PRAXISLEITFADEN 2025

EU AI Act Survival Guide

Der komplette Praxisleitfaden für Unternehmen: Compliance, Risikoklassen & Umsetzungsstrategien

Aktualisiert: Februar 2025

Umfang: Alle Pflichten, Fristen & Checklisten

PRINT-READY EDITION

Inhaltsverzeichnis

1. Einführung: Was ist der EU AI Act?

> *Der EU AI Act (Verordnung EU 2024/1689) ist das weltweit erste umfassende Regelwerk für Künstliche Intelligenz. Seit dem 1. August 2024 gilt er als verbindlicher Rechtsrahmen in der Europäischen Union und setzt neue Maßstäbe für den sicheren, transparenten und menschenzentrierten Einsatz von KI-Systemen.*

Die KI-Verordnung der Europäischen Union markiert einen Wendepunkt in der Regulierung künstlicher Intelligenz. Als weltweit erstes umfassendes Gesetz für KI schafft sie einen einheitlichen Rechtsrahmen, der Innovation fördert und gleichzeitig den Schutz von Gesundheit, Sicherheit und Grundrechten gewährleistet.

Das Gesetz folgt einem risikobasierten Ansatz: Je höher das potenzielle Risiko einer KI-Anwendung für Einzelpersonen und die Gesellschaft, desto strenger sind die Anforderungen an Anbieter und Betreiber. Dieser differenzierte Ansatz ermöglicht es Unternehmen, KI-Systeme verantwortungsvoll zu entwickeln und einzusetzen, ohne Innovationen unnötig zu behindern.

1.1 Ziele und Geltungsbereich

Der EU AI Act verfolgt mehrere zentrale Ziele, die den Rahmen für alle weiteren Regelungen bilden:

- **Sicherheit und Grundrechtsschutz:** Gewährleistung, dass KI-Systeme in der EU sicher sind und die Grundrechte der Bürger respektieren
- **Rechtssicherheit:** Schaffung eines klaren regulatorischen Rahmens für Unternehmen, die KI entwickeln oder nutzen
- **Wettbewerbsfähigkeit:** Stärkung der europäischen KI-Industrie durch vertrauenswürdige und hochwertige KI-Systeme
- **Harmonisierung:** Einheitliche Regeln für den gesamten EU-Binnenmarkt

> **Wichtig zu wissen**
>
> Die Verordnung gilt nicht nur für Unternehmen mit Sitz in der EU, sondern für alle Anbieter und Betreiber, deren KI-Systeme in der Europäischen Union eingesetzt werden. Auch Unternehmen aus den USA, China oder anderen Drittstaaten müssen die Vorschriften einhalten, wenn ihre KI-Produkte oder -Dienstleistungen auf dem EU-Markt angeboten werden.

1.2 Wer ist betroffen?

Der EU AI Act definiert verschiedene Rollen, die jeweils spezifische Pflichten haben. Die wichtigsten Akteure sind:

Rolle	Definition	Beispiele
Anbieter (Provider)	Entwickelt KI-Systeme oder lässt sie entwickeln, um sie unter eigenem Namen zu vertreiben	Softwarehersteller, KI-Startups, Tech-Unternehmen
Betreiber (Deployer)	Setzt KI-Systeme im eigenen Betrieb ein	Unternehmen, Behörden, Organisationen
Importeur	Bringt KI-Systeme aus Drittstaaten in die EU	Händler, Distributoren
Vertriebshändler	Bietet KI-Systeme im EU-Markt an, die nicht von ihm selbst entwickelt wurden	Reseller, Partner
Produkthersteller	Integriert KI-Systeme in Produkte unter eigenem Namen	Gerätehersteller, Automobilindustrie

Eine Person oder Organisation kann mehrere Rollen gleichzeitig einnehmen. Ein Unternehmen, das eine eigene KI-Software entwickelt und intern einsetzt, ist gleichzeitig Anbieter und Betreiber.

1.3 Zeitplan und Fristen

Der EU AI Act wurde am 1. August 2024 offiziell im Amtsblatt der EU veröffentlicht und ist seitdem in Kraft. Die Umsetzung erfolgt jedoch schrittweise, um Unternehmen ausreichend Zeit für die Anpassung zu geben:

1. Aug 2024

Inkrafttreten der Verordnung

Die KI-Verordnung wird offiziell EU-Recht. Unternehmen sollten mit der Vorbereitung beginnen.

2. Feb 2025

Verbotene Praktiken & AI Literacy

Verbot bestimmter KI-Praktiken mit unannehmbarem Risiko. Pflicht zur KI-Kompetenz (Art. 4) tritt in Kraft.

2. Aug 2025

GPAI-Modelle & Governance

Pflichten für General Purpose AI-Modelle. Einrichtung nationaler Aufsichtsbehörden.

2. Aug 2026

Hochrisiko-Systeme

Vollanwendung der Vorgaben für Hochrisiko-KI-Systeme. Konformitätsbewertungen müssen abgeschlossen sein.

2. Aug 2027

Bestehende GPAI-Modelle

Ende der Übergangsfrist für General Purpose AI-Modelle, die vor August 2025 in Verkehr gebracht wurden.

Achtung: Keine Schonfrist!

Die gesetzlichen Fristen sind bindend. Es wird keine Verzögerung oder Schonfrist geben. Unternehmen, die ihre Pflichten nicht rechtzeitig erfüllen, riskieren hohe Bußgelder und Marktausschluss.

Key Takeaways Kapitel 1

- Der EU AI Act gilt seit August 2024 für alle KI-Systeme im EU-Markt
- Auch Unternehmen außerhalb der EU müssen die Vorschriften beachten
- Die Umsetzung erfolgt schrittweise bis August 2027
- Ab Februar 2025 gelten erste konkrete Pflichten

2. Die vier Risikoklassen im Überblick

> *Das Herzstück des EU AI Act ist das risikobasierte Regulierungsmodell. KI-Systeme werden in vier Risikokategorien eingeteilt, die jeweils unterschiedliche Anforderungen an Anbieter und Betreiber stellen.*

Der risikobasierte Ansatz des EU AI Act ist das zentrale Instrument zur Differenzierung der regulatorischen Anforderungen. Nicht jede KI-Anwendung stellt das gleiche Risiko dar – ein Spam-Filter ist grundlegend anders zu bewerten als ein KI-System für die Kreditwürdigkeitsprüfung oder die medizinische Diagnostik.

