Change Rules

100% Know-How. 0% Nonsense.

27. November 2024

reusch law

Einsatz von KI an Hochschulen und Forschungseinrichtungen – Anforderungen und praktische Umsetzung der KI-Verordnung

27.11.2024

RA Stefan Hessel, LL.M.
Salary Partner
Head of Digital Business

Agenda

1. Einführung
2. Anwendungsbereich und Forschungsausnahme
3. Adressaten und Pflichten
4. Best Practices

Einführung

Überblick und Zeitachse

Überblick

- Verordnung (EU) 2024/1689
- Produktbezogene Verordnung
- Festlegung harmonisierter Vorschriften über Künstliche Intelligenz
- Inkrafttreten: **1. August 2024**
- Übergangsfristen nach Inkrafttreten: **6 bis 36 Monate**

Timeline: Übergangsfristen nach der KI-VO

*Vorschriften zu **verbotenen KI-Systemen** anwendbar*

02.02.2025

02.08.2025

*Vorgaben für **GPAI-Systeme** anwendbar (Ausnahme: Bußgelder)*

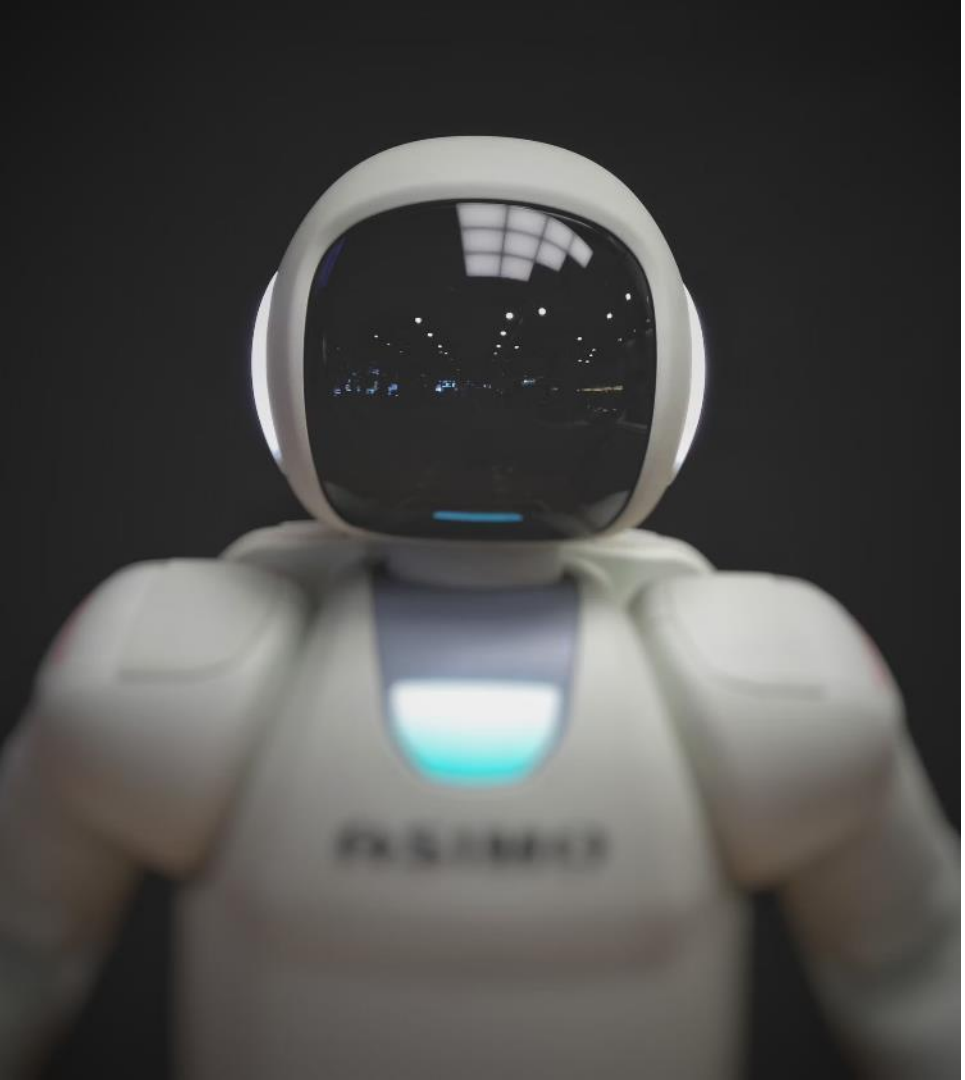
***KI-VO anwendbar** (Ausnahme: Einstufungsvorschrift für Hochrisiko-KI-Systeme)*

