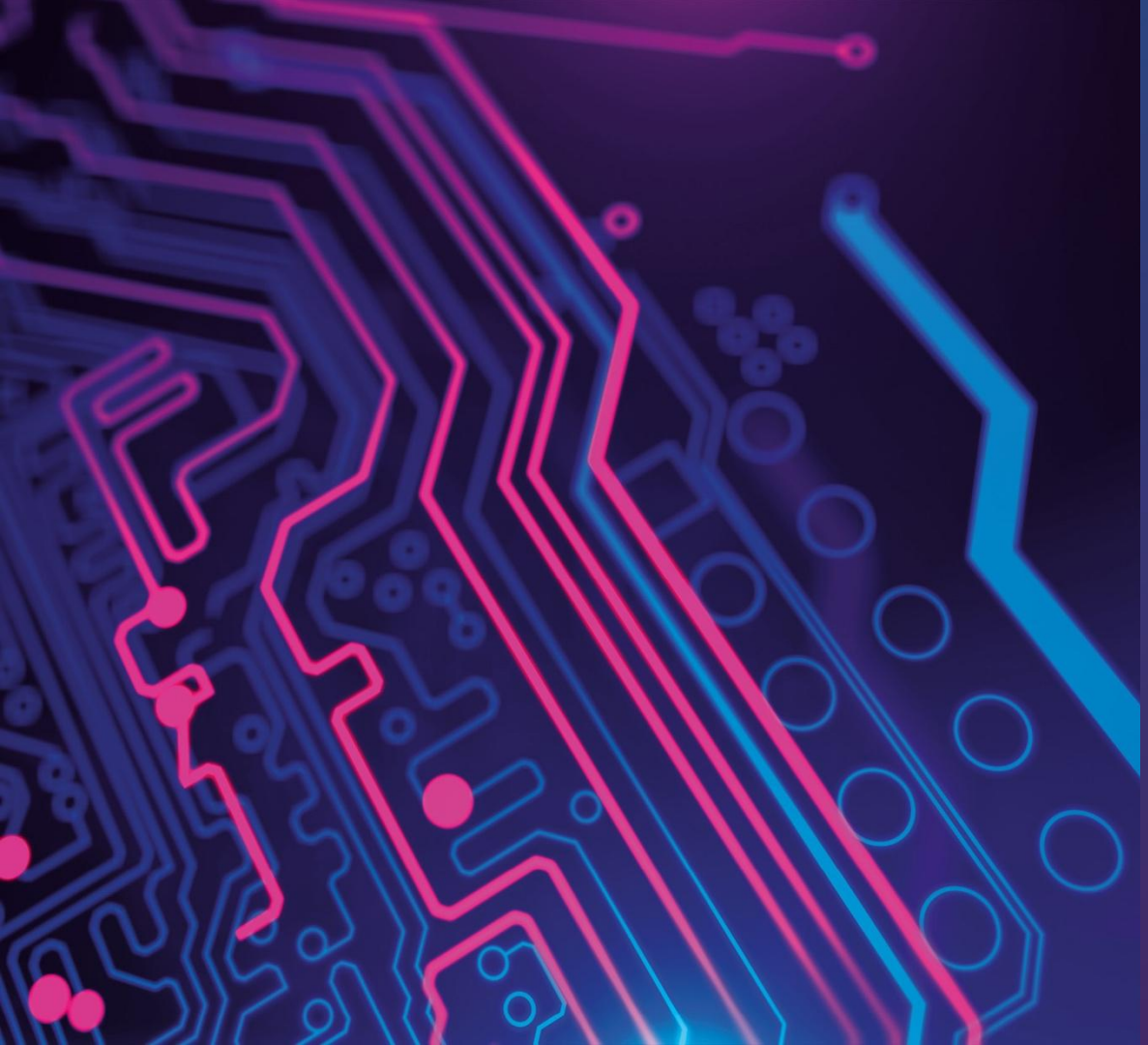


fieldfisher

EU-AI-Act: Praktische Lösungen für KMU

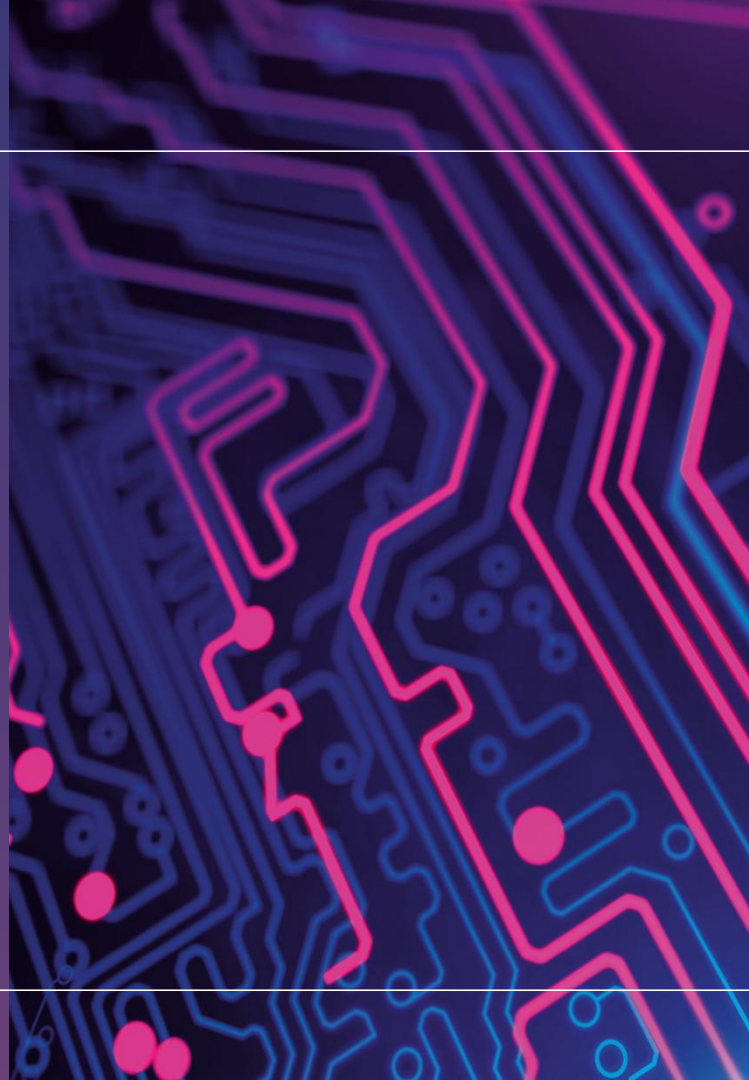
Effiziente Umsetzung und konkrete Handlungsempfehlungen

Marvie Demit
Benedikt Hasibeder
Philipp Reinisch

Wien, 10.06.2025

Agenda

- KI-Technologie:
  Wovon reden wir? Anwendungsbeispiele
- Rechtsgrundlagen:
  KI-Gesetz, Arbeits- und Datenschutzrecht, Haftung
- Umsetzung, Nutzung bestehender Strukturen (?)



KI-Technologie (1)

Begriff KI

→ Eine Maschine kann Aufgaben wie Lernen, Problemlösen, Sprache und Entscheidungsfindung übernehmen.

Arten von KI: Schwache vs. starke KI

→ Umsetzung spezifischer Aufgaben

→ Ist in der Lage, jegliche intellektuelle Aufgabe zu bewältigen, die auch ein Mensch ausführen könnte.

KI-Technologie (2)

Funktionsweise:
Maschinelles Lernen, neuronale Netze

Anwendungsbeispiele:
Automatisierung, Entscheidungsunterstützung, Chatbots, Spracherkennung

- KI lernt aus Daten. Je mehr Daten sie bekommt, desto besser wird sie darin, Aufgaben zu erledigen.
- Funktionsweise wie menschliches Gehirn, können komplexe Muster erkennen
- Chatbots (Verwaltung, Kundenservice)
- Risikobewertung im Finanzsektor
- Spracherkennung, Übersetzungsdienste

Definition eines KI-Systems (Art 3 Z1)

Ein "KI-System" ist ein maschinelles System, das:

1	die so konzipiert sind, dass sie mit unterschiedlichem Grad an Autonomie betrieben werden können und nach dem Einsatz eine Anpassungsfähigkeit aufweisen können, und
2	die für explizite oder implizite Ziele,
3	leitet aus den empfangenen Eingaben ab, wie Ergebnisse wie Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erzeugt werden können,
4	die physische oder virtuelle Umgebungen beeinflussen können.