Risikoklasse	Beschreibung	Anforderungen
UNANNEHMBAR	KI-Systeme, die eine klare Gefahr für Grundrechte und Sicherheit darstellen	**Verboten** – dürfen nicht entwickelt oder eingesetzt werden
HOCH	KI-Systeme in sensiblen Bereichen mit erheblichem Risikopotenzial	Strenge Pflichten: Risikomanagement, Dokumentation, Konformitätsbewertung, CE-Kennzeichnung
BEGRENZT	KI-Systeme mit geringem, aber vorhandenem Risiko	Transparenzpflichten: Nutzer müssen über KI-Einsatz informiert werden
MINIMAL	KI-Systeme mit vernachlässigbarem Risiko	Keine spezifischen Pflichten, freiwillige Codes beachten

2.1 Unannehmbares Risiko (Verboten)

KI-Systeme mit unannehmbarem Risiko sind nach Artikel 5 des EU AI Act verboten. Diese Systeme stellen eine unverhältnismäßige Gefahr für die Grundrechte, die Sicherheit oder die persönliche Autonomie von Menschen dar.

Zu den verbotenen Praktiken gehören:

- **Manipulative Systeme:** KI-Systeme, die subliminale Techniken oder Täuschungsmethoden einsetzen, um das Verhalten von Menschen zu manipulieren und ihnen oder anderen erheblichen Schaden zuzufügen
- **Ausnutzung von Schwächen:** Systeme, die die Schwächen bestimmter Personengruppen (Alter, Behinderung, soziale Situation) ausnutzen, um deren Verhalten zu manipulieren
- **Social Scoring:** Bewertung des Sozialverhaltens von Personen durch öffentliche Behörden, die zu ungerechtfertigter Benachteiligung führt
- **Echtzeit-Biometrie:** Biometrische Fernidentifikation in öffentlich zugänglichen Räumen durch Strafverfolgungsbehörden (mit engen Ausnahmen)
- **Emotionserkennung:** KI-Systeme zur Emotionserkennung am Arbeitsplatz oder in Bildungseinrichtungen (mit Ausnahmen)
- **Scraping von Gesichtsbildern:** Ungezieltes Erfassen von Gesichtsbildern aus dem Internet oder Überwachungskameras für Datenbanken

> **Verbotene Praktiken seit Februar 2025**
>
> Seit dem 2. Februar 2025 sind alle KI-Systeme mit unannehmbarem Risiko EU-weit verboten. Unternehmen, die solche Systeme entwickeln, vertreiben oder einsetzen, müssen diese umgehend stilllegen und können mit erheblichen Sanktionen rechnen.

2.2 Hochrisiko-KI-Systeme

Hochrisiko-KI-Systeme sind in kritischen Bereichen eingesetzte Anwendungen, die erhebliche Auswirkungen auf die Rechte, Sicherheit oder Chancen von Menschen haben können. Diese Systeme unterliegen den umfangreichsten Pflichten des EU AI Act.

Kriterien für Hochrisiko-Systeme:

Ein KI-System gilt als hochriskant, wenn es in einem der folgenden Bereiche eingesetzt wird und gleichzeitig ein erhebliches Risiko für die Gesundheit, Sicherheit oder Grundrechte von Personen darstellt:

- **Kritische Infrastruktur:** Management und Betrieb von Verkehrsinfrastruktur, Wasser-, Gas- und Stromversorgung
- **Bildung:** Bewertung von Lernenden, Zugang zu Bildungseinrichtungen

- **Beschäftigung:** Einstellung, Entlassung, Leistungsbewertung, Beförderung
- **Zugang zu essentiellen Dienstleistungen:** Kreditwürdigkeitsbewertung, Krankenversicherung, Sozialleistungen
- **Strafverfolgung:** Risikobewertung, Polygraphen, Beweisanalyse
- **Migration und Grenzkontrolle:** Asylanträge, Visa, Grenzkontrollen
- **Rechtsprechung:** Unterstützung bei gerichtlichen Entscheidungen

> **Beispiele für Hochrisiko-KI**
>
> - KI-gestützte Bewerbungsauswahl-Software
> - Systeme zur Kreditwürdigkeitsprüfung
> - Medizinische Diagnose-KI
> - Software für die Leistungsbewertung von Mitarbeitern
> - KI-Systeme für die Strafverfolgung

2.3 Begrenztes Risiko

KI-Systeme mit begrenztem Risiko unterliegen primär Transparenzpflichten. Nutzer müssen darüber informiert werden, dass sie mit einem KI-System interagieren oder dass Inhalte durch KI generiert wurden.

Zu dieser Kategorie gehören:

- **Chatbots:** Systeme, die mit Nutzern in menschenähnlicher Form interagieren
- **KI-generierte Inhalte:** Texte, Bilder, Videos oder Audio, die durch KI erstellt wurden
- **Deepfakes:** KI-manipulierte Inhalte, die real erscheinen
- **Emotionserkennung:** Systeme zur Erkennung von Emotionen (außerhalb von Arbeitsplatz und Bildung)
- **Biometrische Kategorisierung:** Einteilung von Personen in Kategorien basierend auf biometrischen Daten

2.4 Minimales Risiko

KI-Systeme mit minimalem Risiko sind weitgehend von der Regulierung ausgenommen. Dazu gehören Anwendungen, die kein oder nur ein verschwindend geringes Risiko für die Rechte oder Sicherheit von Personen darstellen.

Beispiele für minimales Risiko:

- Spam-Filter und Virenscanner
- KI-gestützte Videospiele
- Einfache Empfehlungssysteme (z.B. für Filme oder Musik)
- KI-gestützte Grammatik- und Rechtschreibprüfung
- Optische Zeichenerkennung (OCR)

Für diese Systeme gibt es keine spezifischen Pflichten im EU AI Act. Unternehmen werden jedoch ermutigt, freiwillige Codes of Conduct anzuwenden und ethische Grundsätze zu beachten.

