AI ACT

Walk-Through

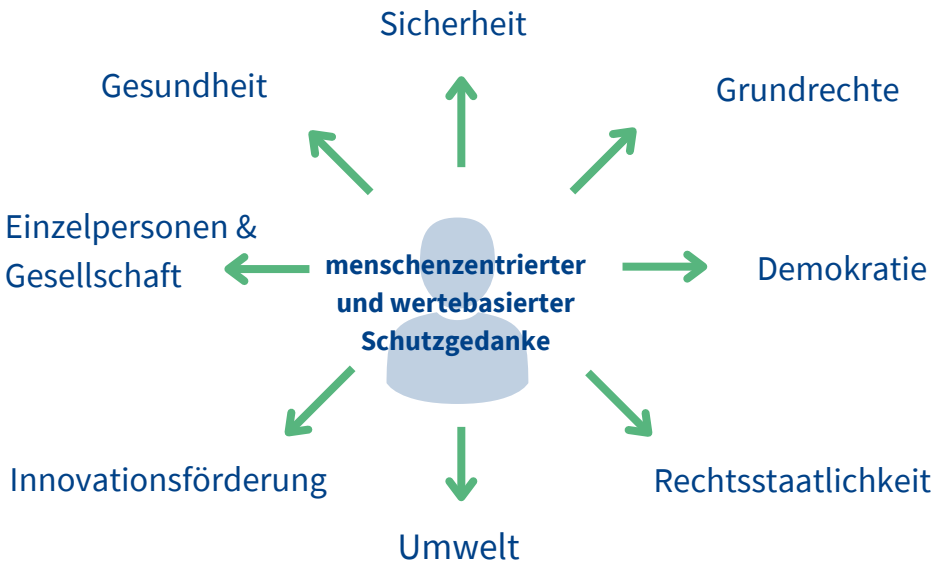
DORDA

| Digital Industries Group |

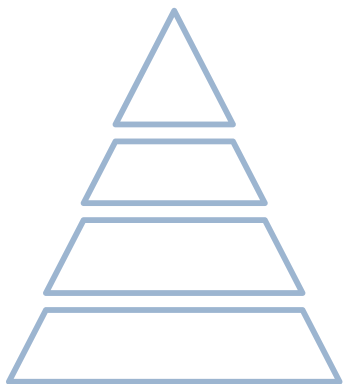
Überblick

Ziele

Der AI Act schafft erstmals einen rechtlichen Rahmen für einen sicheren, vertrauenswürdigen Einsatz von KI-Systemen in der EU. Gleichzeitig soll Innovation gefördert werden.



- Verbotene KI-Systeme
- Hochrisiko-KI-Systeme
- GPAI
- Bestimmte KI-Systeme



Herzstück des AI Act: Der risikobasierte Ansatz

Der AI Act qualifiziert das Risikopotential einer KI anhand eines Klassifizierungssystems. Abhängig von der entsprechenden Einordnung knüpfen besondere Pflichten an die Nutzung eines KI-Systems.