Rechtsgrundlagen (1)

EU KI-Gesetz: Überblick und Ziele

- → Risikobasierter Ansatz, Hochrisiko-KI-Systeme
- → „KI-Beauftragter“ (?)
- → Problem „Black-Box-Entscheidung“

Datenschutz: DSGVO
Automatisierung, Entscheidungsunterstützung, Chatbots, Spracherkennung

- → Rechtsgrundlagen, Datenschutzfolgeabschätzung
- → Einhaltung Betroffenenrechte, Transparenz

Rechtsgrundlagen (2)

Haftungsfragen bei KI-gestützten Entscheidungen

- → Wer haftet für Fehler?
- → Verantwortung des Arbeitgebers

Arbeitsrecht

- → Überwachung von MitarbeiterInnen
- → ArbVG
- → Maßstab Menschenwürde

Akteure im Rahmen des KI-Gesetzes

Betreiber
Begriff, der für einen der folgenden Akteure verwendet wird

Anbieter

Endnutzer

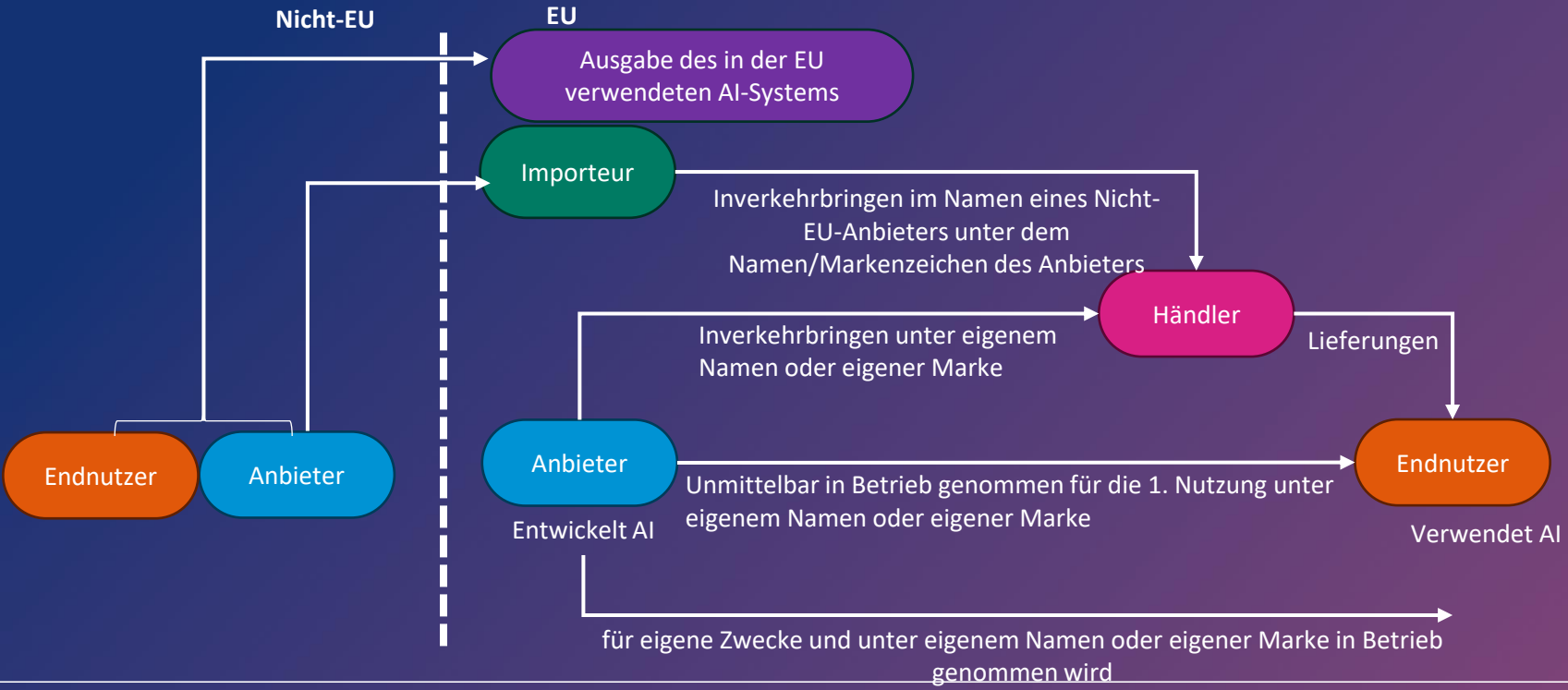
Bevollmächtigte
Bevollmächtigte
Für Nicht-EU-Anbieter