Key Takeaways Kapitel 2

- Vier Risikoklassen: Unannehmbar (verboten), Hoch, Begrenzt, Minimal
- Verbotene Systeme dürfen seit Februar 2025 nicht mehr eingesetzt werden
- Hochrisiko-Systeme unterliegen den umfangreichsten Pflichten
- Transparenzpflichten gelten für Chatbots und KI-generierte Inhalte
- Systeme mit minimalem Risiko sind weitgehend unreguliert

3. Verbotene KI-Praktiken (Art. 5)

> *Artikel 5 des EU AI Act verbietet KI-Praktiken, die als unannehmbares Risiko eingestuft werden. Diese Verbote sind seit dem 2. Februar 2025 in Kraft und haben sofortige Konsequenzen für Unternehmen.*

Die verbotenen KI-Praktiken stellen eine klare rote Linie im EU AI Act dar. Sie basieren auf dem Grundsatz, dass bestimmte Anwendungen künstlicher Intelligenz mit den Grundwerten und Grundrechten der Europäischen Union unvereinbar sind – unabhängig von ihrem konkreten Einsatzzweck oder ihrer technischen Ausgestaltung.

3.1 Manipulative Systeme

KI-Systeme, die darauf ausgelegt sind, das Verhalten von Personen zu manipulieren, sind verboten. Dies gilt insbesondere für Systeme, die:

- **Subliminale Techniken einsetzen:** Botschaften oder Reize, die unterhalb der bewussten Wahrnehmungsschwelle liegen und das Verhalten beeinflussen, ohne dass die betroffene Person dies bemerkt
- **Täuschungsmethoden verwenden:** Techniken, die bewusst getäuschte oder irreführende Informationen einsetzen, um das Verhalten zu manipulieren
- **Erheblichen Schaden verursachen:** Die Manipulation muss zu physischem, psychologischem oder finanziellem Schaden führen können

> **Praxisbeispiel: Verbotene Manipulation**
>
> Ein Online-Spiel für Kinder, das subliminale visuelle Reize einsetzt, um die Spielzeit zu verlängern und In-App-Käufe zu fördern, wäre nach dem EU AI Act verboten. Ebenso verboten wäre eine KI-gestützte Werbeanwendung, die gezielt die Ängste von Verbrauchern ausnutzt, um Käufe zu erzwingen.

3.2 Social Scoring

Das Social Scoring durch öffentliche Behörden ist eines der umstrittensten Elemente im EU AI Act und wird vollständig verboten. Darunter fällt:

- **Bewertung des Sozialverhaltens:** Systematische Bewertung oder Klassifizierung des Verhaltens von Personen basierend auf sozialen Daten
- **Aggregation über verschiedene Kontexte:** Zusammenführung von Daten aus unterschiedlichen Lebensbereichen (z.B. Arbeit, Soziales, Online-Verhalten)
- **Ungerechtfertigte Benachteiligung:** Die Bewertung führt zu einer schlechteren Behandlung in Kontexten, die nicht mit dem ursprünglichen Kontext zusammenhängen

> **Ausnahme: Privates Social Scoring**
>
> Das Verbot gilt primär für öffentliche Behörden. Private Unternehmen dürfen unter bestimmten Bedingungen Scoring-Systeme betreiben (z.B. Kreditscoring), sofern diese nicht über verschiedene Kontexte aggregieren und keine ungerechtfertigte Benachteiligung bewirken.

3.3 Biometrische Echtzeitüberwachung

Die biometrische Fernidentifikation in öffentlich zugänglichen Räumen für Strafverfolgungszwecke ist grundsätzlich verboten. Dies betrifft:

- **Echtzeit-Gesichtserkennung:** Automatische Identifikation von Personen in Echtzeit durch Überwachungskameras
- **Biometrische Datenbanken:** Systeme, die biometrische Daten mit Datenbanken abgleichen, um Personen zu identifizieren
- **Öffentliche Räume:** Straßen, Plätze, öffentliche Gebäude, Verkehrsmittel

Eng begrenzte Ausnahmen:

In sehr spezifischen Fällen kann die biometrische Echtzeitüberwachung erlaubt sein, wenn:

- Die Suche nach einem konkreten Opfer von Entführung, Menschenhandel oder sexueller Ausbeutung betrifft

- Die unmittelbare Bedrohung des Lebens oder der körperlichen Unversehrtheit von Personen vorliegt
- Die Verhinderung eines konkreten, substanziellen und unmittelbaren Terroranschlags betroffen ist
- Die Strafverfolgung schwere Kriminalität (z.B. Mord, Terrorismus) betrifft

Bei jeder Ausnahme müssen zusätzliche Schutzmaßnahmen ergriffen werden, einschließlich vorheriger Genehmigung durch eine unabhängige Stelle und umfassender Dokumentation.

Prüfen Sie Ihre Systeme!

Überprüfen Sie sofort, ob eines Ihrer KI-Systeme unter die verbotenen Praktiken fällt. Bei Unsicherheit konsultieren Sie einen Rechtsexperten.

Key Takeaways Kapitel 3

- Manipulative Systeme mit subliminalen Techniken sind verboten
- Social Scoring durch öffentliche Behörden ist untersagt
- Biometrische Echtzeitüberwachung in öffentlichen Räumen ist grundsätzlich verboten
- Seit Februar 2025 müssen verbotene Systeme stillgelegt werden

4. Hochrisiko-KI: Pflichten im Detail

> *Hochrisiko-KI-Systeme unterliegen den umfangreichsten Anforderungen des EU AI Act. Dieses Kapitel erklärt detailliert, welche Pflichten Anbieter und Betreiber erfüllen müssen.*

Die Pflichten für Hochrisiko-KI-Systeme sind umfassend und durchdacht. Sie decken den gesamten Lebenszyklus eines KI-Systems ab – von der Konzeption über die Entwicklung bis hin zum Betrieb und der Überwachung. Das Ziel ist es, sicherzustellen, dass Hochrisiko-Systeme sicher, transparent und unter menschlicher Kontrolle bleiben.

