

HANDOUT – ABSCHNITT 1–3

EU KI-Verordnung / AI Act

Grundlagen · Risikoklassen · Hochrisiko-KI · Module 1–11

ABSCHNITT 1

Grundlagen & Rechtlicher Rahmen

Module 1–4 | Einführung in den EU AI Act

01 Anwendbarkeit & Gesetzeslage

Einführung

Kurzname:	KI-Verordnung (KIVO) oder EU AI Act
In Kraft:	1. August 2024 – stufenweise bis 2. August 2027
Ansatz:	Risikobasiert: Je höher das Risiko, desto strenger die Anforderungen
Ziel:	Innovation fördern UND Grundrechte schützen
Struktur:	113 Artikel + 13 Anhänge + Erwägungsgründe
Adressaten:	KI-Hersteller (OpenAI, Anthropic, Meta), Importeure, Händler, Nutzer

□ Zeitplan der Anwendbarkeit

Feb 2025: Verbotene Praktiken + KI-Kompetenz-Pflicht | Aug 2026: Hochrisiko-Pflichten | Aug 2027: Alle weiteren Regelungen

⇒ Übung / Reflexion

Was wäre Ihrer Meinung nach ein Beispiel für eine KI, die Ihr Unternehmen einsetzt oder einsetzen könnte? Notieren Sie das Beispiel und überlegen Sie: Welche Risikoklasse könnte es haben?

02 Ethische Grundsätze

7 Prinzipien

Die 7 ethischen Grundsätze des AI Act (Erwägungsgrund 27)

- Menschliches Handeln und menschliche Aufsicht
- Technische Robustheit und Sicherheit
- Privatsphäre und Datengovernance
- Transparenz (KI-Interaktionen erkennbar machen)
- Vielfalt, Nichtdiskriminierung und Fairness
- Soziales und ökologisches Wohlergehen
- Rechenschaftspflicht

□ Praxis-Hinweis

Diese 7 Grundsätze sind rechtlich nicht bindend – sie dienen als Orientierung. Der AI Act selbst ist bindend. Unternehmen können jedoch mit Bezug auf diese Grundsätze Verhaltenskodizes und interne Richtlinien entwickeln.

03

Anwendungsbereich & AusnahmenWer ist
betroffen?

Gilt für:	Unternehmen & Behörden mit EU-Sitz, KI-Anbieter für den EU-Markt, Anbieter mit EU-wirksamen Outputs
Ausnahmen:	Nationale Sicherheit, Militär, Forschung, private Nutzung (Haushaltsausnahme), bestimmte Open-Source-Systeme
Räumlicher Geltungsbereich:	Sehr weit – gilt auch für Anbieter außerhalb der EU, wenn ihre KI in Europa eingesetzt wird
Bestandsschutz:	Hochrisiko-Systeme vor dem 2.8.2026 in Betrieb: dürfen weiter laufen, wenn nicht wesentlich verändert

04

KI-System vs. KI-Modell

Begriffe

KI-System (Art. 3 Nr. 1):	Maschinengestütztes System · autonomer Betrieb · verarbeitet Eingaben → erzeugt Ausgaben (Vorhersagen, Entscheidungen)
KI-Modell (GPAI):	Grundlage für KI-Systeme · nicht zweckgebunden · Beispiele: GPT, Claude, Gemini, LLaMA
Unterschied:	KI-Modell = Rohstoff / Grundlage · KI-System = das konkrete Produkt, das der AI Act reguliert
Relevanz:	Für KI-Modelle gelten eigene Pflichten (Kapitel V) · Risikoklassen betreffen KI-Systeme

ABSCHNITT 2**Akteure & Risikoklassen**

Module 5–7 | Wer hat welche Pflichten?

05 Akteur:innen in der KI-Wertschöpfungskette

Rollen

Anbieter (Hersteller):	Entwickeln und vermarkten KI-Systeme unter eigenem Namen – z. B. OpenAI, SAP, KI-Startups
Betreiber (Nutzer):	Verwenden KI-Systeme beruflich in eigener Verantwortung – Unternehmen, Behörden, NGOs
Einführer (Importeure):	Bringen KI-Systeme aus Drittländern in der EU in Verkehr – tragen Mitverantwortung
Händler:	Vertreiben KI-Systeme im EU-Binnenmarkt – müssen Konformität der Vorlieferanten prüfen
Wichtig:	Weder Organisationsform noch Umsatz entscheiden – auch Vereine und NGOs können betroffen sein

➡ Übung / Reflexion

Welche Rolle(n) nehmen Sie oder Ihr Unternehmen im AI-Act-Sinne ein? Anbieter, Betreiber oder beides? Begründen Sie kurz.