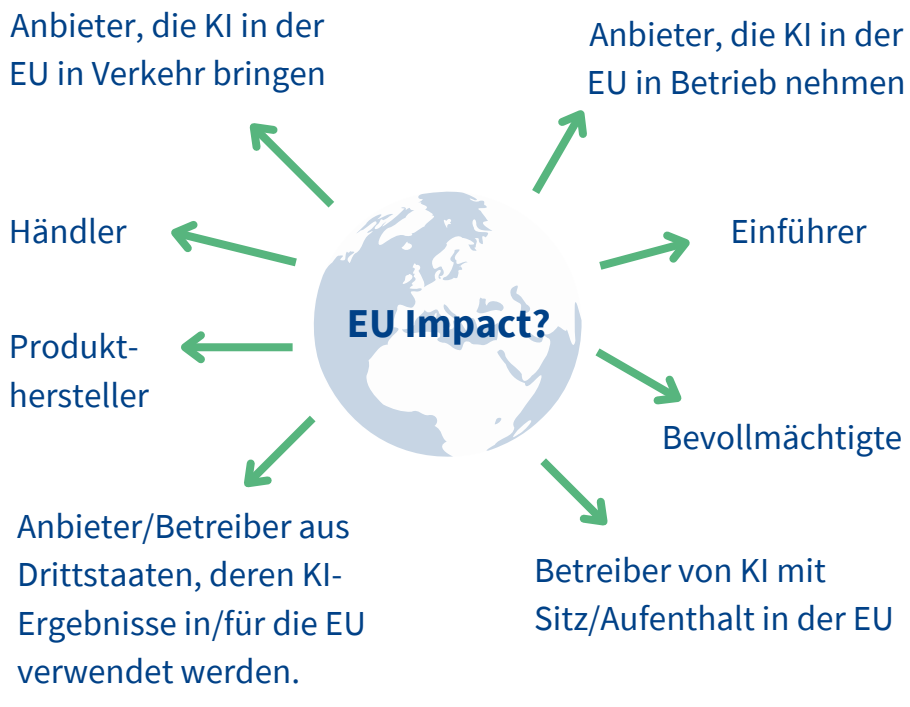
Good News!
Alle KI-Systeme, die nicht unter eine dieser Risikoklassen fallen, sind nach dem AI Act ohne weitere Auflagen erlaubt. Für diese sind lediglich die Bestimmungen zur **AI-Literacy** zu beachten. So haben zukünftig alle Anbieter und Betreiber von KI-Systemen Maßnahmen zu ergreifen, um notwendigen Kenntnisse zur **sachkundigen Verwendung von KI-Systemen** zu vermitteln.

Verpflichtete

Der AI Act nimmt unterschiedliche Akteure in die Pflicht:

- **Anbieter**
- **Betreiber**
- **Einführer und Händler**
- **Produkthersteller**
- **Bevollmächtigte von Anbietern**

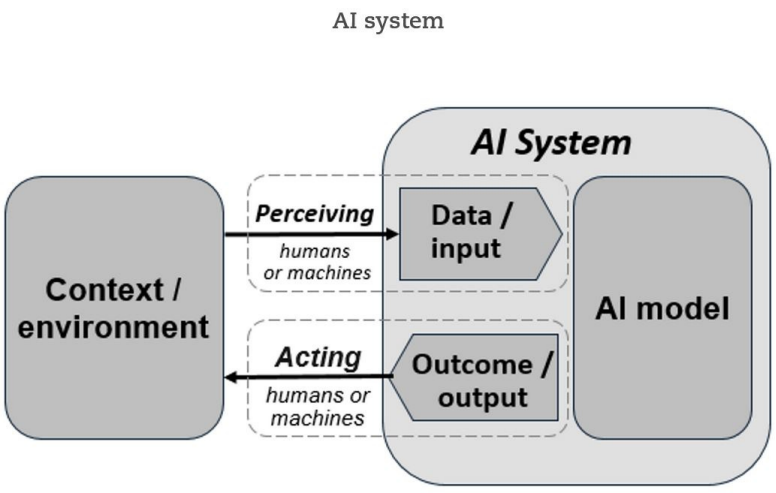
Ein Sitz im Drittstaat entbindet die Akteure nicht von ihren Pflichten, wenn die KI für die EU bestimmt ist.



How-To AI Act-Compliance?

Step 1: Ist mein System als KI iSd AI Act zu qualifizieren?

Parallelen zur OECD-Definition



https://oecd.ai/en/ai-principles

KI-Definition

"KI-System" bezeichnet ein **maschinengestütztes System**, das

- für einen in **wechselndem Maße autonomen Betrieb** ausgelegt ist,
- nach seiner Einführung **anpassungsfähig sein kann**,
- aus den erhaltenen Eingaben für explizite oder implizite Ziele **ableitet, wie Ergebnisse die physische oder virtuelle Umgebung beeinflussen können.**

Ergebnisse können zB Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen sein.

→ **Erhöht die internationale Konvergenz und Akzeptanz**

Definition von GPAI

"**KI-Modell** mit **allgemeinem Verwendungszweck**" bezeichnet ein Modell, das

- eine erhebliche allgemeine Verwendbarkeit aufweist,
- in der Lage ist, unabhängig von der Art und Weise seines Inverkehrbringens ein breites Spektrum unterschiedlicher Aufgaben kompetent zu erfüllen, und
- in eine Vielzahl nachgelagerter Systeme oder Anwendungen integriert werden kann.