4.1 Risikomanagementsystem

Jeder Anbieter eines Hochrisiko-KI-Systems muss ein Risikomanagementsystem einrichten, dokumentieren und pflegen. Dieses System muss:

- **Gesamtlebenszyklus abdecken:** Risiken müssen während der gesamten Lebensdauer des Systems identifiziert, analysiert und minimiert werden
- **Iterativ sein:** Das Risikomanagement ist ein kontinuierlicher Prozess, der regelmäßig überprüft und aktualisiert wird
- **Restrisiken dokumentieren:** Verbleibende Risiken müssen transparent kommuniziert werden
- **Tests umfassen:** Das System muss vor der Markteinführung umfassend getestet werden

Elemente eines Risikomanagementsystems

- Risikoidentifikation und -analyse
- Risikobewertung und -priorisierung
- Risikominimierungsmaßnahmen
- Test- und Validierungsprotokolle
- Post-Market-Monitoring
- Incident-Response-Plan

4.2 Datenqualität und Governance

Die Qualität der Trainings-, Validierungs- und Testdaten ist entscheidend für die Sicherheit und Fairness von KI-Systemen. Der EU AI Act stellt strenge Anforderungen an die Datenqualität:

- **Rechtskonformität:** Daten müssen in Übereinstimmung mit dem EU-Recht erhoben und verarbeitet werden (DSGVO beachten)
- **Angemessene Datenpraktiken:** Daten müssen angemessen für den beabsichtigten Zweck sein
- **Frei von Fehlern:** Daten müssen so weit wie möglich fehlerfrei und vollständig sein
- **Repräsentativität:** Trainingsdaten müssen die Zielpopulation angemessen repräsentieren
- **Diskriminierungsfreiheit:** Daten dürfen keine versteckten Verzerrungen enthalten, die zu Diskriminierung führen

Dokumentationsanforderungen für Daten:

Aspekt	Dokumentationspflicht
Datenquellen	Herkunft aller Trainings-, Validierungs- und Testdaten
Datenmerkmale	Größe, Zusammensetzung, Hauptmerkmale der Datensätze
Datenaufbereitung	Verwendete Verarbeitungsschritte und -techniken

Datenlabeling	Methodik, Verfahren und Qualitätssicherung
Verzerrungen	Bekannte Verzerrungen und Gegenmaßnahmen

4.3 Technische Dokumentation

Die technische Dokumentation ist ein zentrales Element der Hochrisiko-KI-Compliance. Sie muss alle relevanten Informationen über das KI-System enthalten und wird bei der Konformitätsbewertung geprüft.

Pflichtinhalte der technischen Dokumentation:

- **Allgemeine Beschreibung:** Zweck, beabsichtigte Nutzer, Interaktion mit anderen Systemen
- **Systemarchitektur:** Technische Spezifikationen, Algorithmen, Parameter
- **Entwicklungsprozess:** Design-Entscheidungen, Design-Choice-Rationale
- **Leistungskennzahlen:** Genauigkeit, Robustheit, Fairness-Metriken
- **Bekannte Einschränkungen:** Grenzen des Systems, Fehlerquellen
- **Risikomanagement:** Identifizierte Risiken und Gegenmaßnahmen
- **Änderungsprotokoll:** Versionierung und Änderungshistorie

> **Best Practice: Dokumentationsmanagement**
>
> Empfehlen Sie ein zentrales Dokumentenmanagement-System für alle KI-relevanten Unterlagen. Dies erleichtert nicht nur die Compliance, sondern auch die Zusammenarbeit zwischen Entwicklungs-, Compliance- und Geschäftsteams.

4.4 Menschliche Aufsicht

Der EU AI Act verlangt, dass Hochrisiko-KI-Systeme unter angemessener menschlicher Aufsicht betrieben werden. Diese Aufsicht muss:

- **Von qualifizierten Personen wahrgenommen werden:** Die Aufsichtspersonen müssen über ausreichende Fachkenntnisse, Ausbildung und Erfahrung verfügen
- **Wirksam sein:** Die Aufsicht muss tatsächlich in der Lage sein, Fehler oder Risiken zu erkennen und zu korrigieren

- **Rechtzeitig erfolgen:** Die Aufsicht muss rechtzeitig eingreifen können, bevor Schaden entsteht
- **Dokumentiert werden:** Aufsichtsprozesse und -entscheidungen müssen protokolliert werden

Aufgaben der menschlichen Aufsicht:

- Überwachung der Systemleistung und -entscheidungen
- Erkennung und Korrektur von Fehlern oder Verzerrungen
- Entscheidung über die Deaktivierung des Systems bei Risiken
- Schulung und Unterstützung der Endnutzer

Key Takeaways Kapitel 4

- Risikomanagementsystem über den gesamten Lebenszyklus erforderlich
- Hohe Anforderungen an Datenqualität und -dokumentation
- Umfassende technische Dokumentation ist Pflicht
- Menschliche Aufsicht durch qualifizierte Personen notwendig
- CE-Kennzeichnung nach erfolgreicher Konformitätsbewertung

5. General Purpose AI (GPAI) Modelle

> *General Purpose AI (GPAI) Modelle wie GPT-4, Claude oder Gemini unterliegen spezifischen Regelungen. Dieses Kapitel erklärt die Pflichten für Anbieter dieser leistungsstarken KI-Modelle.*

General Purpose AI Modelle haben die KI-Landschaft revolutioniert. Diese Modelle können eine Vielzahl unterschiedlicher Aufgaben erfüllen und bilden die Grundlage für zahlreiche Anwendungen. Der EU AI Act erkennt die besondere Bedeutung und das besondere Risiko dieser Modelle an und stellt spezifische Anforderungen an ihre Anbieter.

5.1 Definition und Abgrenzung

Ein GPAI-Modell ist ein KI-Modell, das:

- **Allgemeine Verwendbarkeit:** Eine breite Palette von Aufgaben erfüllen kann
- **Integration:** In verschiedene downstream-Anwendungen integriert werden kann
- **Vielseitigkeit:** Nicht für einen spezifischen Zweck entwickelt wurde

Beispiele für GPAI-Modelle:

- Große Sprachmodelle (LLMs) wie GPT-4, Claude, Gemini, Llama
- Multimodale Modelle, die Text, Bild und Audio verarbeiten können
- Generative Modelle für Bilder, Video oder Audio

> **Unterscheidung: Modell vs. System**
>
> Wichtig ist die Unterscheidung zwischen einem GPAI-Modell (der zugrunde liegenden KI) und einem GPAI-System (der konkreten Anwendung). Der EU AI Act regelt primär die Modelle, während Systeme je nach Einsatzzweck zusätzlichen Regelungen unterliegen können.

