NEXUS
MANAGEMENT CONSULTING

EU AI Act: Compliance-Fahrplan

Risikoklassifizierung, Pflichten und 5-Schritte-Plan für Unternehmen

Whitepaper | März 2026

Simon Schilling
Geschäftsführer & Principal Consultant
Nexus Management Consulting GmbH | nexuscon.net

Management Summary

Am 2. August 2026 tritt der EU AI Act vollständig in Kraft. Er betrifft nicht nur KI-Entwickler, sondern auch Anwender – also jedes Unternehmen, das ChatGPT, Copilot, RPA mit KI oder eigene Modelle einsetzt. Bußgelder bis 35 Mio. EUR drohen.

> **Ziel**
> Dieses Whitepaper erklärt die vier Risikoklassen, zeigt die konkreten Pflichten und gibt einen praxisnahen 5-Schritte-Plan zur Vorbereitung.

1. Was ist der EU AI Act?

Der EU AI Act verfolgt einen risikobasierten Ansatz: Je höher das Risiko eines KI-Systems, desto strenger die Anforderungen. Er definiert drei Rollen:

- **Anbieter (Provider):** Entwickelt oder vertreibt KI-Systeme
- **Betreiber (Deployer):** Setzt KI-Systeme ein – auch SaaS! Hier fallen die meisten Unternehmen hinein.
- **Importeur:** Bringt KI-Systeme aus Drittländern in die EU

1.1 Timeline

Datum	Was gilt	Bedeutung
02.02.2025	Verbote in Kraft	Verbotene KI-Praktiken sofort einstellen
02.08.2025	GPAI-Regeln	Transparenzpflichten für GPT-ähnliche Modelle
02.08.2026	Vollständige Geltung	Alle Pflichten, alle Bußgelder
02.08.2027	Annex I Pflichten	Eingebettete KI-Systeme

2. Die vier Risikoklassen im Detail

Das Herzstück des EU AI Act ist die Einteilung in vier Risikoklassen:

EU AI Act – Risikopyramide

2.1 Unannehmbares Risiko (verboten seit 02/2025)

Diese KI-Systeme sind in der EU grundsätzlich verboten:

- Social Scoring durch Behörden
- Emotionserkennung am Arbeitsplatz und in Bildungseinrichtungen
- Biometrische Echtzeit-Fernidentifizierung in öffentlichen Räumen
- Manipulative KI-Techniken, die Schaden verursachen

2.2 Hohes Risiko (streng reguliert, ab 08/2026)

KI-Systeme in kritischen Bereichen:

Bereich	Beispiele	Typische Betroffene
Personalwesen	KI-Recruiting, Leistungsbewertung	HR-Abteilungen, Konzerne
Kreditwürdigkeit	Scoring, Bonitätsprüfung	Banken, Fintechs
Bildung	Prüfungsbewertung, Zugangssteuerung	Hochschulen
Kritische Infrastruktur	KI in Energie, Wasser, Verkehr	KRITIS-Betreiber
Medizinprodukte	KI-gestützte Diagnostik	Krankenhäuser, Labore

Die 8 Pflichten für Hochrisiko-KI

- **1. Risikomanagement:** Identifikation, Bewertung und Minimierung von Risiken
- **2. Datenqualität:** Anforderungen an Trainingsdaten
- **3. Technische Dokumentation:** Vollständige Systembeschreibung
- **4. Logging:** Automatische Aufzeichnung der Systemaktivitäten
- **5. Transparenz:** Klare Information an Nutzer
- **6. Menschliche Aufsicht:** Human-in-the-Loop / Human-on-the-Loop
- **7. Genauigkeit & Robustheit:** Zuverlässigkeit, Schutz vor Bias
- **8. Cybersecurity:** Schutz vor Manipulation und Angriffen

2.3 Begrenztes Risiko (Transparenzpflichten)

Betrifft nahezu jedes Unternehmen mit Chatbots oder KI-generierten Inhalten:

- Chatbots müssen als KI gekennzeichnet werden
- KI-generierte Inhalte müssen als solche erkennbar sein
- Deepfakes müssen gekennzeichnet werden

2.4 Minimales Risiko

Spam-Filter, Empfehlungssysteme – keine besonderen Pflichten. Freiwillige Verhaltenskodizes empfohlen.

3. Bußgelder

Verstoß	Bußgeld	KMU-Regelung
Verbotene KI-Praktiken	Bis 35 Mio. EUR oder 7 % Umsatz	Reduziert, keine Ausnahme von Pflichten
Hochrisiko-Anforderungen	Bis 15 Mio. EUR oder 3 % Umsatz	Reduziert
Falsche Info an Behörden	Bis 7,5 Mio. EUR oder 1 % Umsatz	Reduziert

4. 5-Schritte-Plan zur Vorbereitung

Schritt 1: KI-Inventar erstellen

Erfassen Sie alle KI-Systeme – auch die „unsichtbaren":

Kategorie	Beispiele	Häufig übersehen?
Eigenentwickelt	ML-Modelle, Python-Skripte mit LLM	Nein
SaaS mit KI	ChatGPT, GitHub Copilot, DeepL Pro	Ja – Shadow AI!
Eingebettete KI	Copilot in M365, Salesforce Einstein	Ja
RPA mit KI	UIPath DocumentUnderstanding	Teilweise
Analytics	Recommendation Engines, Scoring	Ja

Schritt 2: Risikoklassifizierung

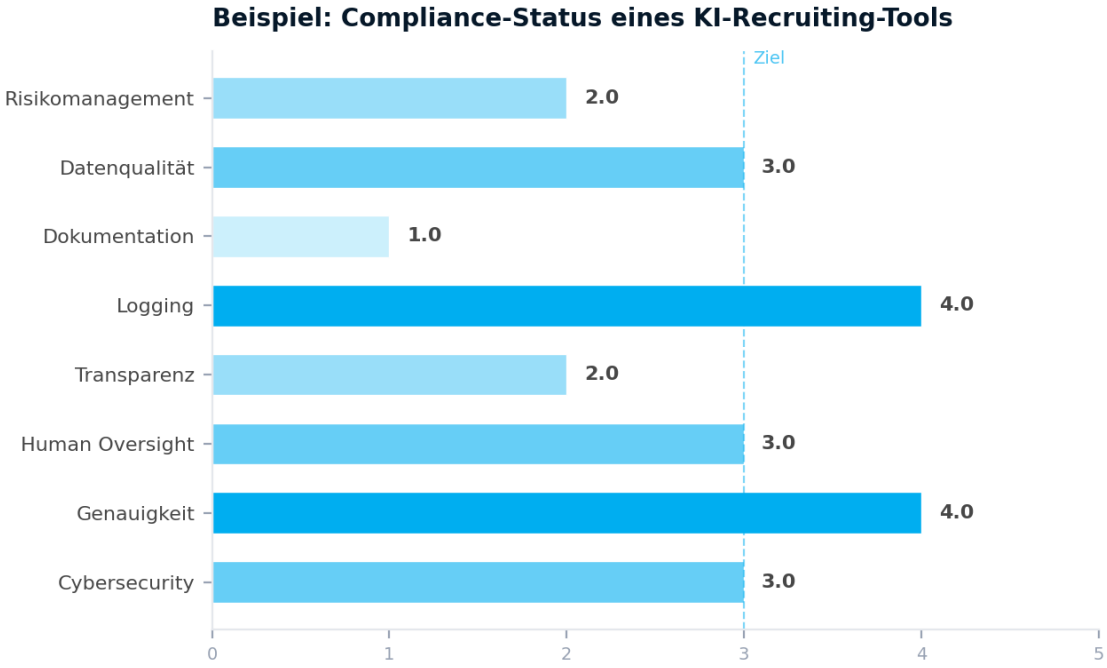
Ordnen Sie jedes identifizierte KI-System einer der vier Risikoklassen zu. Nutzen Sie die Annex-Listen des AI Act (Annex I für Produktsicherheit, Annex III für Hochrisiko-Bereiche) als Prüfraster. Dokumentieren Sie die Begründung

für jede Einstufung – die Aufsichtsbehörden werden diese nachfragen. Bei Unsicherheit empfiehlt sich eine konservative Einstufung: Eine spätere Herabstufung ist deutlich einfacher als eine nachträgliche Hochstufung.

Besonders wichtig: Auch KI-Systeme, die von Drittanbietern als „minimal risk" eingestuft werden, können in Ihrem spezifischen Einsatzkontext als Hochrisiko gelten. Die Risikoklasse hängt nicht nur vom System ab, sondern auch vom Einsatzzweck.

Schritt 3: Gap-Analyse für Hochrisiko-Systeme

Für jedes als Hochrisiko eingestufte System müssen die 8 Anforderungen des Art. 9–15 systematisch geprüft werden. Die folgende Visualisierung zeigt ein typisches Ergebnis aus einem EU AI Act Assessment. In der Praxis sind technische Anforderungen (Logging, Cybersecurity) oft besser erfüllt als organisatorische (Risikomanagement, Transparenz, Dokumentation):



Schritt 4: KI-Governance aufbauen

KI-Governance ist das organisatorische Rückgrat der EU AI Act Compliance. Ohne klare Rollen, Prozesse und Entscheidungswege bleibt die Compliance auf dem Papier. Laut einer Umfrage von PwC (2024) haben nur 23 % der Unternehmen in der EU bereits eine formale KI-Governance-Struktur etabliert:

- **Rollen definieren:** Wer ist für KI-Compliance verantwortlich? CIO, CDO, CISO oder ein dedizierter AI Officer? In größeren Organisationen empfiehlt sich ein KI-Board mit Vertretern aus IT, Fachbereich, Compliance und Datenschutz.
- **Genehmigungsprozess:** Neue KI-Systeme dürfen erst nach Risikoklassifizierung und Compliance-Prüfung freigegeben werden. Das gilt auch für SaaS-Tools und eingebettete KI.