Abgrenzung zu herkömmlicher Software

Typische Merkmale einer KI:

- Fähigkeit zur Ableitung aus Eingaben oder Daten
- Nutzung von Techniken, wie maschinellem Lernen, logik- und wissensgestützten Konzepten
- Systeme mit verschiedenen Graden an Autonomie

Keine KI:

- Software, die auf ausschließlich von natürlichen Personen definierten Regeln für das automatische Ausführen von Operationen beruht

Beispiele

KI-Systeme können zB in folgenden Anwendungen integriert sein (im Einzelfall zu prüfen):

- Spam Filter
- Chatbots, Voicebots
- Tools zur automatisierten Auswertung von Bewerbungen, Bearbeitung von Kundenanfragen, Anträgen, Abwicklung von Verträgen etc
- Roboter-unterstützte Geräte, wie etwa in der Medizin
- Bonitätsscoring-Systeme
- Sensorik-unterstützte Systeme, wie etwa im Straßenverkehr

Praxistipp

Im Rahmen einer Bestandsaufnahme ist zu prüfen, ob KI-Systeme iSd AI Act bereits eingesetzt werden.
Die AI Act-Anforderungen sind außerdem bei neuen Use Cases immer mitzubedenken.

Step 2: Fällt die Nutzung in den Anwendungsbereich des AI Act?

Ausnahmen vom Anwendungsbereich

Beispiele

- Nutzung ausschließlich zu **militärischen Zwecken**
- Nutzung zu **Verteidigungszwecken** oder zu Zwecken der **nationalen Sicherheit**
- Entwicklung und Inbetriebnahme ausschließlich zur **wissenschaftlichen Forschung und Entwicklung**
- **Test- und Entwicklungstätigkeiten** zu KI-Systemen, bevor diese in Verkehr gebracht oder in Betrieb genommen werden, sofern die Tests nicht unter realen Bedingungen erfolgen
- Nutzung durch natürliche Person zu **ausschließlich persönlichen und nicht beruflichen Zwecken**
- Bereitstellung von KI-Systemen unter **freien und quelloffenen Lizenzen**, ausgenommen bestimmte, Hochrisiko- und verbotene KI-Systeme

Praxistipp

Die Ausnahmebestimmungen sind eng auszulegen. Ob die Voraussetzungen erfüllt sind, ist daher im Einzelfall zu prüfen. Für die Privatwirtschaft sind die Ausnahmen für Open Source Software und Test-/Entwicklungstätigkeiten am relevantesten.

Step 3: In welcher Rolle nutze ich KI?

Eine Sache der gesamten Lieferkette

Die Verhaltenspflichten und Verbote des AI Act richten sich in erster Linie an den **Anbieter von KI-Lösungen**. Das ist, wer KI-Systeme **entwickelt oder entwickeln** lässt und sie unter eigenen Namen **in Verkehr bringt** oder **in Betrieb nimmt**. Um keine Rechtsschutzlücke zu öffnen, können **auch andere Marktteilnehmer dieselben Pflichten** treffen. Für die gesamte Lieferkette - **vom Hersteller bis zum Endnutzer** - ist daher das Regelungswerk des AI Act relevant.

Anbieter

Hersteller und Vertreiber unter eigenem Namen

Einführer

Importeur mit Niederlassung in der EU, der die KI aus einem Drittland in die EU einführt

Händler

Anbieter auf dem Unionsmarkt

Betreiber

Verwendung in eigener Verantwortung

Praxistipp

Auch abseits des klassischen Anbieters können Tätigkeiten vom AI Act erfasst sein. Daher sollte die Anwendbarkeit des AI Act in jeder Rolle geprüft werden.

Step 4: In welche Risikoklasse fällt das KI-System und welche Pflichten müssen erfüllt werden?

Verbotene KI-Systeme

Darunter fallen zB folgende KI-Systeme:

- KI-Systeme, die Techniken der unterschwelligen Beeinflussung außerhalb des Bewusstseins einer Person oder absichtlich manipulative oder täuschende Techniken einsetzen, um das Verhalten einer Person/Gruppe wesentlich zu beeinflussen und die Entscheidungsfindung derart beeinträchtigen , dass ein erheblicher Schaden zugefügt wird/werden kann
- Social-Scoring von Personen
- Biometrische Echtzeitidentifizierung in öffentlich zugänglichen Räumen außerhalb der engen Ausnahmen

Verbotene KI-Systeme dürfen in der EU **weder in Verkehr gebracht noch betrieben** werden.

Ausnahmen bestehen nur in einem engen Bereich, insb für die **Strafverfolgung**. Unter bestimmten Voraussetzung ist die Verwendung von biometrischer Echtzeitidentifizierung erlaubt.

Widerlegung durch Risikoabwägung teilweise möglich

Der Hochrisiko-Charakter der in Anhang III zum AI Act aufgelisteten Anwendungen kann widerlegt werden, wenn das KI-System **kein erhebliches Risiko der Beeinträchtigung in Bezug auf die Gesundheit, Sicherheit oder Grundrechte** natürlicher Personen birgt, indem es unter anderem nicht das Ergebnis der Entscheidungsfindung wesentlich beeinflusst. Diese Risikoabwägung ist nach den im AI Act festgelegten Kriterien vorzunehmen.

Pflichten

Hochrisiko KI-Systeme dürfen nur unter Einhaltung besonderer Auflagen in der EU in Verkehr gebracht und verwendet werden, wie zB

- **Einrichtung und Aufrechterhaltung eines Risikomanagementsystems, insb Durchführung einer AI Risiko-Abschätzung**
- **Grundrechte-Folgenabschätzung für Anhang III-Anwendungen**
- **Einhaltung von Datenqualitätsanforderungen**
- **Technische Dokumentationspflichten**
- **Aufzeichnungspflichten**
- **Transparenzpflichten**
- **Menschliche Aufsicht**
- **Gewährleistung von Genauigkeit, Robustheit und Cybersicherheit**

Daneben müssen Anbieter insb auch eine **EU-Konformitätserklärung** ausstellen und eine **CE-Kennzeichnung** anbringen. Details sind in Abschnitt 2 ff des AI Act und seinen Anhängen geregelt.

Hochrisiko KI-Systeme

Dazu zählen KI-Systeme, die

- als Sicherheitskomponente genutzt werden und unter die in **Anhang I zum AI Act** aufgelisteten Vorschriften fallen (zB RL zur Sicherheit von Spielzeugen oder Aufzügen) oder selbst ein solches Produkt sind,
- in **Anhang III zum AI Act** aufgelistet sind, insb iZm biometrischen Anwendungen, kritischen Infrastrukturen, allgemeiner und beruflicher Bildung, Beschäftigung, Personalmanagement, Inanspruchnahme grundlegender privater und öffentlicher Dienste/Leistungen (insb KI-Systeme für die Kreditwürdigkeitsprüfung, die über die Aufdeckung von Finanzbetrug hinausgehen), Strafverfolgung, Migration, Asyl, Grenzkontrolle, Rechtspflege und demokratischen Prozessen.

Details sind dem Anhang I und III zu entnehmen.

Praxistipp

Der Fokus der Compliance-Prüfung sollte auf Hochrisiko-Klassifizierungen liegen. An diese Einordnung knüpfen nämlich die meisten Pflichten an.

GPAI

GPAI zeichnet sich dadurch aus, dass diese Modelle aufgrund ihrer **Leistungsfähigkeit und ihres Umfangs** für **unterschiedliche Zwecke** herangezogen werden können. Der Entwickler legt somit nicht die tatsächliche Endnutzung fest.

Bei einer Rechenleistung von mehr als **10^25 FLOPS** handelt es sich dabei grundsätzlich um ein **Modell mit systemischem Risiko**.

Pflichten

Alle Anbieter von GPAI müssen die Systementwicklung und **Trainingsinhalte** ausreichend dokumentieren und auch entsprechende **Informationen für nachgelagerte Anbieter** bereitstellen. Dazu zählen zB:

- Information über Funktionen und Grenzen des GPAI-Modells
- Umsetzung einer Strategie zur Einhaltung der urheberrechtlichen Bestimmungen in der EU
- Zusammenfassungen über die, für das Training verwendeten Inhalte

Anbieter von GPAI mit **systemischen Risiken** müssen darüber hinaus weitere Anforderungen umsetzen, wie zB die Durchführung einer **Modellbewertung** auf mögliche Risiken, Einhaltung von **Meldepflichten** und Gewährleistung von **Cybersicherheitsmaßnahmen**.