5.2 Pflichten für GPAI-Anbieter

Seit dem 2. August 2025 gelten für Anbieter von GPAI-Modellen spezifische Pflichten. Diese umfassen:

1. Technische Dokumentation:

- Detaillierte Beschreibung des Modells (Architektur, Parameter, Trainingsmethoden)
- Informationen über Trainingsdaten (Quellen, Größe, Zusammensetzung)
- Rechenressourcen und Energieverbrauch
- Bekannte Einschränkungen und Risiken

2. Transparenzberichte:

- Regelmäßige Veröffentlichung von Transparenzberichten
- Inhalte müssen für die AI Office zugänglich sein
- Informationen über Sicherheitsbewertungen und Red-Teaming

3. Urheberrecht:

- Respektierung von Urheberrechten bei Trainingsdaten
- Umsetzung von Opt-out-Mechanismen (z.B. robots.txt)
- Dokumentation der eingesetzten Maßnahmen

4. Information für Downstream-Anbieter:

- Bereitstellung von Modellkarten und Dokumentation
- Klare Angabe von Fähigkeiten und Grenzen
- Integrationshinweise und Best Practices

5.3 Systemische Risiken

GPAI-Modelle mit systemischem Risiko unterliegen zusätzlichen, verschärften Pflichten. Ein Modell gilt als systemisch, wenn:

- Es eine hohe Rechenleistung für das Training erfordert (Schwellenwert: >10^25 FLOP)
- Es von der EU-Kommission aufgrund anderer Kriterien als systemisch eingestuft wird

Zusätzliche Pflichten für systemische Risiken:

- **Modellbewertung:** Regelmäßige Bewertung und Dokumentation systemischer Risiken
- **Risikominderung:** Umsetzung angemessener Maßnahmen zur Risikominderung
- **Sicherheitsvorfälle:** Meldung schwerwiegender Vorfälle an die AI Office
- **Interne Tests:** Durchführung von Sicherheitstests und Red-Teaming
- **Verhaltenskodex:** Einhaltung des von der EU erstellten Verhaltenskodex

> **Systemische Risiken: Beispiele**
>
> Systemische Risiken können umfassen: Verbreitung von Desinformation, Unterstützung bei Cyberangriffen, Entwicklung gefährlicher Substanzen, massenhafte Verletzung von Privatsphäre, Diskriminierung auf großer Skala.

Key Takeaways Kapitel 5

- GPAI-Modelle unterliegen spezifischen Transparenzpflichten
- Technische Dokumentation und Transparenzberichte sind Pflicht
- Urheberrechte müssen bei Trainingsdaten beachtet werden
- Systemische Risiken erfordern verschärfte Maßnahmen
- Der EU-Verhaltenskodex bietet konkrete Orientierung

6. AI Literacy: Schulungspflicht (Art. 4)

> *Artikel 4 des EU AI Act führt eine der wichtigsten und am häufigsten übersehenen Pflichten ein: die Förderung von KI-Kompetenz (AI Literacy). Seit Februar 2025 müssen alle Mitarbeitenden, die mit KI arbeiten, über ausreichende Kenntnisse verfügen.*

Die KI-Kompetenzpflicht ist ein Paradigmenwechsel in der KI-Regulierung. Sie erkennt an, dass technische Systeme nur so gut sind wie die Menschen, die sie entwickeln, betreiben und überwachen. Ohne ausreichendes Verständnis für KI können Mitarbeitende Risiken nicht erkennen, Fehler nicht korrigieren und das Potenzial der Technologie nicht ausschöpfen.

6.1 Was bedeutet KI-Kompetenz?

Der EU AI Act definiert KI-Kompetenz als die Fähigkeit von Anbietern und Betreibern sowie deren betroffenen Mitarbeitenden,:

- **KI-Systeme zu verstehen:** Grundlegendes Verständnis der Funktionsweise, Möglichkeiten und Grenzen von KI
- **Risiken einzuschätzen:** Fähigkeit, potenzielle Risiken und negative Auswirkungen von KI zu erkennen
- **KI verantwortungsvoll einzusetzen:** Kenntnis ethischer Grundsätze und rechtlicher Anforderungen
- **Angemessen zu interagieren:** Fähigkeit, effektiv mit KI-Systemen zu arbeiten und diese zu überwachen

Elemente der KI-Kompetenz:

Kompetenzbereich	Inhalte	Zielgruppe
Technisches Verständnis	Funktionsweise von KI, Algorithmen, maschinelles Lernen, Grenzen der Technologie	Entwickler, Data Scientists

Rechtliche Grundlagen	EU AI Act, DSGVO, Haftungsfragen, regulatorische Anforderungen	Compliance, Management
Ethische Aspekte	Fairness, Transparenz, Verantwortung, Diskriminierungsvermeidung	Alle Mitarbeitende
Risikomanagement	Risikoerkennung, Incident-Response, menschliche Aufsicht	Betreiber, Aufseher
Praktische Anwendung	Umgang mit konkreten KI-Systemen, Fehlererkennung, Korrekturmaßnahmen	Endnutzer

> **Anpassung an die Rolle**
>
> Die erforderliche KI-Kompetenz hängt vom jeweiligen Aufgabenbereich ab. Ein KI-Entwickler benötigt tiefgehendes technisches Wissen, während ein Endnutzer vor allem verstehen muss, wie er das System korrekt bedient und Fehler erkennt.

6.2 Umsetzung im Unternehmen

Unternehmen müssen sicherstellen, dass ihre Mitarbeitenden über die erforderliche KI-Kompetenz verfügen. Die praktische Umsetzung obliegt dem jeweiligen Unternehmen – es gibt keine vorgeschriebene Form der Schulung.

Mögliche Umsetzungsformen:

- **Interne Schulungen:** Eigene Trainingsprogramme, Workshops, E-Learning-Kurse
- **Externe Kurse:** Zertifizierte Weiterbildungen, Seminare, Online-Kurse
- **On-the-Job-Training:** Praktische Einweisung und Begleitung bei der Arbeit mit KI
- **Dokumentation:** Handbücher, Richtlinien, Best-Practice-Guides
- **Regelmäßige Updates:** Fortlaufende Weiterbildung bei neuen Entwicklungen

Best Practice: Schulungskonzept

Entwickeln Sie ein strukturiertes Schulungskonzept mit verschiedenen Ebenen: Basiswissen für alle Mitarbeitenden, vertieftes Wissen für KI-Nutzer, spezialisiertes Wissen für Entwickler und Betreiber. Dokumentieren Sie alle Schulungen nachweislich.

Dokumentationsanforderungen:

Obwohl keine formale Zertifizierung vorgeschrieben ist, sollten Unternehmen folgende Dokumentation führen:

- Teilnehmerlisten und Anwesenheitsnachweise für Schulungen
- Inhalte und Lernziele der Schulungen
- Qualifikationsnachweise der Trainer
- Regelmäßige Aktualisierung der Schulungsinhalte
- Nachweis der Teilnahme für jeden Mitarbeitenden

Jetzt handeln!

Prüfen Sie sofort den KI-Kompetenzstand Ihrer Mitarbeitenden. Entwickeln Sie ein Schulungskonzept und dokumentieren Sie alle Maßnahmen.

Key Takeaways Kapitel 6

- Seit Februar 2025 gilt die Pflicht zur KI-Kompetenz
- Alle Mitarbeitenden mit KI-Kontakt müssen geschult werden
- Schulungen müssen an die jeweilige Rolle angepasst sein
- Dokumentation der Schulungen ist essentiell
- Keine formale Zertifizierung, aber Nachweispflicht

7. Transparenzpflichten

> *Transparenz ist ein Grundpfeiler des EU AI Act. Nutzer müssen wissen, wenn sie mit KI interagieren oder wenn Inhalte durch KI generiert wurden. Dieses Kapitel erklärt die konkreten Anforderungen.*

Transparenz schafft Vertrauen und ermöglicht informierte Entscheidungen. Wenn Nutzer wissen, dass sie mit einem KI-System interagieren, können sie die Informationen angemessen einordnen und bei Bedarf Vorsichtsmaßnahmen ergreifen. Der EU AI Act verankert diese Erkenntnis in verbindlichen Pflichten.

7.1 Chatbots und KI-Interaktion

Wenn Nutzer mit einem KI-System interagieren, das in menschenähnlicher Form kommuniziert (z.B. Chatbots, virtuelle Assistenten), müssen sie darüber informiert werden, dass es sich um eine KI handelt.

Konkrete Anforderungen:

- **Klare Kennzeichnung:** Die Information muss klar und verständlich sein
- **Zu Beginn der Interaktion:** Die Information sollte am Anfang der Kommunikation erfolgen
- **Keine Täuschung:** Das Design darf nicht vorspiegeln, dass ein Mensch antwortet

> **Praxisbeispiel: Chatbot-Kennzeichnung**
>
> Ein Kundenservice-Chatbot sollte zu Beginn der Konversation mitteilen: "Hallo! Ich bin ein KI-gestützter Assistent. Wie kann ich Ihnen helfen?" oder ähnlich eindeutig kennzeichnen, dass keine menschliche Interaktion stattfindet.

7.2 KI-generierte Inhalte

KI-generierte oder KI-manipulierte Inhalte müssen als solche gekennzeichnet werden. Dies gilt für:

- Texte, die durch KI erstellt wurden
- Bilder, die durch KI generiert oder verändert wurden
- Audio- und Videoinhalte mit KI-Beteiligung

Anforderungen an die Kennzeichnung:

- **Offensichtlich:** Die Kennzeichnung muss für den durchschnittlichen Nutzer erkennbar sein
- **Dauerhaft:** Die Information sollte nicht leicht entfernt werden können
- **Verständlich:** Klare Formulierung wie "KI-generiert" oder "Durch KI erstellt"

7.3 Deepfakes

Deepfakes – KI-manipulierte Inhalte, die authentisch wirken – unterliegen besonders strengen Kennzeichnungspflichten. Dies gilt für:

- Videos mit veränderten Gesichtern oder Stimmen
- Audioaufnahmen, die KI-generiert oder verändert wurden
- Bilder, die Personen in neuen Kontexten zeigen

> **Besondere Vorsicht bei Deepfakes**
>
> Deepfakes bergen besondere Risiken für Desinformation und Identitätsdiebstahl. Die Kennzeichnungspflicht ist daher besonders streng. Bei Nichtkennzeichnung können erhebliche rechtliche Konsequenzen drohen.

Ausnahmen:

In bestimmten Fällen können die Transparenzpflichten eingeschränkt oder ausgesetzt werden:

- **Künstlerische oder satirische Inhalte:** Wenn der künstlerische, kreative oder satirische Charakter offensichtlich ist
- **Strafverfolgung:** In bestimmten Fällen zur Verhinderung oder Aufklärung von Straftaten
- **Öffentliche Sicherheit:** Bei Gefahren für Leib und Leben

Key Takeaways Kapitel 7

- Chatbots müssen als KI-Systeme gekennzeichnet werden
- KI-generierte Inhalte erfordern deutliche Kennzeichnung
- Deepfakes unterliegen besonders strengen Pflichten
- Die Kennzeichnung muss klar, verständlich und dauerhaft sein
- Bestimmte Ausnahmen für künstlerische und sicherheitsrelevante Inhalte

8. Sanktionen und Bußgelder

> *Der EU AI Act sieht erhebliche Sanktionen für Verstöße vor. Das Verständnis der möglichen Konsequenzen ist entscheidend für die Einordnung der Compliance-Bedürftigkeit.*

Die Sanktionsregelungen des EU AI Act gehören zu den strengsten im globalen Vergleich. Sie spiegeln die Bedeutung wider, die die EU dem verantwortungsvollen Einsatz von KI beimisst. Für Unternehmen bedeutet dies: Compliance ist nicht optional, sondern existenziell.

8.1 Höhe der Strafen

Der EU AI Act sieht ein gestaffeltes Bußgeldsystem vor, das sich nach der Schwere des Verstoßes richtet:

Verstoß	Bußgeld
Verbotene KI-Praktiken (Art. 5)	Bis zu 35 Millionen EUR oder 7% des weltweiten Jahresumsatzes (je nachdem, was höher ist)
Pflichten für Hochrisiko-KI	Bis zu 15 Millionen EUR oder 3% des weltweiten Jahresumsatzes
Pflichten für GPAI-Modelle	Bis zu 15 Millionen EUR oder 3% des weltweiten Jahresumsatzes
Falsche Angaben / Nichtkooperation	Bis zu 7,5 Millionen EUR oder 1,5% des weltweiten Jahresumsatzes

> **Beispielrechnung**
>
> Ein Unternehmen mit einem weltweiten Jahresumsatz von 1 Milliarde EUR, das gegen das Verbot manipulativer KI-Systeme verstößt, könnte mit einer Strafe von bis zu 70 Millionen EUR rechnen (7% von 1 Mrd.).