02.08.2026

02.08.2027

***Einstufungsvorschrift** für Hochrisiko-KI-Systeme inklusive Pflichten anwendbar (Art. 6 Abs. 1, Anhang I KI-VO)*

Anwendungsbereich und Forschungsausnahme



Anwendungsbereich

- **Sachlich**: „KI-System“
  - Maschinengestütztes System
  - Autonomer Betrieb
  - Anpassungsfähig
  - Erstellung von Ausgaben, die die Umgebung beeinflussen können

→ Weites Begriffsverständnis

- **Räumlich**: Marktortprinzip
  - KI-System oder Output im EU-Markt

Nur wenige Ausnahmen vom Anwendungsbereich

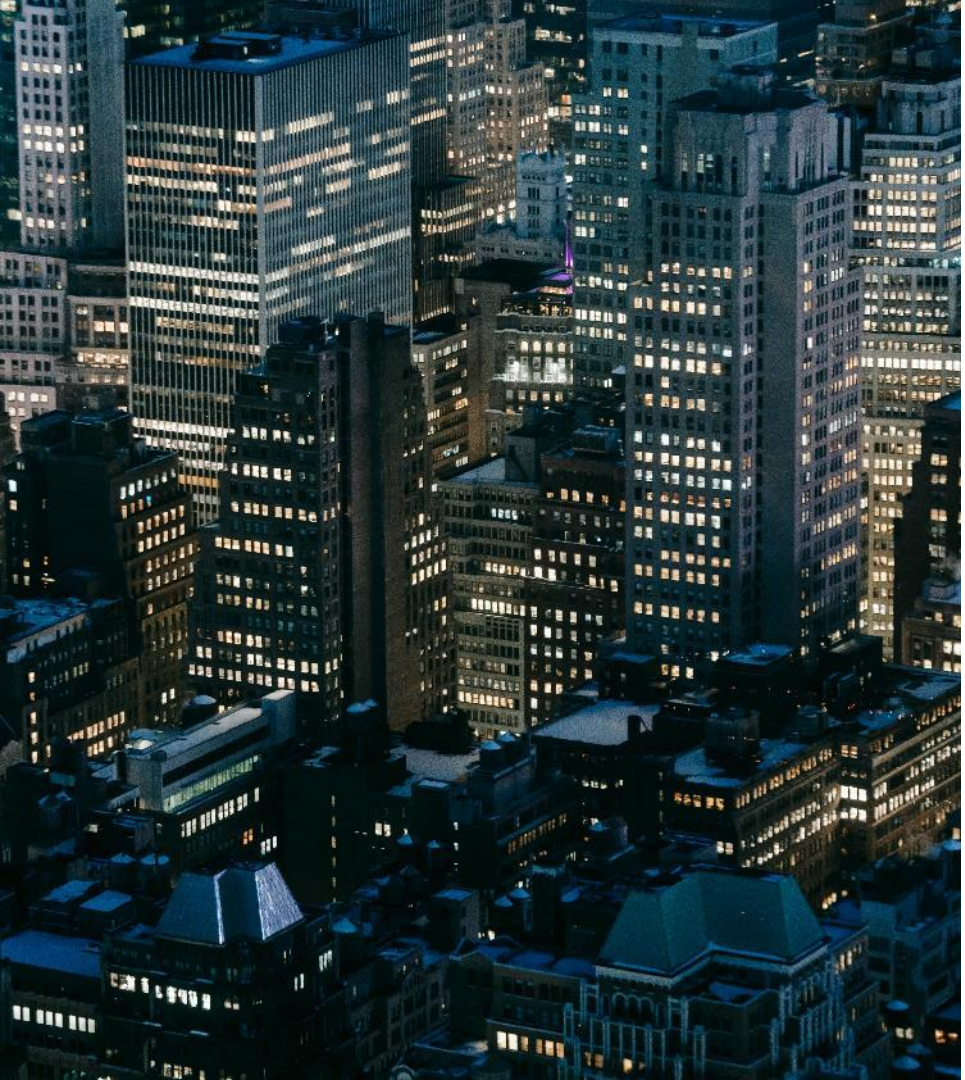
- Forschungs-, Test- und Entwicklungstätigkeiten zu KI-Systemen, bevor diese in Verkehr gebracht oder in Betrieb genommen werden (**Rückausnahme**: Tests unter Realbedingungen)
- Open Source Software (**Rückausnahme**: verbotene KI, Hochrisiko-KI-Systeme & bestimmte Transparenzpflichten anwendbar)
- Nationale Sicherheit
- Wissenschaftliche Forschung (***„Wissenschaftsprivileg“***)

