LexisNexis®

DORDA

AI Act Compliance

Alexandra Ciarnau, Axel Anderl

22.5.2024

#Cybercrime
Handbuch für die Praxis

Cyberattacken sind eines der akutesten Bedrohungsszenarien für Unternehmen.
Dieses Werk beruht auf Erfahrungswerten des hochkarätigen Autorenteams aus der Betreuung zahlreicher Mandanten in Cyberkrisen.

Dieses Praxishandbuch soll Ihnen daher als **Leitfaden, Handlungsanweisung** und **Stütze** für die notwendige **Präventionsarbeit**, aber auch im Anlassfall als Hilfe dienen.

Der Inhalt deckt die relevanten Rechtsgebiete vom Datenschutz- über das Versicherungs- und das Gesellschaftsrecht bis hin zum Zivil- und Strafrecht ab.
Mit zahlreichen Beispielen aus der Praxis ist es **bewusst lösungsorientiert** gestaltet.

1. Auflage
Preis: € 68,00
Anzahl Seiten: 328
ISBN: 978-3-7007-8566-8

Jetzt im Webshop bestellen

Erscheint in Kürze:

#Blockchain in der Rechtspraxis
SBN: 978-3-7007-8313-8
Auflage: 2., neu bearbeitete Auflage
Erscheinungsdatum: 30.06.2024
Autoren: Anderl Axel, Artner Stefan, Baumann Christian, Brandstetter Magdalena, Brogyányi Christoph, ...
Herausgeber: Anderl Axel
Seitenanzahl: 300
Preis: EUR 69,00*

Jetzt vorbestellen

*Beim Kauf dieses Artikels handelt es sich um eine Vorbestellung.

Der angegebene Preis kann sich gegebenenfalls noch ändern.

Anwältin im IT/IP und Datenschutzteam und Co-Leiterin der Digital Industries Group

- Schwerpunkte: IT-/IP- und Datenschutzrecht, New Technology
- Autorin zahlreicher Fachpublikationen und einschlägige Lehrtätigkeit an Universitäten
- Co-Autorin #Blockchain, LexisNexis, IP in der Praxis bei Manz, UWG Praxishandbuch bei Linde, Handbuch Nachhaltigkeitsrecht bei Manz, Nachhaltige Finanzierung bei Linde
- Vorstandsmitglied von Women in AI Austria
- Standortleiterin DORDA sphere

Alexandra Ciarnau

alexandra.ciarnau@dorda.at

Managing Partner, Leiter des IT/IP und Datenschutzteams und der Digital Industries Group

- Führender IT/IP/Datenschutz-Experte in den Anwaltsrankings (Legal 500, Chambers: Leading Individual); Hall of Fame TMT legal500; elf ILO Client Choice Awards
- Schwerpunkte: IT-Verträge, Out- und Cloudsourcing und New Technology
- Autor zahlreicher Fachpublikationen und einschlägige Lehrtätigkeit an Universitäten
- (Co-)Herausgeber des NISG-Kommentars, Verlag Manz; Herausgeber #Blockchain sowie #Cybersecutity, jeweils Verlag LexisNexis; IP in der Praxis, Verlag Manz und UWG Praxishandbuch, Verlag Linde