Weitere Sanktionsmöglichkeiten:

- **Marktverbot:** Das KI-System darf nicht mehr vertrieben oder betrieben werden
- **Rückruf:** Bereits im Umlauf befindliche Systeme müssen zurückgerufen werden
- **Korrekturauflagen:** Verpflichtung zur Behebung der Mängel
- **Öffentliche Nennung:** Veröffentlichung des Verstoßes

8.2 Durchsetzung und Kontrolle

Die Überwachung und Durchsetzung des EU AI Act erfolgt auf mehreren Ebenen:

Nationale Ebene:

- Jeder EU-Mitgliedstaat muss eine nationale Marktüberwachungsbehörde benennen
- In Deutschland wird dies die Bundesnetzagentur (BNetzA) sein
- Diese Behörden führen Inspektionen durch und verhängen Sanktionen

Europäische Ebene:

- Das AI Office der EU-Kommission überwacht GPAI-Modelle
- Die European Artificial Intelligence Board koordiniert die Zusammenarbeit
- Bei grenzüberschreitenden Verstößen kann die EU-Kommission direkt eingreifen

> **KI-Service-Desk der BNetzA**
>
> Die Bundesnetzagentur hat einen KI-Service-Desk eingerichtet, der Unternehmen – insbesondere KMU – bei Fragen zum EU AI Act unterstützt. Nutzen Sie dieses kostenlose Angebot für erste Orientierung.

Kontrollmechanismen:

- **Dokumentationsprüfung:** Aufforderung zur Vorlage technischer Unterlagen
- **Systemtests:** Überprüfung der Funktionsweise von KI-Systemen
- **Betriebsinspektionen:** Vor-Ort-Kontrollen bei Unternehmen
- **Meldewesen:** Pflicht zur Meldung von Sicherheitsvorfällen

Key Takeaways Kapitel 8

- Verbotene Praktiken: bis zu 35 Mio. EUR oder 7% Umsatz
- Hochrisiko-Verstöße: bis zu 15 Mio. EUR oder 3% Umsatz
- Marktverbote und Rückrufe sind möglich
- Nationale Behörden (BNetzA) und EU AI Office überwachen die Einhaltung
- Der KI-Service-Desk der BNetzA bietet Unterstützung

9. Compliance-Checkliste

> *Diese Checkliste führt Sie Schritt für Schritt durch die wichtigsten Maßnahmen zur EU AI Act-Compliance. Verwenden Sie sie als praktisches Werkzeug für die Umsetzung in Ihrem Unternehmen.*

Eine strukturierte Herangehensweise ist der Schlüssel zur erfolgreichen Compliance. Die folgende Checkliste deckt alle wesentlichen Bereiche ab und hilft Ihnen, den Überblick zu behalten.

9.1 Schritt-für-Schritt-Anleitung

Phase 1: Inventarisierung und Klassifizierung

- [ ] Alle KI-Systeme im Unternehmen identifizieren und dokumentieren
- [ ] Für jedes System die Risikoklasse bestimmen (unannehmbar, hoch, begrenzt, minimal)
- [ ] Verbotene Systeme sofort stilllegen und dokumentieren
- [ ] Hochrisiko-Systeme priorisieren und detailliert analysieren
- [ ] Eigene Rolle klären: Anbieter, Betreiber, Importeur oder Vertriebshändler

Phase 2: Hochrisiko-Systeme (falls zutreffend)

- [ ] Risikomanagementsystem gemäß Art. 9 einrichten
- [ ] Datenqualität und -governance sicherstellen (Art. 10)
- [ ] Technische Dokumentation erstellen (Art. 11)
- [ ] Protokollierungsfunktion implementieren (Art. 12)
- [ ] Transparenzinformationen für Betreiber bereitstellen (Art. 13)
- [ ] Menschliche Aufsicht konzipieren und einrichten (Art. 14)
- [ ] Genauigkeit, Robustheit und Cybersicherheit gewährleisten (Art. 15)
- [ ] Qualitätsmanagementsystem implementieren (Art. 17)

- [ ] Konformitätsbewertung durchführen (Art. 43)
- [ ] CE-Kennzeichnung anbringen (Art. 48)
- [ ] EU-Konformitätserklärung erstellen (Art. 47)

Phase 3: GPAI-Modelle (falls zutreffend)

- [ ] Technische Dokumentation erstellen und aktualisieren
- [ ] Transparenzberichte für das AI Office erstellen
- [ ] Urheberrechtsmaßnahmen implementieren
- [ ] Informationen für Downstream-Anbieter bereitstellen
- [ ] Bei systemischem Risiko: Zusatzpflichten erfüllen

Phase 4: Transparenzpflichten

- [ ] Chatbots und KI-Interaktionen kennzeichnen
- [ ] KI-generierte Inhalte als solche markieren
- [ ] Deepfakes entsprechend kennzeichnen
- [ ] Kennzeichnungskonzept dokumentieren

Phase 5: AI Literacy

- [ ] Bedarfsermittlung für KI-Schulungen durchführen
- [ ] Schulungskonzept entwickeln
- [ ] Schulungen durchführen und dokumentieren
- [ ] Regelmäßige Aktualisierung planen

9.2 Dokumentationsanforderungen

Eine lückenlose Dokumentation ist essentiell für die Compliance. Folgende Dokumente müssen Sie führen:

Dokument	Inhalt	Aufbewahrung

KI-Inventar	Liste aller KI-Systeme, Risikoklassen, Verantwortliche	Permanent aktualisiert
Technische Dokumentation	Systembeschreibung, Architektur, Daten, Tests	10 Jahre nach Markteinführung
Risikomanagement-Doku	Risikoanalysen, Gegenmaßnahmen, Reviews	10 Jahre
Konformitätserklärung	EU-Konformitätserklärung für Hochrisiko-Systeme	10 Jahre
Schulungsnachweise	Teilnehmerlisten, Inhalte, Qualifikationen	5 Jahre
Protokolle	Betriebsprotokolle, Vorfälle, Korrekturmaßnahmen	6 Monate (mindestens)

Tipp: Dokumentenmanagement

Verwenden Sie ein zentrales Dokumentenmanagement-System mit Versionskontrolle und Zugriffsrechten. Stellen Sie sicher, dass alle relevanten Dokumente bei Bedarf schnell verfügbar sind.

Download: Compliance-Checkliste

Erstellen Sie eine individuelle Checkliste für Ihr Unternehmen. Passen Sie die Punkte an Ihre spezifischen KI-Systeme und Rollen an.