„Diese Verordnung gilt nicht für KI-Systeme oder KI-Modelle, einschließlich ihrer Ausgabe, die eigens für den alleinigen Zweck der wissenschaftlichen Forschung und Entwicklung entwickelt und in Betrieb genommen werden.“

Art. 2 Abs. 6 KI-VO

Adressaten und Pflichten

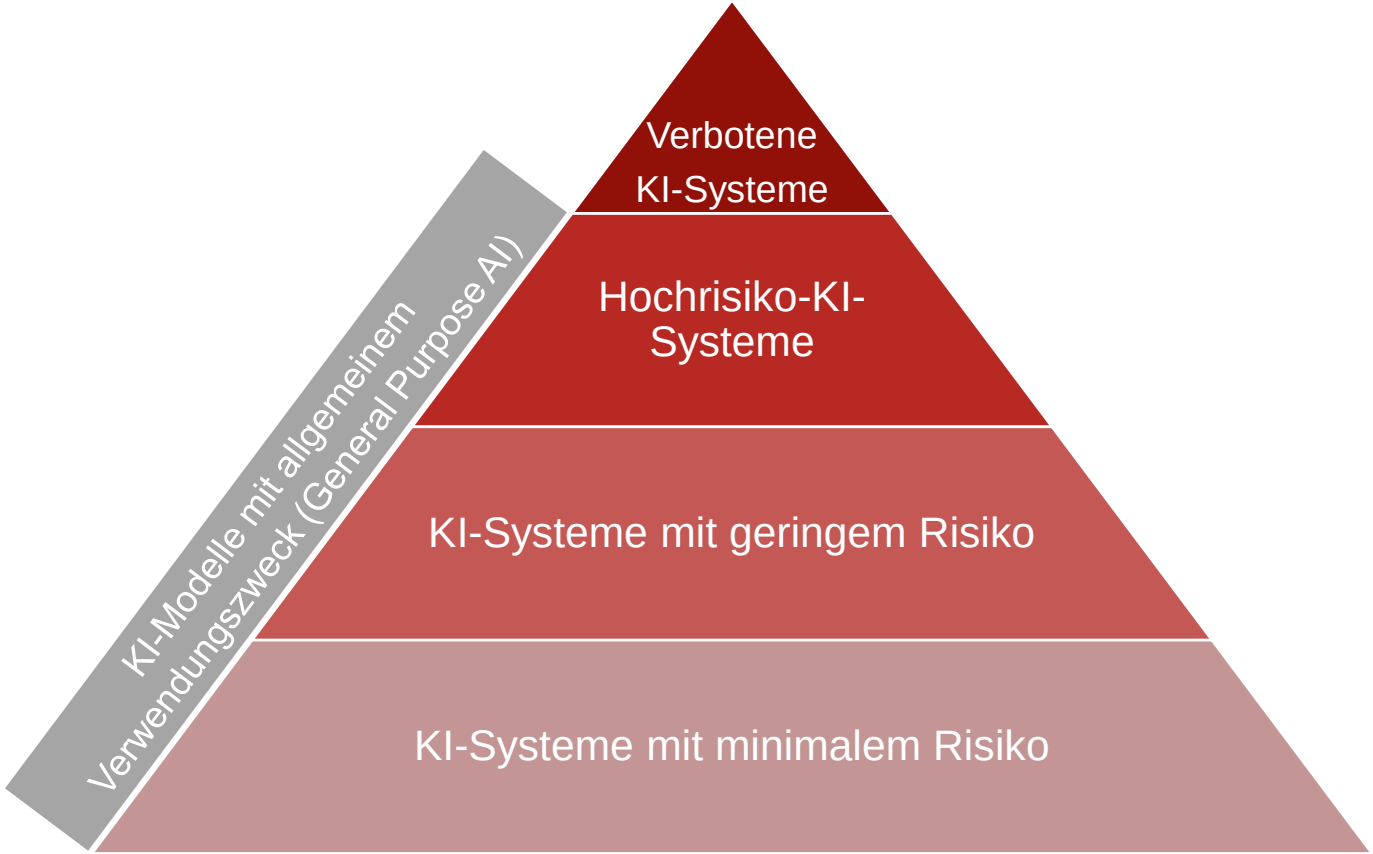
Wer muss was umsetzen?



