AI ACT

Walk-Through

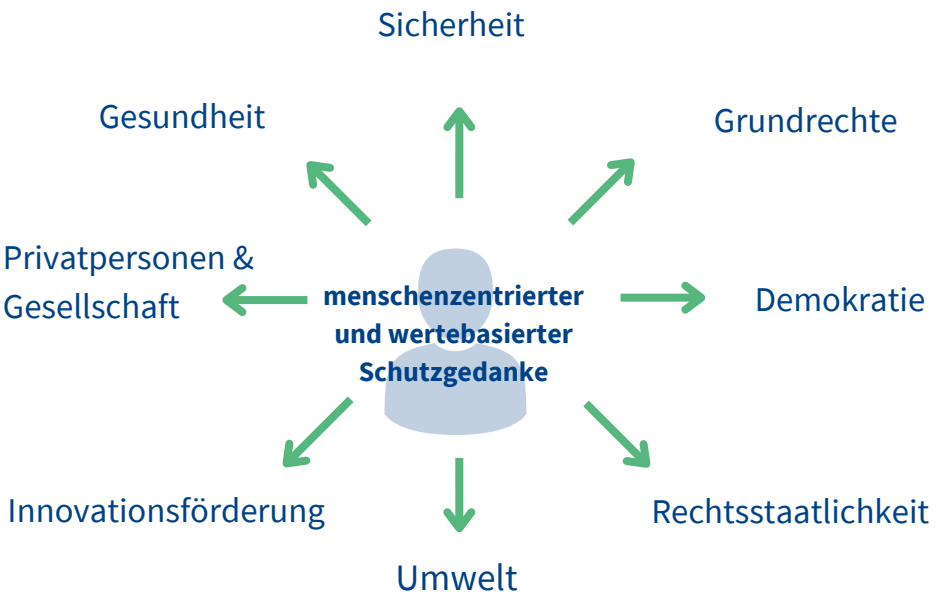
DORDA

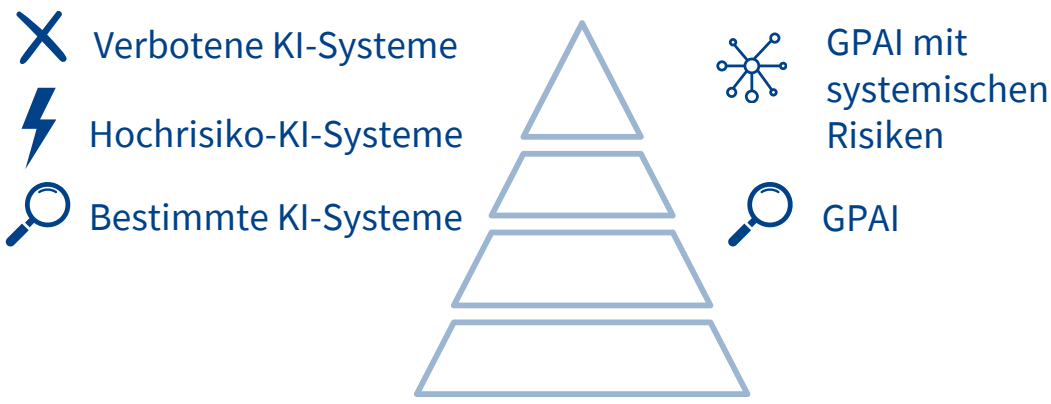
| Digital Industries Group |

Überblick

Ziele

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





Good News! Alle KI-Systeme, die nicht unter eine dier Risikoklassen fallen, sind nach dem AI Act ohne weitere Maßnahmen erlaubt.