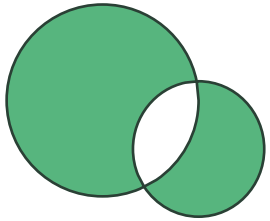
Axel Anderl

axel.anderl@dorda.at

Agenda

Ziele und Zwecke des AI Act / Status im Gesetzgebungsverfahren

Umsetzungsfristen und Priorisierung



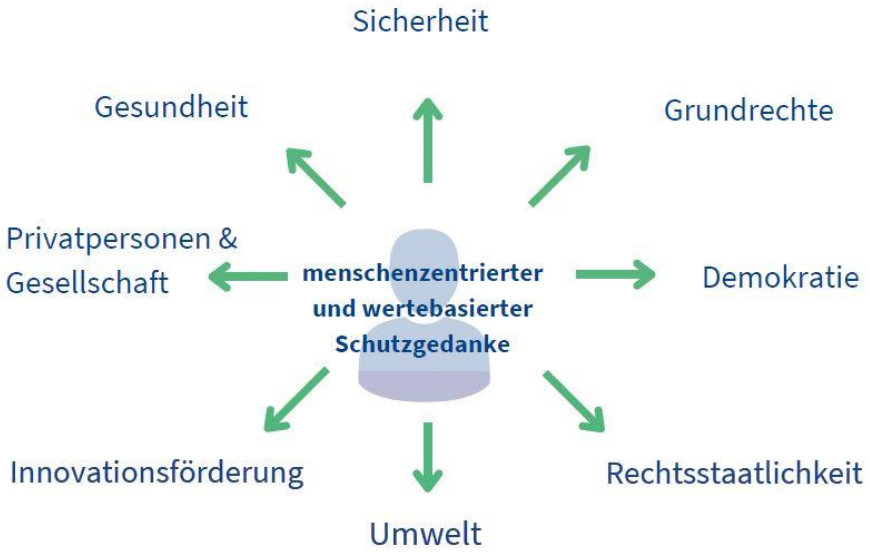
Anwendungsbereich des AI Act

Meine Rolle in der Lieferkette

Der risikobasierte Ansatz

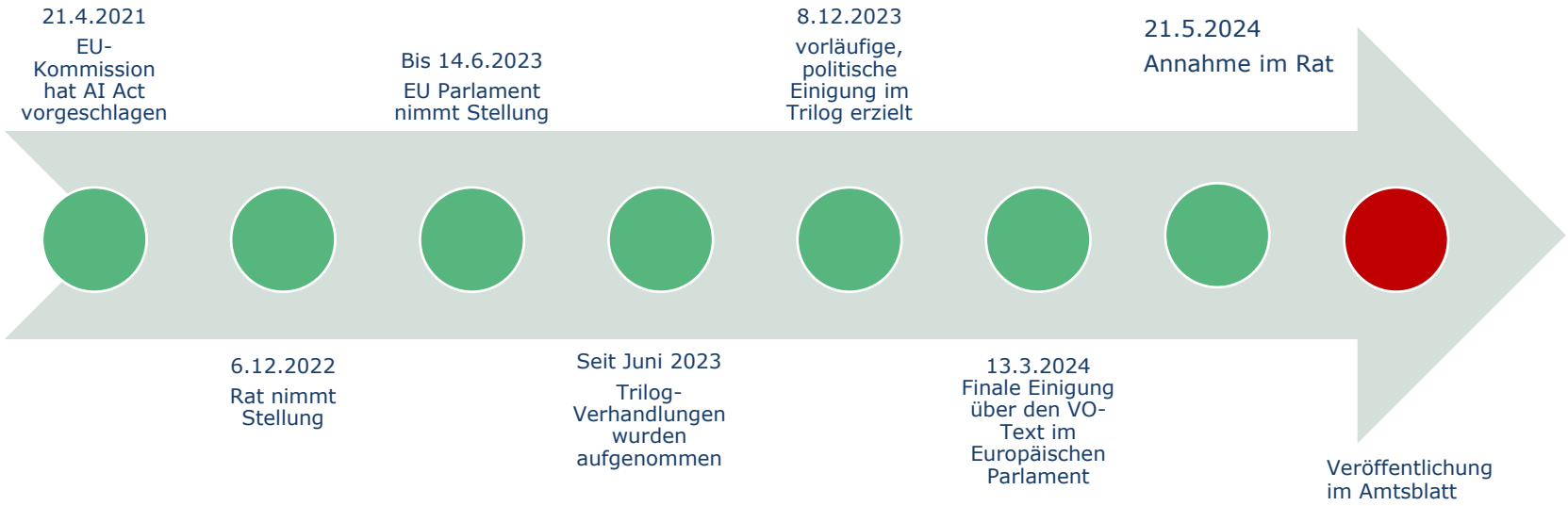
Ziele und Zwecke

- Sicherer und vertrauenswürdiger Einsatz von KI
- Schaffung eines einheitlichen, hohen Schutzniveaus