Wichtigste Akteure der KI-VO

- **Anbieter**, die KI-Systeme in Verkehr bringen oder in Betrieb nehmen oder KI-Modelle mit allgemeinem Verwendungszweck in Verkehr bringen
- **Betreiber** von KI-Systemen
- **Produkthersteller**, die KI-Systeme zusammen mit ihrem Produkt unter ihrem eigenen Namen oder ihrer Handelsmarke in den Verkehr bringen oder in Betrieb nehmen

Risikobasierter Ansatz: Einteilung von KI in Risikogruppen



Verbotene KI-Praktiken

Verbotene KI-Praktiken

- Bestimmte KI-Praktiken aufgrund eines „**unannehmbaren Risiko**“ verboten
- Unannehmbares Risiko = Bedrohung der Werte der Union (Menschenwürde, Freiheit, Gleichheit, Demokratie, Rechtsstaatlichkeit, Grundrechte)
- Verbot der Herstellung, des Inverkehrbringens, der Inbetriebnahme oder die Verwendung der KI-Systeme
- Frist: 02.02.2025

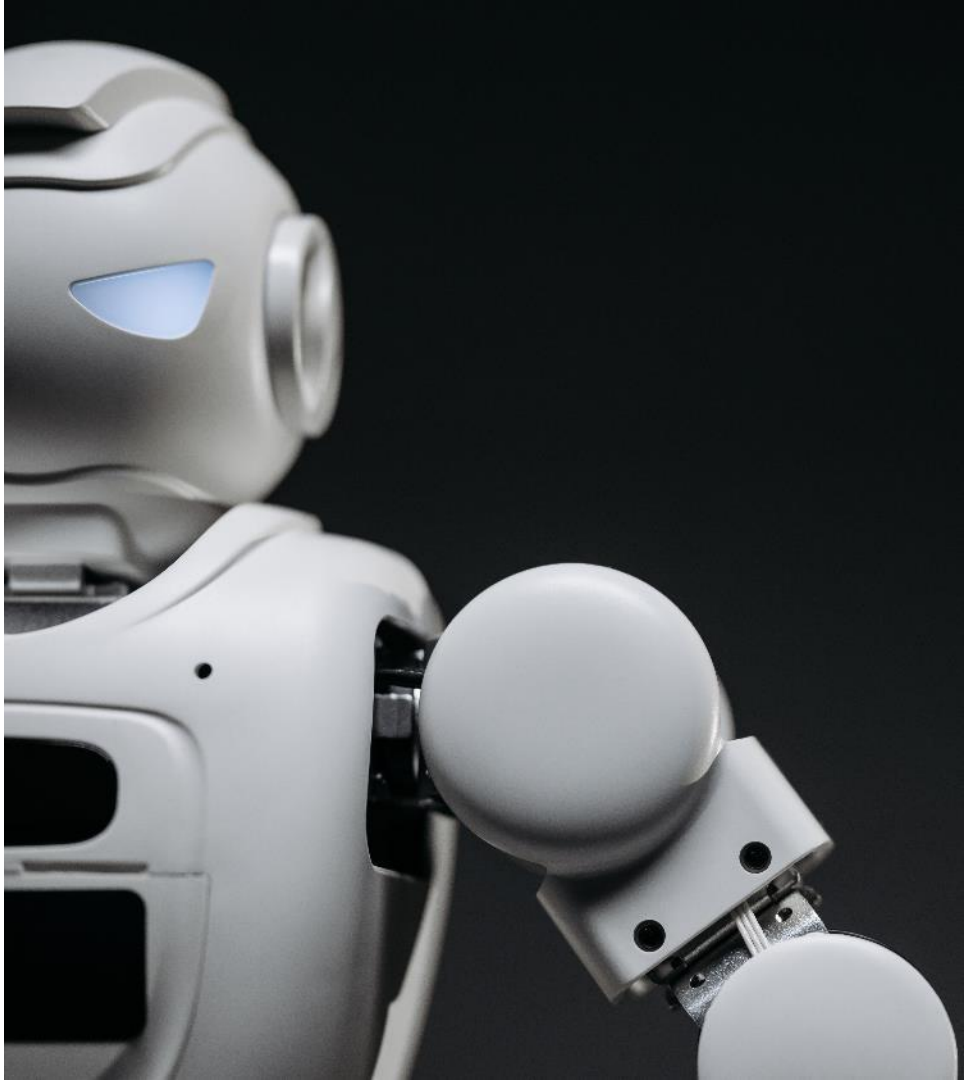
Verbotene KI-Praktiken (Beispiele)

- Techniken der unterschwelligen Beeinflussung außerhalb des Bewusstseins einer Person oder absichtlich manipulative oder täuschende Techniken
- Ausnutzung der Vulnerabilität / Schutzbedürftigkeit von Personen aufgrund ihres Alters, einer Behinderung oder einer bestimmten sozialen oder wirtschaftlichen Situation
- Bewertung / Einstufung von Personen über einen bestimmten Zeitraum auf der Grundlage ihres sozialen Verhaltens oder bekannter, abgeleiteter oder vorhergesagter persönlicher Eigenschaften oder Persönlichkeitsmerkmale mit der Folge einer Schlechterstellung oder Benachteiligung
- Erstellung oder Erweiterung von Datenbanken zur Gesichtserkennung durch das ungezielte Auslesen von Gesichtsbildern aus dem Internet oder von Überwachungsaufnahmen
- Ableitung von Emotionen einer Person am Arbeitsplatz und in Bildungseinrichtungen (Rückausnahme: Verwendung aus medizinischen Gründen oder Sicherheitsgründen)
- Biometrische Kategorisierung von Personen

Strenge Vorgaben an Hochrisiko-KI

Hochrisiko-KI-Systeme

- Als hochriskant sollten solche KI-Systeme eingestuft werden, die erhebliche schädliche Auswirkungen auf die Gesundheit, die Sicherheit und die Grundrechte von Personen in der Union haben (Ewgr. 46 KI-VO)
- Einstufung beruht auf der Zweckbestimmung
- Prüfung erfolgt durch Adressaten der KI-VO
- Begründung erforderlich, wenn KI nicht als hochriskant angesehen wird