Importeure

Händler

Betroffene Person

Aktivitäten, die unter das AI-Gesetz fallen



Klassifikation

Verbotene AI-Systeme

- Kognitive Verhaltensmanipulation zur Umgehung des freien Willens, z. B.: Unterschwellige Werbung
- Ausnutzung von Schwachstellen (Alter, körperliche oder geistige Behinderung).
- Social Scoring und biometrische Kategorisierung von sensiblen Merkmalen
- Erstellung von Gesichtserkennungsdatenbanken durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder aus Videoüberwachungsaufnahmen
- Erkennung von Emotionen am Arbeitsplatz oder im Bildungssystem

Hochriskante KI-Systeme

- Rechtspflege und Demokratie, Biometrie, kritische Infrastrukturen, allgemeine und berufliche Bildung, Beschäftigung und Arbeitskräftemanagement, Strafverfolgung, wesentliche Dienste, Migration usw.
- Gefahr einer Beeinträchtigung der Gesundheit, der Sicherheit und der Grundrechte der Menschen

GPAI-Modelle und generative KI

z. B. Große Sprachmodelle (z. B. ChatGPT)

Transparenzanforderungen für bestimmte KI-Systeme und GPAI-Modelle

- z. B. Chatbots, generative KI oder Deep Fakes
- Diese KI-Systeme oder GPAI-Modelle können risikoreich sein oder nicht
- den Menschen die Möglichkeit geben, eine informierte Entscheidung zu treffen oder sich aus einer bestimmten Situation zurückzuziehen

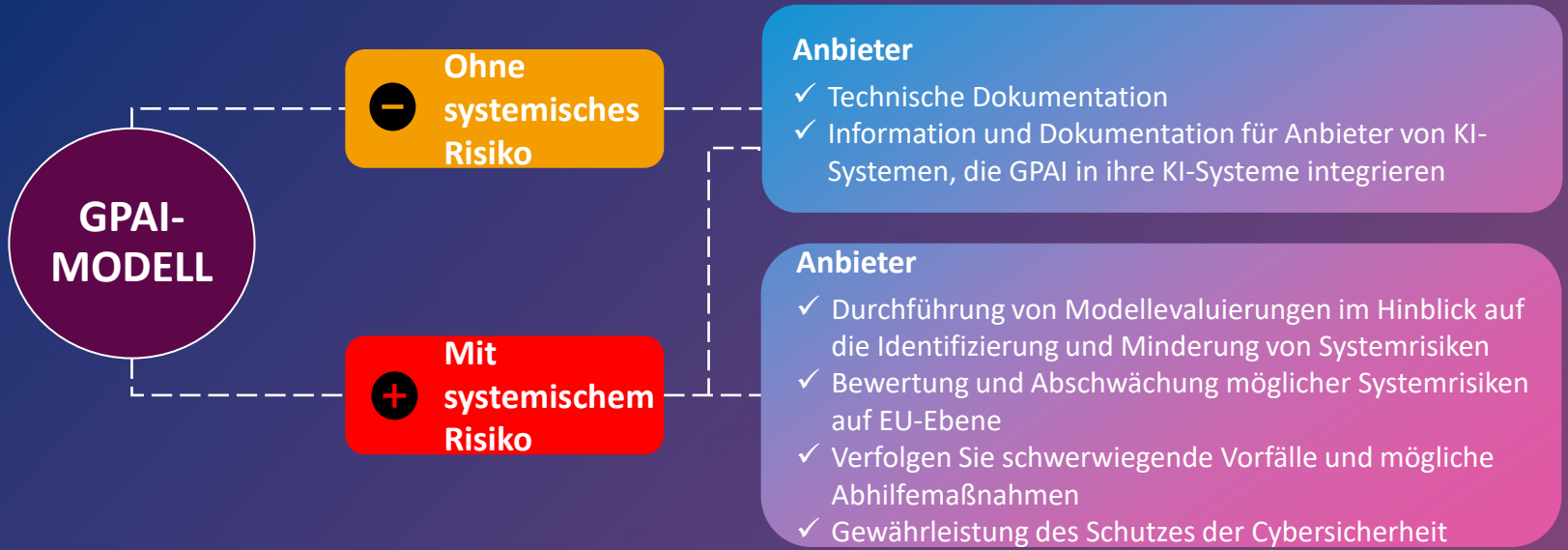
Unregulierte KI-Systeme, z. B. KI-gestützte