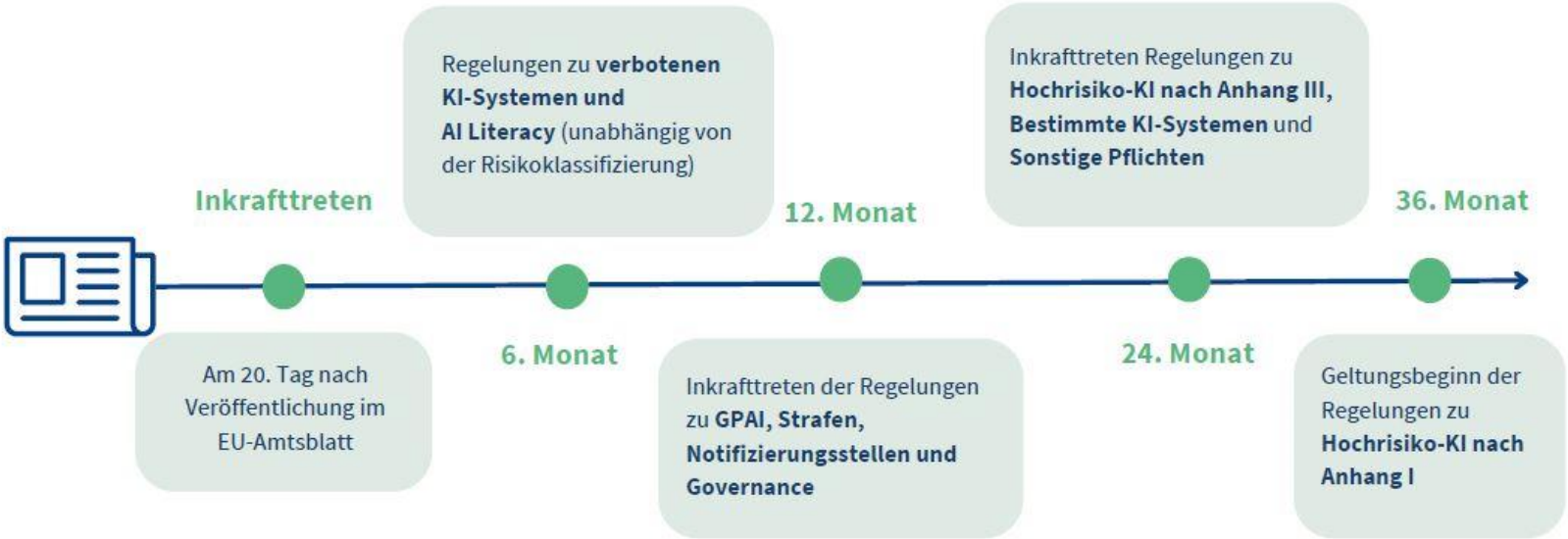


- Förderung von Innovationen
  - KI-Reallabore
  - Ausnahmen vom Anwendungsbereich
  - Risikobasierter Ansatz
  - Berücksichtigung von KMUs

Status


21.4.2021
EU-Kommission hat AI Act vorgeschlagen
6.12.2022
Rat nimmt Stellung
Bis 14.6.2023
EU Parlament nimmt Stellung
Seit Juni 2023
Trilog-Verhandlungen wurden aufgenommen
8.12.2023
vorläufige, politische Einigung im Trilog erzielt
13.3.2024
Finale Einigung über den VO-Text im Europäischen Parlament
21.5.2024
Annahme im Rat
Veröffentlichung im Amtsblatt

Umsetzungsfristen und Priorisierung



Umsetzungsfristen und Priorisierung

Ist mein System als KI iSd AI Act zu qualifizieren?

- Prio 1 → Bestandsaufnahme
- Prio 1 → Umsetzung der KI-Kompetenz (betrifft Anbieter/Betreiber)

Fällt die Nutzung in den Anwendungsbereich des AI Act?

- Prio 1

In welcher Rolle nutze ich AI?