Einstufung als Hochrisiko-KI-System (Art. 6 KI-VO)

- **Var. 1**: Hochrisiko-KI-System aufgrund Harmonisierungsvorschriften:
  - Sicherheitsbauteil oder eigenständiges Produkt
  - Unterfällt den in Anhang I aufgeführten Harmonisierungsrechtsvorschriften
  - Unterliegt einer Konformitätsbewertungspflicht durch Dritte
- Beispiele: Maschinen, Spielzeug, Funkanlagen, Medizinprodukte & In-vitro-Diagnostika
- Frist: 02.08.2027

Einstufung als Hochrisiko-KI-System (Art. 6 KI-VO)

- **Var. 2**: Hochrisiko-KI-Systeme nach Anhang III, z.B.:
  - Biometrische Fernidentifizierungssysteme
  - Sicherheitsbauteile im Rahmen der Verwaltung und des Betriebs kritischer digitaler Infrastruktur
  - KI-Systeme, die bestimmungsgemäß für die Einstellung oder Auswahl natürlicher Personen verwendet werden
- Ausnahme kein hohes Risiko → Rückausnahme: Profiling
- Frist: 02.08.2026

Anforderungen an die Konformität von Hochrisiko-KI-Systemen

- Risikomanagement während des gesamten Lebenszyklus
  - Risikoermittlung & -bewertung
  - Risikomanagementmaßnahmen
- Datenqualität, Datenverwaltung und Managementpraktiken für Trainings-, Validierungs- und Testdatensätze
  - Datensätze relevant, repräsentativ, fehlerfrei und vollständig
- Schulung
  - Allgemeine KI-Kompetenz
  - Ggf. Schulung der Betreiber

- Technische Dokumentation & Protokollierung (Anhang IV)
- Transparenz & Information (Betriebsanleitungen)
- Menschliche Aufsicht
- Genauigkeit, Robustheit und Cybersicherheit
- Pflicht zur Grundrechte-Folgenabschätzung für bestimmte Betreiber (z.B. Einrichtungen des öffentlichen Rechts, private Einrichtungen, die öffentliche Dienste erbringen)

Wechselwirkung mit dem Cyber Resilience Act

- Zusätzlich zu den Anforderungen der KI-VO:
  - Anforderungen an die Cybersicherheit von Produkten mit digitalen Elementen
  - Anforderungen an Umgang mit Sicherheitslücken
  - Nachweis der Cybersicherheitsanforderungen aus der KI-VO in der technischen Dokumentation

General Purpose AI

General Purpose AI (GPAI)

- **GPAI:**
  - KI-Modelle mit allgemeiner Verwendbarkeit
  - Erfüllung eines breiten Spektrums unterschiedlicher Aufgaben
  - In zahlreiche nachgelagerte Systeme oder Anwendungen integriert
- **Ausnahme**: Forschungs- und Entwicklungstätigkeiten oder Konzipierung von Prototypen
- Frist: 02.08.2025

GPAI und GPAI mit systemischen Risiken

GPAI:

- **Pflichten**:
  - Technische Dokumentation
  - Informations- und Kooperationspflichten ggü. Downstream-Anbietern und der EU-Kommission
  - Strategie zur Einhaltung des EU-Urheberrechts
  - Liste über urheberrechtlich geschützte Trainingsdaten
- **Ausnahme**: Open Source (Rückausnahme: GPAI mit systemischen Risiken)

GPAI mit systemischen Risiken:

- **Systemisches Risiko** = Risiko aufgrund der Fähigkeiten mit hoher Wirkkraft von GPAI und erhebliche Auswirkungen auf dem Unionsmarkt über die gesamte Wertschöpfungskette hinweg
- **Zusätzliche Pflichten**:
  - Modelevaluierung
  - Risikobewertung und -reduzierung
  - Meldung von schwerwiegenden Vorfällen inklusive Abhilfemaßnahmen
  - Cybersecurity by Design

Nachweis über „codes of practice“

KI-Systeme mit geringem oder minimalem Risiko

KI-Systeme mit geringem oder minimalem Risiko

- **KI-Systeme mit geringem Risiko:** Transparenzpflichten für bestimmte KI-Systeme, z.B.
  - KI-Systeme zur direkten Interaktion mit Personen
  - Kennzeichnung KI-generierter Inhalte (inkl. Deep-Fakes)
  - Systeme zur biometrischen Kategorisierung oder Emotionserkennung
- **KI-Systeme mit minimalem Risiko**
  - Ausarbeitung freiwilliger Verhaltenskodizies
- Frist: 02.08.2026

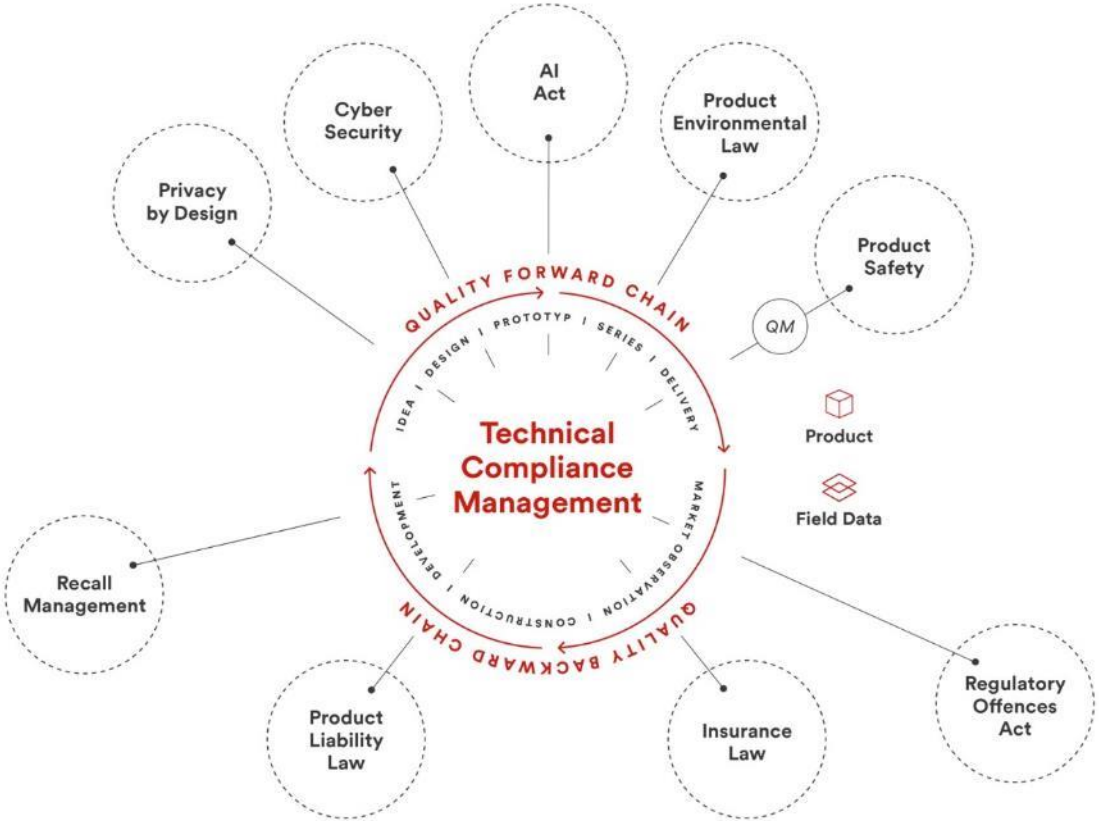
Best Practices

Umsetzung der rechtlichen Anforderungen

- Bewertung der genutzten KI-Anwendungen
- Ermittlung der anwendbaren Regelungen und Pflichten nach der KI-VO, inkl. Risikoklassifizierung
- Betrachtung weiterer rechtlicher Aspekte, insb. Datenschutz und Geistiges Eigentum
- Maßnahmen
  - Technisch (soweit möglich)
  - Organisatorisch: KI-Strategie, Richtlinien zum Einsatz von KI, Schulung und Sensibilisierung
- Monitoring