- Videospiele
- Spam-Filter

Klassifikation der KI-Systeme

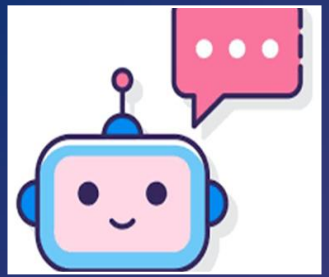
Hochriskante KI?
GRUNDSATZ - "risikoreiche" KI-Systeme sind:
• ein **Produkt** oder ein **Sicherheitsbauteil eines Produkts** sind, das den EU-Harmonisierungsvorschriften (**Anhang I**) unterliegt und **einer Konformitätsbewertung durch Dritte unterzogen** werden muss
• **ein erhebliches Risiko für die** Gesundheit, die Sicherheit oder die Grundrechte von natürlichen Personen darstellen (**Anhang III**)
AUSNAHME - nicht als "risikoreiche" KI-Systeme betrachtet werden, die kein erhebliches Risiko einer Beeinträchtigung der Gesundheit, der Sicherheit oder der Grundrechte natürlicher Personen darstellen, u. a. weil sie das Ergebnis der Entscheidungsfindung nicht wesentlich beeinflussen
AUSNAHME VON DER AUSNAHME - Profiling

Klassifikation: GPAI-Modell (= “KI mit allg Verwendungszweck”)



Transparenz

KI-Systeme, die direkt mit Menschen interagieren



Anbieter müssen Personen darüber informieren, dass sie mit einer Maschine interagieren

Generative KI

Die Anbieter müssen sicherstellen, dass alle Ausgaben (Audio, Bild, Video, Text) als künstlich erzeugt oder manipuliert gekennzeichnet sind.

Systeme zur Erkennung von Emotionen

Die Einsatzkräfte müssen die gefährdeten Personen über die Funktionsweise des Systems informieren

Deep Fakes

Bereitsteller müssen offenlegen, dass Inhalte künstlich erzeugt oder manipuliert wurden

Geldbußen

35 Millionen Euro oder 7% des weltweiten Jahresumsatzes

- Das Inverkehrbringen eines verbotenen KI-Systems.

15 Millionen Euro oder 3% des weltweiten Jahresumsatzes

- Die meisten Verstöße im Zusammenhang mit hochriskanten KI-Systemen und GPAI
- Verpflichtungen für Anbieter, Importeure, Vertreiber und Verteiler

7,5 Millionen Euro oder 1 % des weltweiten Jahresumsatzes

- Erteilung unrichtiger, unvollständiger oder irreführender Auskünfte an die Aufsichtsbehörden in Beantwortung einer Anfrage

Haftung nach dem EU AI Act

- Anbieter (Provider):
  - Konformität des KI-Systems mit den Anforderungen des EU AI Act.
  - Dokumentation der Hochrisiko-KI (z. B. medizinische Diagnosesysteme, Kreditbewertung)
  - Tragen Verantwortung für fehlerhafte KI
- Bereitsteller (Deployers):
  - Unternehmen, die KI einsetzen, haften für den korrekten und rechtskonformen Einsatz.
  - stellen sicher, dass die KI nicht diskriminierend oder rechtswidrig agiert.
- Importeure und Händler:
  - Können haftbar sein, wenn sie wissentlich nicht rechtskonforme KI-Produkte in die EU bringen oder weiterverkaufen.