- Prio 1

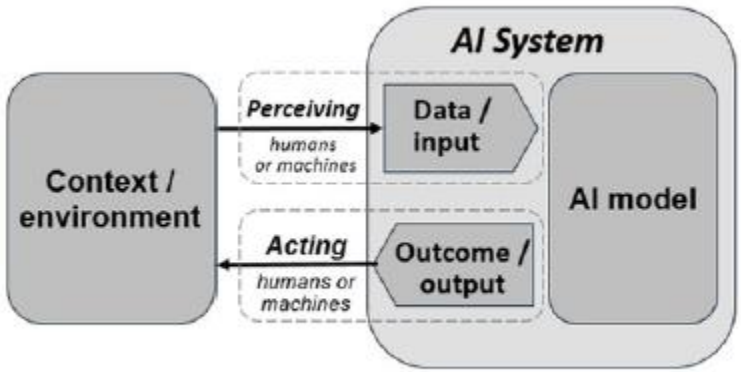
In welche Risikoklasse fällt das KI-System und welche Pflichten muss ich erfüllen?

- Prio 1 bei Hochrisiko → daran knüpfen die meisten Pflichten an
- Prio 2 bei GPAI
- Prio 3 bei bestimmte KI-Systeme

→ Umsetzung

Anwendungsbereich des AI Act

- „**KI-System**" ist ein **maschinengestütztes System**, das
  - für einen in **wechselndem Maße autonomen Betrieb** ausgelegt sind,
  - nach seiner Einführung **anpassungsfähig sein kann** und
  - aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie **Ergebnisse** wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen hervorgebracht werden, die **physische oder virtuelle Umgebungen beeinflussen** können.
- EN-Fassung spricht auch von „inference"
  - Für technische Beurteilung releva
- Angelehnt an OECD-Definition



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

Anwendungsbereich des AI Act

- Abgrenzung zu herkömmlicher Software?
- ErwGr gehen nur knapp darauf ein

KI

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

Herkömmliche Software

- Software basiert ausschließlich auf von natürlichen Personen definierten Regeln für das automatische Ausführen von Operationen
- Software basiert auf herkömmliche Programmieransätze

Anwendungsbereich des AI Act

- „**KI-Modell mit allgemeinen 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.

- Beispiele
  - OpenAI
  - MistralAI
  - Gemini

Ausnahmen vom Anwendungsbereich

Relevante Beispiele

- **Wissenschaftliche Forschung und Entwicklung**
- **Entwicklungstätigkeiten** unter nicht-realen Bedingungen
- **Bereitstellung unter freier und quelloffener Lizenz**
  - Voraussetzungen:
    - Kostenfrei
    - Offenlegung der Parameter, einschließlich Gewichte, Informationen über die Modellarchitektur und Informationen über die Modellnutzung
  - Ausnahme: GPAI mit systemischen Risiken