Pflichten

Bestimmte KI-Systeme können ein besonderes Risiko eines Identitätsbetrugs oder einer Täuschung in sich bergen. Daher unterliegen sie vorwiegend **Transparenzvorschriften**.

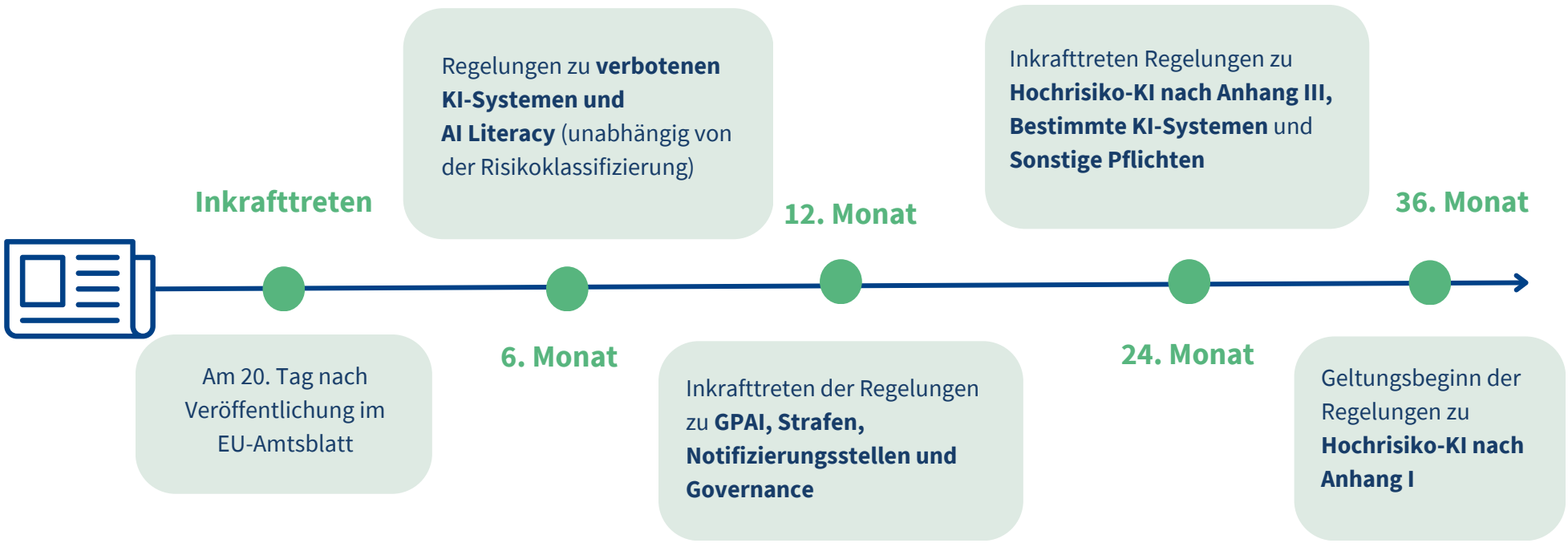
Anbieter haben sicherzustellen, dass **synthetische Inhalte** auch als solche erkennbar sind und ein Nutzer über die **Interaktion mit einer Maschine** aufgeklärt wird. Auch den Betreiber trifft eine Aufklärungspflicht, wenn es sich bei den generierten Inhalten um "**Deepfakes**" handelt.

Bestimmte KI-Systeme

Dazu zählen zB KI-Systeme, die zur direkten Interaktion mit natürlichen Personen verwendet werden (klassische Chatbots) oder die synthetische Audio-, Bild-, Video- oder Textinhalte erzeugen. Dabei sind regelmäßig auch GPAI-Modelle integriert.