Herzstück des AI Act: Der risikobasierter Ansatz

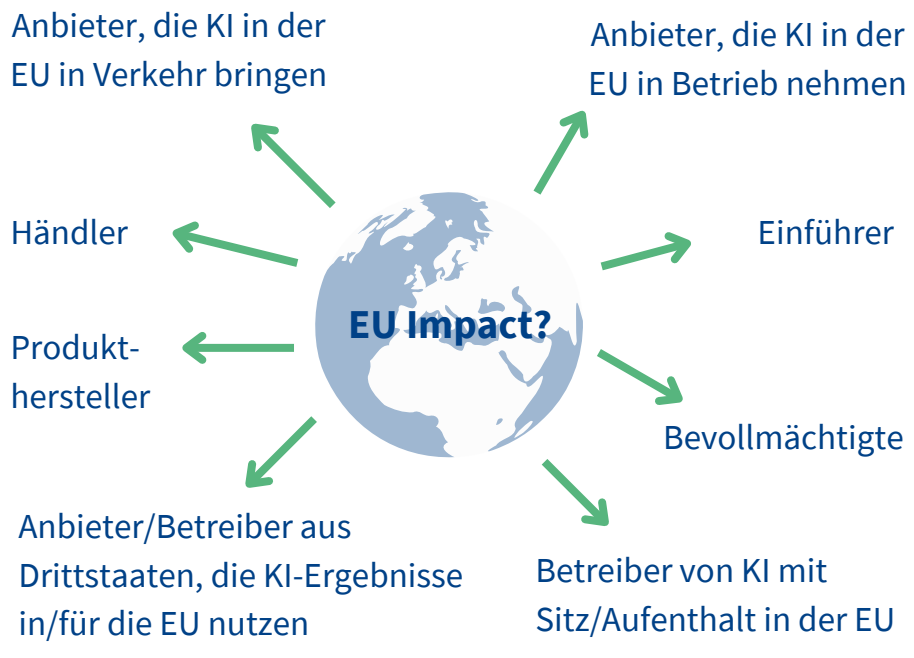
Der AI Act qualifiziert das Risikopotential einer KI anhand eines Klassifizierungssystems. Abhängig von der entsprechenden Einordnung knüpfen unterschiedliche Pflichten an die Nutzung eines KI Systems. KI-Systeme mit allgemeinem Verwendungszweck (General Purpose AI; “GPAI”) sind gesondert geregelt.

Verpflichtete

Der AI Act nimmt unterschiedliche Akteure in die Pflicht:

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

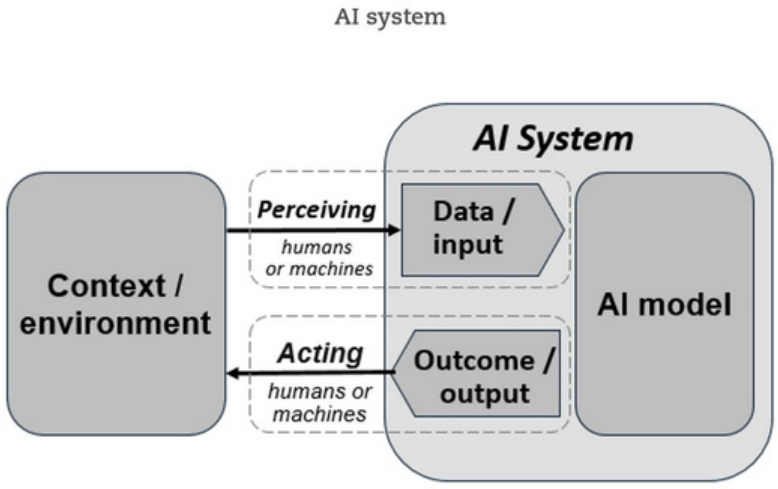
Ein Sitz im Drittstaat entbindet die Akteure nicht von ihren Pflichten, wenn das KI-System für die EU bestimmt ist.



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 Eingaben für explizite oder implizite Ziele ableitet, wie dadurch hervorgebrachte **Ergebnisse die physische oder virtuelle Umgebungen 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.

Ausnahmen: Modelle für Forschungs- und Entwicklungstätigkeiten sowie für das Design von Prototypen.

Abgrenzung zu herkömmlicher Software

Typische Merkmale einer KI:

- Fähigkeit zur Ableitung aus Eingaben oder Daten
- Nutzung von Techniken, wie maschinelles Lernen, logi- und wissensgestützte Konzepte
- Systeme mit verschiedenen Graden an Autonomie

Keine KI-Systeme:

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

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

Durchführung einer Bestandsaufnahme, ob KI-Systeme iSd AI Act bereits eingesetzt werden und Berücksichtigung bei neuen Use Cases.

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

Ausnahmen vom Anwendungsbereich

- Nutzung ausschließlich zu **militärischen Zwecken**
- Nutzung zu **Verteidigungszwecken** oder zu Zwecken der **nationalen Sicherheit**
- Entwicklung und Inbetriebnahme ausschließlich zur **wissenschaftlichen Forschung und Entwicklung**
- **Entwicklungstätigkeiten** vor Inverkehrbringen in einer Testumgebung, sofern sie nicht unter realen Bedingungen erfolgen
- Nutzung durch natürliche Person zu **ausschschließlichen persönlichen und nicht beruflichen Zwecken**
- Bereitstellung unter **freien und quelloffenen Lizenzen**

KI-Systeme die unter freien und quelloffenen Lizenzen bereitgestellt werden, dürfen dennoch **keine verbotenen KI-Systeme** darstellen.

Fallen diese KI-Systeme in die **Hochrisiko-Kategorie** müssen die Pflichten und Voraussetzungen des AI Act beachtet werden.