Meine Rolle in der Lieferkette

Anbieter

Hersteller und Vertreiber unter eigenem Namen

Einführer

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

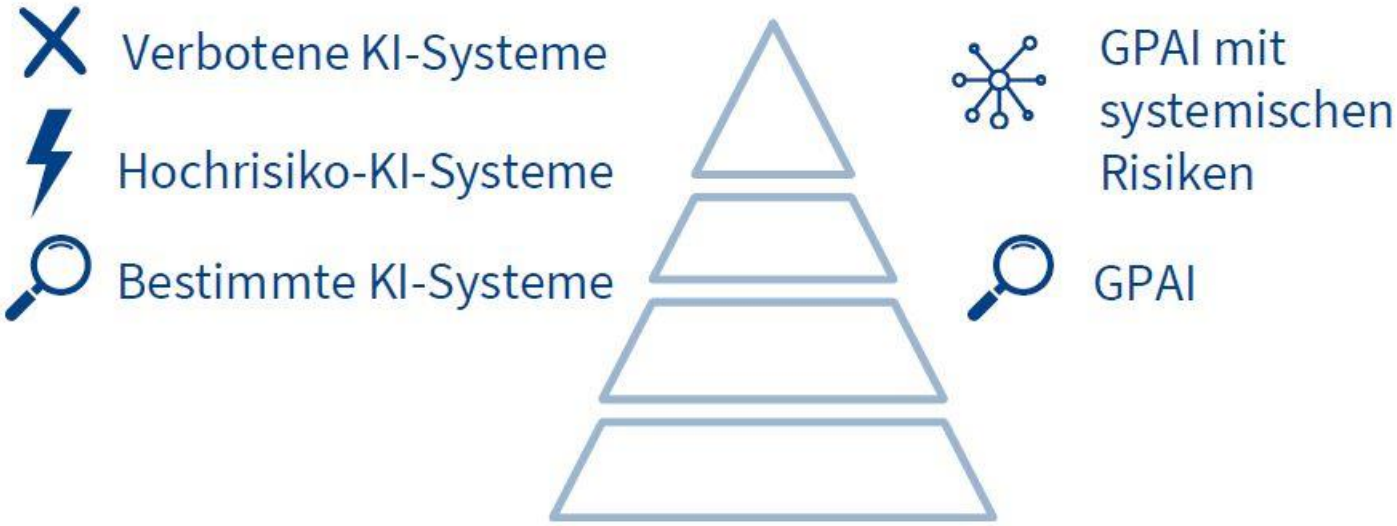
Händler

Anbieter auf dem Unionsmarkt

Betreiber

Verwendung in eigener Verantwortung

Der risikobasierte Ansatz



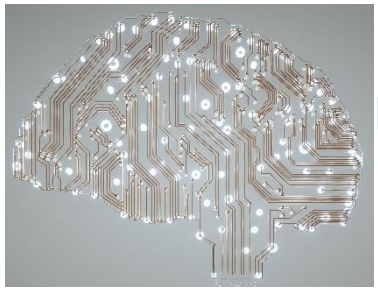
Der risikobasierte Ansatz – Verbotene KI

Beispiele aus Art 5

Biometrische Kategorisierung → politische Meinung, Gewerkschaftsmitgliedschaft, religiöse oder weltanschauliche Überzeugungen, Rasse, Sexualleben oder sexuelle Ausrichtung ohne gesetzliche Grundlage

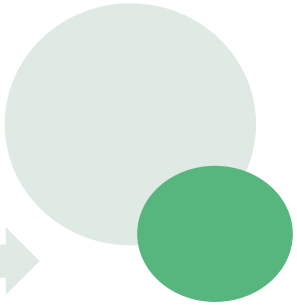
Emotionserkennung am Arbeitsplatz →

Der risikobasierte Ansatz – Verbotene KI



Reize, zB über Töne, Bilder, Videos

Manipulative, täuschende Techniken



Außerhalb der Wahrnehmung

Beeinflussung der Entscheidung

Große finanzielle Schäden

Social Scoring

Der risikobasierte Ansatz – Hochrisiko-KI

Art 6 ff + Beispiele aus Anhang I/III

- KI-Systeme, die als Sicherheitskomponente genutzt werden und unter die in **Anhang I** aufgelisteten Vorschriften fallen
  - zB Sicherheit von Spielzeugen, Sicherheit von Aufzügen
- KI-Systeme, die **in Anhang III** aufgelistet sind
  - Biometrik
    - zB Biometrische Fernidentifizierungssysteme, Biometrische Kategorisierung, Emotionserkennung
  - Kritische Infrastruktur
    - zB Kritische digitale Infrastruktur, Straßenverkehr, Wasser-, Gas-, Wärme- und Stromversorgung

  - Allgemeine und berufliche Bildung

Der risikobasierte Ansatz – Hochrisiko-KI

- Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit
  - Gezielte Schaltung von Stellenanzeigen, Sichtung von Bewerbungen, Bewertung von Bewerbern
  - Entscheidungen über Arbeitsbedingungen (zB Beförderung)
- Zugänglichkeit und Inanspruchnahme grundlegender privater und grundlegender öffentlicher Dienste und Leistungen
  - zB Kreditwürdigkeitsprüfung und Bonitätsbewertung (ausgenommen zur Aufdeckung von Finanzbetrug)
- Strafverfolgung
- Migration, Asyl und Grenzkontrolle
- Rechtspflege und demokratische Prozesse