Key Takeaways Kapitel 9

- Systematische Inventarisierung aller KI-Systeme
- Korrekte Risikoklassifizierung ist entscheidend
- Hochrisiko-Systeme erfordern umfassende Maßnahmen
- Lückenlose Dokumentation über den gesamten Lebenszyklus
- Regelmäßige Reviews und Aktualisierungen planen

10. Praxis-Tipps und nächste Schritte

> *Der EU AI Act stellt Unternehmen vor große Herausforderungen, bietet aber auch Chancen. Dieses abschließende Kapitel gibt praktische Tipps für die erfolgreiche Umsetzung.*

Die Umsetzung des EU AI Act ist kein einmaliges Projekt, sondern ein kontinuierlicher Prozess. Unternehmen, die Compliance frühzeitig und strategisch angehen, können nicht nur Risiken minimieren, sondern auch Wettbewerbsvorteile erzielen.

10.1 Sofortmaßnahmen

Wenn Sie mit der Umsetzung beginnen, sollten Sie folgende Schritte priorisieren:

Woche 1-2

KI-Inventar erstellen

Identifizieren Sie alle KI-Systeme in Ihrem Unternehmen. Dokumentieren Sie Zweck, Anbieter, Einsatzbereich und verantwortliche Personen.

Woche 3-4

Risikoklassifizierung

Ordnen Sie jedes System einer Risikoklasse zu. Prüfen Sie, ob verbotene Systeme vorhanden sind und stillgelegt werden müssen.

Woche 5-8

Priorisierung und Planung

Priorisieren Sie Hochrisiko-Systeme. Erstellen Sie einen Umsetzungsplan mit Zeitplan, Verantwortlichen und Budget.

Woche 9-12

Erste Maßnahmen umsetzen

Beginnen Sie mit den dringendsten Maßnahmen: AI Literacy, Transparenzpflichten, Dokumentation.

10.2 Langfristige Strategie

Über die ersten Maßnahmen hinaus sollten Sie eine langfristige KI-Governance-Strategie entwickeln:

- **KI-Governance-Rahmen:** Definieren Sie Rollen, Verantwortlichkeiten und Entscheidungsprozesse für KI im Unternehmen
- **Ethik-Richtlinien:** Entwickeln Sie unternehmensspezifische ethische Grundsätze für den KI-Einsatz
- **Cross-funktionales Team:** Bilden Sie ein Team aus Recht, IT, Compliance und Fachbereichen
- **Regulatorisches Monitoring:** Beobachten Sie neue Entwicklungen und Anpassungen des EU AI Act
- **Stakeholder-Kommunikation:** Kommunizieren Sie Ihre KI-Strategie transparent nach innen und außen

10.3 Wichtige Ressourcen

Nutzen Sie die verfügbaren Ressourcen für die Umsetzung:

- **KI-Service-Desk der BNetzA:** Kostenlose Beratung für Unternehmen, insbesondere KMU
- **AI Office der EU-Kommission:** Leitlinien, FAQs und Unterstützung bei GPAI-Modellen
- **EU AI Act Service Desk:** Zukünftige zentrale Anlaufstelle der EU-Kommission
- **Branchenverbände:** Viele Branchenverbände bieten spezifische Leitfäden an
- **Rechtsexperten:** Bei komplexen Fragen sollten Sie spezialisierte Berater konsultieren

> **ISO 42001: KI-Managementsystem**
>
> Die ISO/IEC 42001 bietet einen Rahmen für KI-Managementsysteme. Sie ist freiwillig, kann aber als Orientierung für die Implementierung dienen und das Vertrauen von Kunden und Partnern stärken.

10.4 Chancen nutzen

Der EU AI Act ist nicht nur eine regulatorische Herausforderung, sondern bietet auch Chancen:

- **Vertrauen aufbauen:** Compliance schafft Vertrauen bei Kunden, Partnern und der Öffentlichkeit
- **Wettbewerbsvorteil:** Frühe Umsetzung kann Sie gegenüber zögerlichen Wettbewerbern positionieren
- **Qualitätssteigerung:** Die Anforderungen führen zu besseren, sichereren KI-Systemen
- **Marktzugang:** Compliance ist Voraussetzung für den Zugang zum EU-Markt
- **Innovation fördern:** Klare Regeln schaffen Planungssicherheit für KI-Investitionen

> **Erfolgsfaktor: Kultureller Wandel**
>
> Die erfolgreichsten Unternehmen werden die KI-Compliance nicht als lästige Pflicht, sondern als Chance für verantwortungsvollen und nachhaltigen KI-Einsatz verstehen. Ein Kulturwandel hin zu "Responsible AI" ist der Schlüssel zum langfristigen Erfolg.

Starten Sie jetzt!

Der EU AI Act ist Realität. Je früher Sie mit der Umsetzung beginnen, desto besser sind Sie aufgestellt. Nutzen Sie diesen Guide als Ausgangspunkt und passen Sie die Maßnahmen an Ihre spezifische Situation an.

Key Takeaways Kapitel 10

- Beginnen Sie sofort mit dem KI-Inventar und der Risikoklassifizierung
- Entwickeln Sie eine langfristige KI-Governance-Strategie
- Nutzen Sie verfügbare Ressourcen wie den KI-Service-Desk
- Verstehen Sie Compliance als Chance, nicht als Last
- Fördern Sie eine Kultur der verantwortungsvollen KI-Nutzung

Fazit

Der EU AI Act ist das umfassendste KI-Regelwerk weltweit und stellt Unternehmen vor erhebliche Herausforderungen. Gleichzeitig schafft er einen klaren Rahmen für den verantwortungsvollen Einsatz von Künstlicher Intelligenz.

Die erfolgreiche Umsetzung erfordert:

- Ein umfassendes Verständnis der eigenen KI-Systeme und deren Risikoklassifizierung
- Eine strukturierte Herangehensweise mit klaren Prioritäten und Zeitplänen
- Lückenlose Dokumentation über den gesamten Lebenszyklus
- Kontinuierliche Überwachung und Anpassung an neue Entwicklungen
- Ein unternehmensweites Commitment für verantwortungsvolle KI

Mit diesem Survival Guide haben Sie ein umfassendes Werkzeug an der Hand, um die Herausforderungen des EU AI Act zu meistern. Die Investition in Compliance zahlt sich aus – durch rechtliche Sicherheit, gesteigertes Vertrauen und nachhaltigen Wettbewerbsvorteil.

> *"Der EU AI Act ist nicht das Ende der KI-Innovation, sondern der Beginn einer verantwortungsvollen Ära der Künstlichen Intelligenz in Europa."*

EU AI Act Survival Guide

Version 1.0 | Februar 2025

Dieses eBook dient als Orientierungshilfe und ersetzt keine rechtliche Beratung.