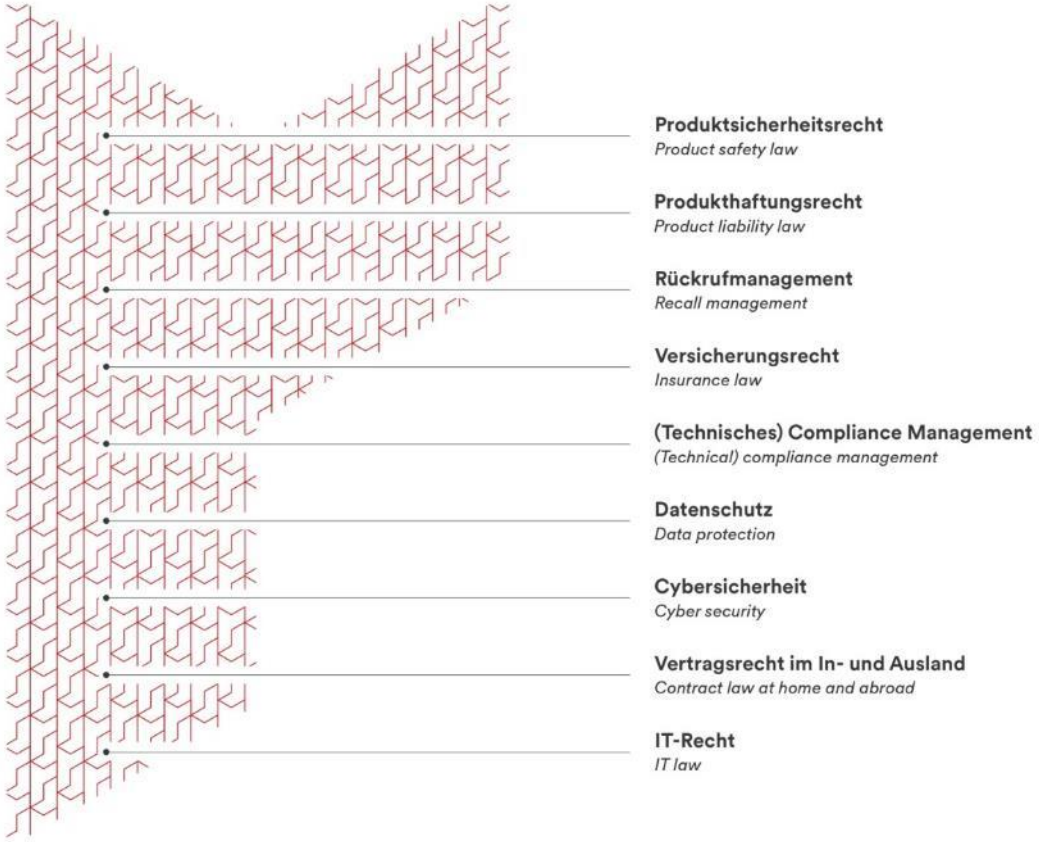
Was wir machen

Spezialisierte Services, Lösungen & Beratung.



Was wir machen

Effektivität ist nicht verhandelbar.



Was uns auszeichnet

International aktiv. In Deutschland daheim.

Dank unseres weltweiten Partnernetzwerks – vertreten in allen relevanten Industrienationen – können wir in vielen Ländern umfassende Beratung aus einer Hand anbieten.

Get in touch with us!

reusch law

Berlin
Joachimsthaler Straße 34
10719 Berlin

T + 49 30 / 2332 895 0
F + 49 30 / 2332 895 11
E info@reuschlaw.de

Saarbrücken
Stengelstraße 1
66117 Saarbrücken

T + 49 681 / 859 160 0
F + 49 681 / 859 160 11
E info@reuschlaw.de