Der risikobasierte Ansatz – Hochrisiko-KI

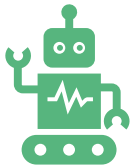
Widerlegung durch Risikoabwägung bei Hochrisiko-Anwendungen

- Nur für vordefinierte Anwendungen in Anhang III möglich
- Voraussetzungen
  - Kein erhebliches Risiko der Beeinträchtigung bzgl Gesundheit, Sicherheit oder Grundrechte
  - Keine Beeinträchtigung in dem das Ergebnis die Entscheidungsfindung nicht wesentlich beeinflusst
  - Eng gefasste Verfahrensaufgabe, bloße Erkennung von Entscheidungsmustern, vorbereitende Maßnahme etc
- AI Act gibt Parameter zur Risikoabwägung vor
- Einschätzung liegt in eigener Verantwortung – keine Einbindung von Behörden vorgesehen

Der risikobasierte Ansatz – Hochrisiko-KI

- Inverkehrbringung nur unter Einhaltung strenger Auflagen, wie zB
  - Betrieb von KI gemäß dem allgemein anerkannten Stand der Technik
  - Einrichtung, Anwendung, Dokumentation und Aufrechterhaltung eines Risikomangementsystems
  - Daten und Datengovernance → meint den Einsatz von Techniken zum Modelltraining mit Trainings-, Validierungs- und Testdatensätzen, wobei insb Herkunft, Datenqualität, Bias, Verzerrungen und Lücken erkannt werden müssen, um eine "fehlerfreie" Software zu gewährleisten → in der Praxis wird die Bias-Messung eine der größten Herausforderungen darstellen.
  - Technische Dokumentation vor Inverkehrbringung oder Inbetriebnahme
  - Aufzeichnungspflichten ("Protokollierung") während des gesamten Lebenszyklus
  - Transparenz- und Informationsbereitstellungspflichten für Betreiber →
  - Menschliche Aufsicht
  - Genauigkeit, Robustheit und Cybersicherheit
- Weitere Pflichten für Anbieter und Betreiber
- Berücksichtigung bei der IT-Beschaffung

Der risikobasierte Ansatz – Bestimmte KI-Systeme & GPAI



- Bestimmte KI-Systeme unterliegen primär Transparenzvorschriften
  - Kennzeichnungspflichten bei Interaktion mit KI
  - Minimierung des Täuschungsrisikos und Identitätsbetrugs

- GPAI
  - Offenlegung, dass Inhalt von KI generiert wurde
  - Verhinderung der Erzeugung illegaler Inhalte
  - Veröffentlichung von allgemeinen Zusammenfassungen über trainingsrelevante, urheberrechtlich geschützte Inhalte
- Sonderpflichten für GPAI mit systemischen Risiken
  - Voraussetzung: Hohe Leistungsfähigkeit, mind 10^25 FLOPS

Geldbußen nach dem AI Act

Mind the bigger picture

ABGB

RL-Resilienz kritischer Einrichtungen

AI-Act

TKG

NIS2- RL

Grund-rechte

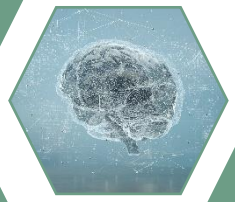
Cyber-Resilience-Act

UrhG

DSGVO

DSA

UWG
KSchG



DSG

KI-Haftungs-RL

Industrie-Spezifika

Data Governance Act

Data Act

PHG

Haftung

DORDA

Vielen Dank für Ihre Aufmerksamkeit!

TIER 1 Legal500 2007-2024: TMT
TIER 1 Legal500 2020-2024: Data Privacy & Data Protection
TIER 1 Legal500 2021-2024: Intellectual Property
BAND 1 Chambers Europe 2008-2024: TMT:IT

DORDA Rechtsanwälte GmbH · Universitätsring 10 · 1010 Wien · www.dorda.at