Step 5: Fristgerechte Umsetzung

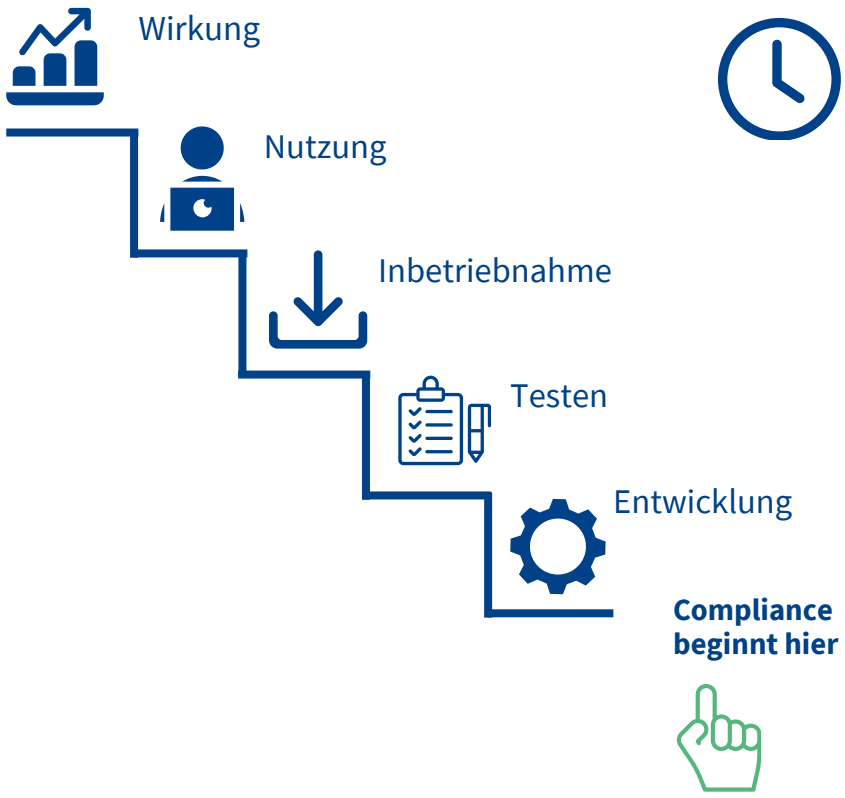
Wichtige Compliance Fristen



Für bereits auf dem Markt befindliche bzw in Betrieb genommene KI-Systeme gelten zT abweichende Bestimmungen.

Die **Regelungen des AI Act** werden **schrittweise** nach Inkrafttreten der Verordnung **anwendbar**.

Um eine rechtssichere Verwendung von aktuellen oder in Entwicklung befindlichen KI-Systemen zu gewährleisten, sind **bereits jetzt entsprechende Compliance-Maßnahmen ratsam.** Andernfalls besteht das Risiko, dass die fehlende Vorarbeit eine **fristgerechte Erfüllung** der notwendigen Pflichten verhindert. Die Folgen können empfindliche **Geldbußen** sein.



Geldstrafen

Verstoß gegen Bestimmungen zu **verbotenen KI-Systemen**	bis zu **EUR 35 Mio** oder **7%** des Jahresumsatzes
Verstoß gegen Bestimmungen zu **Hochrisiko KI-Systemen**, **Bestimmungen zu GPAI** und **Transparenzpflichten für bestimmte KI-Systeme**	bis zu **EUR 15 Mio** oder **3%** des Jahresumsatzes
Falschaussagen bei zuständiger Behörde im KI-Verfahren	bis zu **EUR 7,5 Mio** oder **1%** des Jahresumsatzes

Das **Strafmaß** ist nach oben durch den Pauschalsatz oder den Prozentwert begrenzt - je nachdem welcher **Betrag höher** ist.

Für **KMUs und Start-Ups** gilt eine **Sonderregelung**. Hier wird für das Höchstmaß der Strafen der jeweils **niedrigere Betrag** herangezogen.

Innovationspartner digitaler Champions.

Axel Anderl
Managing Partner
Head of IT/IP/Datenschutz
Head of Digital Industries Group

axel.anderl@dorda.at

Alexandra Ciarnau
Co-Head of Digital Industries Group
Rechtsanwältin IT/IP/Datenschutz
Head of Metaverse
Board Member of Women in AI Austria

alexandra.ciarnau@dorda.at

Benjamin Kraudinger
Rechtsanwaltsanwärter
IT/IP/Datenschutz
Digital Industries Group

benjamin.kraudinger@dorda.at