- **Schulungen:** Alle Mitarbeitenden, die KI-Systeme einsetzen, müssen über Transparenzpflichten und Kennzeichnungsregeln informiert sein.
- **Reporting:** Regelmäßiger KI-Compliance-Status an die Geschäftsführung – analog zum NIS2-Cybersicherheits-Reporting.

Schritt 5: Dokumentation und Monitoring

Der EU AI Act verlangt umfangreiche und laufende Dokumentation – insbesondere für Hochrisiko-Systeme. Dies ist keine einmalige Aufgabe, sondern ein kontinuierlicher Prozess:

- **Technische Dokumentation** für alle Hochrisiko-Systeme gemäß Art. 11 – inklusive Systembeschreibung, Zweck, Grenzen, Testverfahren und Genauigkeitsmetriken
- **Logging-System** für automatische Aufzeichnung aller relevanten Systemaktivitäten – als Grundlage für Nachvollziehbarkeit und Audit
- **KI-System-Register** als lebendes Dokument, das bei jeder Änderung (neues System, Risikoklassenänderung, Außerbetriebnahme) aktualisiert wird
- **Regelmäßige Überprüfung** mindestens jährlich, ob die Risikoklassifizierung noch korrekt ist und die Compliance-Maßnahmen noch greifen

5. EU AI Act + NIS2: Synergien nutzen

Viele Unternehmen sind gleichzeitig betroffen. Ein integrierter Ansatz spart erheblich Zeit und Geld:

Anforderung	EU AI Act	NIS2	Synergie
Risikomanagement	Art. 9	Art. 21	Gemeinsames Framework
Dokumentation	Art. 11	ISMS-Doku	Einheitliches DMS
Incident Response	Monitoring	24h/72h	Integrierter Prozess
Schulungen	Transparenz	GF-Pflicht	Kombiniertes Programm
Audits	Konformität	BSI-Prüfung	Integrierter Audit-Plan

6. Fazit & nächste Schritte

Der EU AI Act ist keine ferne Zukunft – August 2026 steht unmittelbar bevor. Unternehmen, die jetzt mit der Vorbereitung beginnen, haben einen klaren Vorteil gegenüber denen, die auf die ersten Enforcement-Fälle warten. Die Erfahrung mit der DSGVO-Einführung 2018 zeigt: Wer frühzeitig handelt, spart langfristig erhebliche Kosten und vermeidet Hektik kurz vor der Deadline.

Der wichtigste erste Schritt: Wissen, welche KI-Systeme im Unternehmen eingesetzt werden und in welche Risikoklasse sie fallen. Ein EU AI Act Compliance Assessment liefert in 4–6 Tagen ein vollständiges KI-System-Register, die Risikoklassifizierung aller Systeme und einen priorisierten Maßnahmenplan – zum Festpreis.

EU AI Act Assessment (4–6 Tage, Festpreis): nexuscon.net/eu-ai-act-assessment

NIS2 + AI Act kombiniert: nexuscon.net/compliance

→ Jetzt Erstgespräch vereinbaren

Quellen & Referenzen

Die folgenden Quellen wurden für dieses Whitepaper herangezogen:

- Europäisches Parlament (2024): Verordnung (EU) 2024/1689 – EU AI Act, Amtsblatt der EU, 12. Juli 2024. → Quelle
- Europäische Kommission (2024): „AI Act – Regulatory Framework". → Quelle
- Europäisches Parlament (2022): Richtlinie (EU) 2022/2555 – NIS2-Richtlinie. → Quelle
- BSI (2025): „Künstliche Intelligenz sicher gestalten" – Leitfaden des BSI. → Quelle
- High-Level Expert Group on AI (2019): „Ethics Guidelines for Trustworthy AI", Europäische Kommission. → Quelle
- PwC (2024): „Responsible AI Survey 2024 – EU AI Act Readiness". → Quelle
- Gartner (2024): „Predicts 2025: AI Governance Will Become a Board-Level Priority". → Quelle
- OECD (2024): „OECD AI Policy Observatory – Regulatory Tracker". → Quelle
- DSGVO: Verordnung (EU) 2016/679 – Datenschutz-Grundverordnung. → Quelle
- ISO/IEC 42001:2023 – Artificial Intelligence Management System (AIMS). → Quelle

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

Über den Autor

Simon Schilling

Geschäftsführer & Principal Consultant

Nexus Management Consulting GmbH | Stuttgart

AWS Solutions Architect | PRINCE2 | Azure Architect | TOGAF 9 | ITIL v3

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

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

Über Nexus Management Consulting

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

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

Leistungsportfolio

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

Kontakt aufnehmen

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

Im Kaisemer 11 | 70191 Stuttgart | Nexus Management Consulting GmbH

→ Jetzt Erstgespräch buchen