Näheres zur **Klassifizierung** unter **Step 4**

Praxistipp

Die Voraussetzungen der einzelnen Ausnahmen ist im Einzelfall genau zu prüfen. Die Ausnahmebestimmungen sind eng auszulegen.

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 die KI **entwickelt oder entwickeln lässt** oder sie unter eigenen Namen **in Verkehr bringt** oder **in Betrieb nimmt**. Um keine Rechtsschutzlücke zu öffnen, treffen **auch andere Marktteilnehmer die selben Pflichten**. Für die gesamte Lieferkette - **vom Hersteller bis zum Endnutzer -** ist daher das Regelungswerk des AI Acts relevant.

Anbieter

Hersteller und Vertreiber unter eigenem Namen

Einführer

Importeur aus einem Drittland in die EU mit Niederlassung in der Union

Händler

Anbieter auf dem Unionsmarkt

Betreiber

Verwendung in eigener Verantwortung

Praxistipp

Auch abseits des klassischen Anbieters können Tätigkeiten vom AI Act erfasst sein. Mit einem Assessment zum Umfang der Anwendbarkeit können Compliance-Risiken frühzeitig erkannt und mitigiert werden.

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

Verbotene KI-Systeme

Darunter fallen insb KI-Systeme zu einem oder mehrerer der folgenden Zwecke:

- Manipulation von Personenenverhalten mit erheblichem Schadensrisiko
- Social-Scoring
- Automatisierte Gesichtserkennung
- Biometrische Echtzeitidentifizierung

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

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

Widerlegung durch Risikoabwägung teilweise möglich

Der Hochrisiko-Charakter der in Anhang III zum AI Act aufgelisteten Anwendungen kann allerdings widerlegt werden, wenn es **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 **Parameter** vorzunehmen.

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),
- in **Anhang III zum AI Act** aufgelistet sind (zB bestimmte biometrische Anwendungen, AI in kritischen Infrastrukturen, in der allgemeinen und beruflichen Bildung, gewisse KI-Systeme im HR, Kreditscoring, Risikobewertung und Preisbildung iZm Kranken- und Lebensversicherungen).

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 einer 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 ihren Anhängen geregelt.

Praxistipp

Das Augenmerk im AI Act-Compliance-Projekte sollte auf die Hochrisiko-Klassifizierung liegen. Diese Einordnung bringt die meisten Pflichen mit sich und ist zu priorisieren. Die Kommission wird bis spätestens 18 Monaten nach Inkrafttreten Leitlinien zur praktischen Umsetzung von Hochrisiko-KI erlassen und eine Liste an Beispielen für derartige KI-Systeme bereitstellen. Unter Berücksichtigung der 24-monatigen Umsetzungsfrist ist ein Zuwarten aber sehr riskant.

Pflichten

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

Bestimmte KI-Systeme

Dazu zählen zB KI-Systeme, die zur Interaktion mit Personen entwickelt wurden (klassische Chatbots) oder Inhalte erzeugen.

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 systemischen Risiko**.

Pflichten

Alle Anbieter von GPAI müssen die Systementwicklung und **Trainingsinhalte** ausreichend dokumentieren und auch entsprechende **Informationen für nachgelagerte Anbieter** bereitstellen, damit diese das System nachvollziehen können. Dazu zählen:

