Umsetzung regulatorischer Anforderungen wird die Hinzuziehung fachkundiger Beratung empfohlen.

## Impressum und Urheberrecht



**Kontakt**

CONTORO SOLUTIONS OÜ
E-Mail: info@contoro.solutions
Web: www.contoro.solutions Web: www.nadovo.ai

**Stand:** Juni 2026