


# KI-VERORDNUNG RECHTSKONFORM UMSETZEN



KI | Rechtssicher eingesetzt.  
Risiken | Souverän gemanagt.  
Lösungen | Mandantenorientiert entwickelt.

## KI nach der KI-VO ist viel mehr als nur KI!

Die KI-VO ist eine EU-Verordnung, die harmonisierte Vorschriften für die Entwicklung und den Einsatz von künstlicher Intelligenz (KI) festlegt. Sie beschreibt die Rahmenbedingungen für die Entwicklung und den Einsatz, definiert verbotene Praktiken und enthält zahlreiche, insbes. produktsicherheitsrechtliche Vorgaben für KI-Modelle und KI-Systeme sowie deren Anbieter und Betreiber.

Viele, die es bisher gar nicht vermuten, fallen **ab dem 02. August 2027** unter die KI-VO.



## Betroffene Unternehmen

### Hochrisiko-KI; Generativer KI

**Nicht jede KI wird reguliert, sondern im Wesentlichen nur „Hochrisiko-KI-Systeme“.** Nur wenige allgemeine Pflichten hat der Gesetzgeber für generative KI normiert. Nicht jede KI ist ein Hochrisiko-KI-System. Aber zum Beispiel KI im HR-Bereich, Sicherheitssoftware oder Steuerungssoftware für kritische Infrastrukturen, die KI nutzt, werden in Zukunft als Hochrisiko-KI-Systeme erfasst.

**Produktsicherheitsrecht: Verpflichtung für Hersteller, Einführer und Händler**

Die KI-VO unterfällt dem Produktsicherheitsrecht, das eine CE-Kennzeichnung für Hochrisiko-KI-Systeme verlangt.

Hersteller treffen die meisten Pflichten. **Ein klassischer GPT-Wrapper oder jeder Nutzer eines White-Label-KI-Products gilt als Hersteller in diesem Sinne!** Firmen, die KI-Systeme aus Drittstaaten in die EU importieren oder innerhalb der EU vertreiben, sind verpflichtet, die Einhaltung der Anforderungen der KI-VO sicherzustellen.

### Unternehmensgröße

Die KI-VO gilt unabhängig von der Größe und des Umsatzes! Sie gilt also auch für kleine und mittlere Unternehmen wie Start-ups, sofern sie KI-Systeme entwickeln, vertreiben oder nutzen.

### Geografische Reichweite

Die Verordnung betrifft alle Unternehmen, deren KI-Systeme in der EU eingesetzt werden oder deren Ergebnisse Personen in der EU beeinflussen, selbst wenn das Unternehmen seinen Sitz außerhalb der EU hat.

### Ausnahmen

Nicht betroffen sind Unternehmen, die nicht in einem regulierten Sektor tätig sind, sowie Einrichtungen, welche die Schwellenwerte nicht überschreiten.

## Sanktionen

Bei Verstößen gegen die KI-Verordnung drohen erhebliche Sanktionen. Für verbotene KI-Praktiken können Bußgelder bis zu EUR 35 Mio. oder 7 % des weltweiten Jahresumsatzes verhängt werden. **Pflichtverletzungen bei Hochrisiko-KI-Systemen werden mit bis zu EUR 15 Mio. oder 3 % des Umsatzes geahndet. Falsche oder irreführende Angaben können Bußgelder bis zu EUR 7,5 Mio. oder 1 % des Umsatzes nach sich ziehen.** Zusätzlich sind nationale Maßnahmen wie Verwarnungen, Anordnungen zur Beseitigung von Verstößen oder sogar Marktverbote möglich. Die Höhe der Geldbußen richtet sich nach Art, Schwere und Dauer des Verstoßes.

## Fristen

**2. Februar 2025:** Verbot bestimmter KI-Praktiken (z.B. Social Scoring), Umsetzung der KI-Kompetenz bei Geschäftsleitung und Mitarbeitern (insb. Schulungen).

**2. August 2025:** Pflichten für Anbieter von KI-Modellen mit allgemeinem Verwendungszweck (GPAI), Bei nationaler Behörden, erste Governance-Regeln.

**2. August 2027:** Die meisten weiteren Vorschriften, insbesondere für Hochrisiko-KI-Systeme werden anwendbar.



## Neue Pflichten (Auszug)

### Allgemein

- KI-Kompetenz herstellen und nachweisen Schulung der Mitarbeiter

### KI mit beschränktem Risiko (z.B. KI-generierte Inhalte)

- Transparenzpflicht - betroffene Person Interaktion informieren
- Deepfakes explizit markieren
- Emotionserkennungs-/ Biometriesysteme offenlegen
- Bei Texten zur Information der Öffentlichkeit KI- Erzeugung transparent machen

### Hochrisiko-KI-Systeme (z.B. Personal, Bildung, Sicherheits-software für kritische Infrastruktur)

- Risikomanagementsystem einrichten (Anbieter)
- Konformitätsbewertungsverfahren
- Menschliche Aufsicht ermöglichen/ Aufsicht sicherstellen
- Zweckgemäße Verwendung gemäß Gebrauchsanweisung
- Kontinuierliche Überwachung und Risikobewertung
- Umfassende Dokumentation/ Protokollierung
- Bei Problemen System aussetzen und Anbieter informieren
- Meldung schwerwiegender Vorfälle an die Aufsichtsbehörde
- Grundrechtfolgenabschätzung

---

## Unsere Beratung zur NIS-2-Compliance

### Initialanalyse und Bestandsaufnahme

- Prüfung, ob und wie KI-Systeme im Unternehmen vom AI Act betroffen sind.
- Identifikation von Compliance-Lücken und Handlungsbedarf.
- GAP-Analyse

### Vertragsgestaltung und Haftungsmanagement

- Prüfung und Anpassung von Verträgen mit
- KI-Anbietern und Geschäftspartnern.
- Beratung zu Haftungsfragen

### Entwicklung von Governance-Strukturen

- Gestaltung und Implementierung von internen Richtlinien (insb. KI-Richtlinie), Kontrollmechanismen und Verantwortlichkeiten

### Risikobewertung und Klassifizierung

- Unterstützung bei der Einstufung der eingesetzten KI-Systeme nach Risikoklassen.
- Beratung zur Durchführung und Dokumentation von Risikoanalysen (etwa Grundrechts-Folgenabschätzungen und Datenschutz-Folgenabschätzungen).

### Datenschutz und Transparenz

- Sicherstellung der Einhaltung datenschutzrechtlicher Vorgaben bei KI-Anwendungen.
- Beratung zu Transparenzpflichten.

### Schulungen und Sensibilisierung

- Durchführung von Workshops und Training der der Geschäftsleitung und Mitarbeiter zu rechtlichen Anforderungen (KI-Kompetenz-Schulung)

Vertrauen Sie auf unsere Expertise –  
als starker Partner für rechtssichere  
und praxisnahe Lösungen rund um das  
Thema Informationssicherheit

Berlin  
Chemnitz  
Düsseldorf  
Frankfurt  
Hamburg  
Köln  
München  
Stuttgart