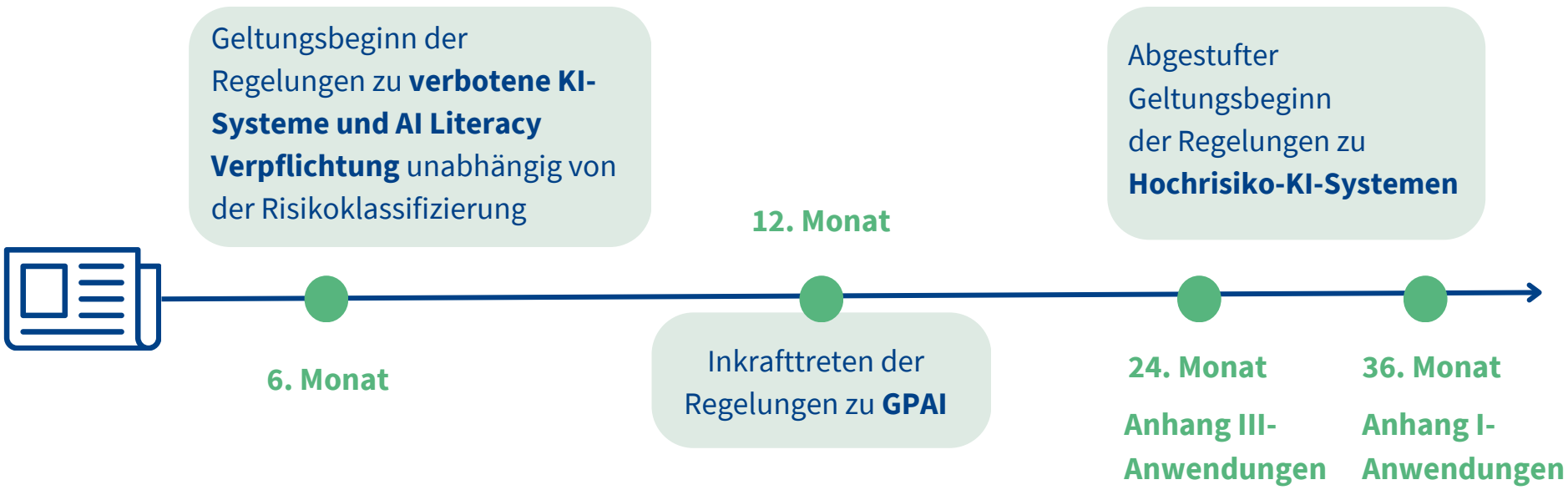
- Offenlegung, dass der Inhalt durch KI generiert wurde
- Verhinderung der Erzeugung illegaler Inhalte durch entsprechendes Product Design
- Veröffentlichung von allgemeinen Zusammenfassungen über die für das Training verwendeten urheberrechtlich geschützten Inhalten

Anbieter von GPAI mit **systemischen Risiken** müssen überdies eine **Modellbewertung** auf mögliche Risiken durchführen, bestimmte **Meldepflichten** erfüllen und **Cybersicherheitsmaßnahmen** gewährleisten.

Für Entwickler und Anbieter von freier, quelloffener Software gelten Sonderregelungen.

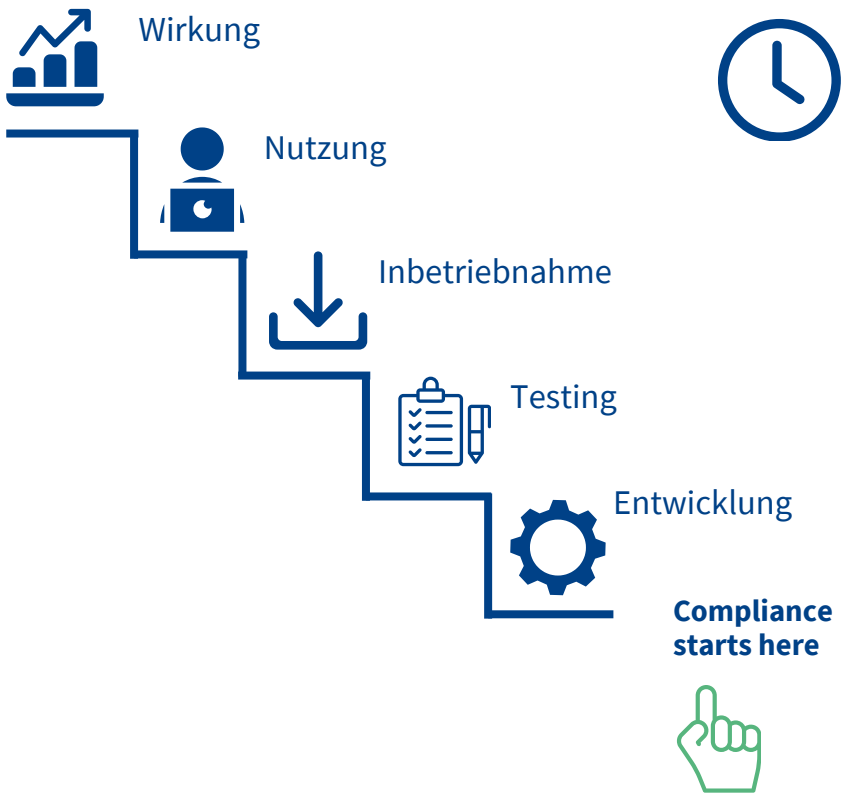
Step 5: Fristgerechte Umsetzung

Wichtige Compliance Fristen



Die **Regelungen des AI-Acts** werden **schrittweise** nach Inkrafttreten des Gesetzes für die betroffenen Personen **wirksam**.

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



Geldstrafen

Verstoß gegen Bestimmungen zu **verbotenen KI-Systemen** und **Data-Governance**	bis zu **EUR 35 Mio** oder **7%** des Jahresumsatzes
Verstoß gegen **allgemeine Compliance-Pflichten** und **Bestimmungen zu GPAI**	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