06 Die 4 Risikoklassen

Überblick

Klasse	Beschreibung	Beispiele & Pflichten
☐ Unannehmbares Risiko	VERBOTEN seit 2. Feb. 2025	Social Scoring, Predictive Policing, biometrische Echtzeitüberwachung
☐ Hohes Risiko	Erlaubt – streng reguliert · Ab Aug 2026	Personalentscheidungen, Bildungszugang, Medizinprodukte
☐ Begrenztes Risiko	Transparenzpflichten (Art. 50)	KI-Chatbots müssen sich als KI zu erkennen geben
☐ Minimales Risiko	Kaum reguliert	Spamfilter, KI-Computerspiele, einfache Empfehlungssysteme

07 Verbotene KI-Praktiken (Artikel 5)

Seit 2. Feb. 2025

Diese KI-Praktiken sind seit dem 2. Februar 2025 verboten:

- Unterschwellige Beeinflussung (manipulativ, außerhalb des Bewusstseins)
- Ausnutzung von Schwäche oder Schutzbedürftigkeit von Personen
- Social Scoring: Schlechterstellung durch Bewertung sozialen Verhaltens
- Predictive Policing: Risikobeurteilung zur Vorhersage von Straftaten
- Datenbanken zur Gesichtserkennung durch unbefugtes Scraping
- Emotionserkennung in Büro, Schule und ähnlichen Bereichen

- Biometrische Kategorisierung nach Weltanschauung, Religion, politischer Meinung
- Biometrische Echtzeit-Fernidentifizierung in öffentlichen Räumen (Strafverfolgung)

⚠ **Wichtiger Hinweis**

Die Liste enthält Ausnahmen und Gegenausnahmen – z. B. ist Gesichtserkennung zur Suche nach Entführungsoptionen unter bestimmten Bedingungen erlaubt. Detailprüfung im Einzelfall notwendig!

⇒ **Übung / Reflexion**

Prüfen Sie: Setzt Ihr Unternehmen oder Ihre Behörde aktuell Systeme ein, die unter eine der verbotenen Praktiken fallen könnten? Wenn ja, welche Schritte sind nötig?

ABSCHNITT 3**Hochrisiko-KI**

Module 8–11 | Anforderungen, Anbieter- und Betreiberpflichten

08 Wann ist ein KI-System Hochrisiko?

Artikel 6

Weg 1 – Integrierte Produkte:	KI in regulierten Produkten: Spielzeuge, Aufzüge, Medizinprodukte, Kfz, Luftfahrt, persönliche Schutzausrüstung
Weg 2 – Anwendungszweck:	Biometrie, kritische Infrastruktur, Bildung, Personalentscheidungen, Sozialleistungen, Strafverfolgung
Stichtag:	Ab 2. August 2026 greifen die meisten Hochrisiko-Pflichten
Ausnahmen:	Detailprüfung im Einzelfall erforderlich – Gesetz enthält zahlreiche Ausnahmen

09 Anforderungen an Hochrisiko-KI

Artikel 9–15

Hochrisiko-KI-Systeme müssen folgende Anforderungen erfüllen:

- Stand der Technik einhalten
- Risikomanagement-System betreiben
- Hohe Datenqualität gewährleisten
- Technische Dokumentation anfertigen (Anhang IV)
- Protokoll- und Aufzeichnungspflichten erfüllen
- Pflichtinformationen bereitstellen (Artikel 13)
- Menschliche Aufsicht sicherstellen
- Genauigkeit, Robustheit und Cybersicherheit gewährleisten

10 Pflichten der Anbieter:innen

10 Pflichten

Anbieter von Hochrisiko-KI-Systemen müssen:

- Handelsname + Kontaktadresse anbringen
- Qualitätsmanagementsystem betreiben
- Dokumentation erstellen und aufbewahren
- Protokolle aufbewahren
- Konformitätsbewertungsverfahren durchlaufen
- CE-Kennzeichnung anbringen
- In EU-Datenbank für Hochrisiko-KI registrieren
- Pflichtinformationen bereitstellen
- Barrierefreiheitsanforderungen erfüllen
- Mit Behörden zusammenarbeiten (ggf. EU-Bevollmächtigten benennen)

11 Pflichten der Betreiber:innen

Artikel 26

Betreiber von Hochrisiko-KI-Systemen müssen:

- Technische und organisatorische Maßnahmen umsetzen (laut Betriebsanleitung verwenden)
- Menschliche Aufsicht an kompetente Personen übertragen

- Eingabedaten: dem Verwendungszweck entsprechend und repräsentativ
- Betrieb des KI-Systems überwachen
- Schwerwiegende Vorfälle melden (Tod, schwere Verletzung, Grundrechtsverletzung → Aufsichtsbehörde)
- Datenschutz-Folgenabschätzung durchführen (bei personenbezogenen Daten)
- Betroffene über den KI-Einsatz informieren

⇒ Übung / Reflexion

Übung: Sie betreiben ein KI-System zur Unterstützung von Personalentscheidungen. Welche der oben genannten Pflichten treffen Sie als Betreiber? Erstellen Sie eine kurze Checkliste.

Mustafa Cinar – KI-Trainer & Berater

ki.mustici.de | kontakt@mustici.de