Umsetzung: 6-Punkte-Plan

1. Erstellung “Landkarte" der KI-Systeme und Bestimmung der Anwendbarkeit des EU-KI-Gesetzes
2. Bestimmung der Risikoklassifizierung der untersuchten Systeme und Modelle
3. Verstehen Sie die Rolle der Organisation, z. B. als Anbieter, Verteiler usw.
4. Implementierung eines KI-Governance-Rahmens, der die bestehenden Risiko- und Governance-Rahmen nutzt
5. Durchführung einer KI-Lückenanalyse und Erstellung eines nach Prioritäten geordneten Fahrplans für die Einhaltung der Vorschriften.
6. Laufende Überwachung und Fortbildung gewährleisten

DSB	KI-Funktion
Juristisches Mandat, vollständige Stellenbeschreibung in GDPR	k.A.
Schwerpunkt: personenbezogene Daten	+ nicht-personenbezogene Daten
Gleiche Grundsätze: Fairness, Transparenz, Datenqualität, risikobasierter Ansatz	
Compliance-Funktion (Aufsicht darüber, dass personenbezogene Daten im Einklang mit den Datenschutzgesetzen verarbeitet werden)	+ Ethik
Unterstützung für DPIA, ROPAs - zur Ermittlung und Minimierung von Risiken	+ Klassifizierung, Benachrichtigung
Entwicklung und Aktualisierung von Strategien/Leitlinien	Gleiches gilt für .
Schulungen	Gleiches gilt für .
Verwaltung von DSR und Datenschutzverletzungen	Gleiches gilt für .
Berichterstattung	Gleiches gilt für .
Kontaktstelle mit Regler	Gleiches gilt für .
Profil : Recht, Compliance, Risiko, IT-Sicherheit	+ Ethik?

Nutzung der GDPR-Überschneidung

Zielsetzung	GDPR	EU-KI-Gesetz
Schutz der Grundrechte und -freiheiten/Schwerpunkt auf den Grundsätzen	Recht auf Privatsphäre, Nicht-Diskriminierung Grundsätze der Datenschutz-Grundverordnung (Artikel 5, Artikel 22)	Recht auf Privatsphäre, Nichtdiskriminierung, freie Meinungsäußerung, z. B. Schutz vor schädlicher Überwachung Grundsätze des EU-KI-Gesetzes (Erwägungsgrund 27): Menschliches Handeln und Aufsicht, technische Robustheit und Sicherheit, Datenschutz und Datenverwaltung, Transparenz, Vielfalt, Nichtdiskriminierung, Fairness, soziales und ökologisches Wohlergehen
Transparenz	Transparenz bei der Datenverarbeitung; Wahrung der Datenrechte, Mitteilung von Datenverletzungen (Artikel 12, 13 und 14)	Gebrauchsanweisungen/technische Informationen (AI-Systeme mit hohem Risiko) (Artikel 11 und 13) Bekanntmachungen über bestimmte Systeme und GPAI-Modelle/technische und sonstige Informationen über GPAI-Modelle (Artikel 50 und 53)
Risikobewertung und -minderung	Datenschutz-Folgenabschätzung (Artikel 35)	Konformitätsbewertungen durch den Anbieter (Systeme mit hohem Risiko) (Artikel 43) Bewertung der Grundrechte durch den Bereitsteller (bestimmte Hochrisikosysteme) (Artikel 27)
Menschliche Aufsicht und Rechenschaftspflicht	Menschliches Eingreifen bei bestimmten automatisierten Entscheidungen (Artikel 22)	Menschliche Aufsicht über KI-Systeme mit hohem Risiko (Artikel 14)

KI/Privatsphärenmanagement:

- **Erweitern Sie das, was Sie aus der Perspektive der Datenschutz-Governance bereits haben, z. B. Datenschutzbestimmungen, Datenschutzfolgenabschätzungen, Datenschutzrichtlinien**
- **Vergewissern Sie sich, dass das, was Sie bereits in Bezug auf den Datenschutz haben, den spezifischen KI-Herausforderungen im Zusammenhang mit dem Datenschutz entspricht.**

Kontaktdaten

Philipp Reinisch

Fieldfisher Austria
Rechtsanwalt | Partner

+43 1 928 163 40 18
philipp.reinisch@fieldfisher.com
LinkedIn: