NOERR

Compliance beim Einsatz von Künstlicher Intelligenz

Ist die Zeit reif für einen KI Compliance Officer?

RAin Marieke Luise Merkle

RA Dr. Niklas Maamar

17.08.2023

Live-Webinar: Ablauf & Hinweise

Fragen im Chat:

- Sie haben die Möglichkeit, live über den Chat Fragen zu stellen.
- Wenn Sie eine Frage stellen, bleiben Sie gegenüber den übrigen Webinar-Teilnehmern anonym. Nur die Speaker sehen die von Ihnen gestellten Fragen.
- Bitte haben Sie Verständnis dafür, dass wir ggf. nicht jede Frage beantworten können. Sie können gerne im Nachgang auf uns zukommen.

Datenschutzhinweis:

Bitte beachten Sie, dass der Veranstalter Video- und Audioaufzeichnungen des Webinars machen kann und diese ggf. im Internet verbreitet.

Präsentation:

Die Präsentation wird den Teilnehmern des Webinars im Nachgang zur Verfügung gestellt.

Übersicht

Einführung

[Code geleakt - Samsung verbietet ChatGPT für seine Angestellten - watson.ch]

[Google warnt eigene Mitarbeiter:innen vor Chatbots wie Bard - t3n.de]

Einführung

STREIT UM DATENSCHUTZ

Zoom darf Kundeninfos für KI-Training nur mit Zustimmung nutzen

AKTUALISIERT AM 08.08.2023 - 10:49

Der Videokonferenzdienst ist in der Pandemie stark gewachsen und hat viele Nutzer gewonnen. Doch nun zieht Zoom den Unmut vieler Kunden auf sich.

MERKEN 1 Min.

[Zoom: Datennutzung zum KI-Training nur mit Zustimmung der Nutzer - faz.net]

ZOOM TERMS OF SERVICE

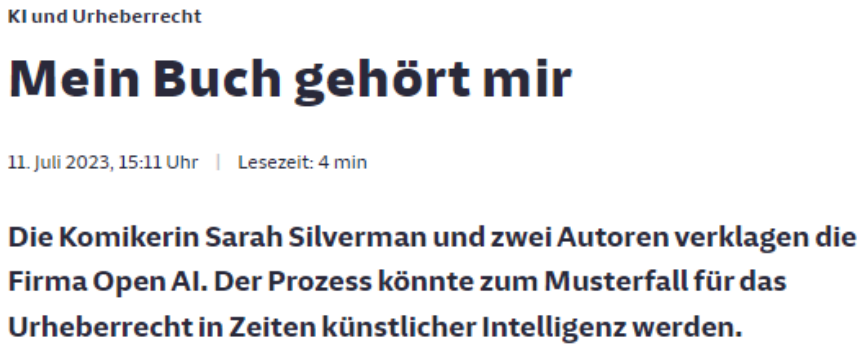
Effective Date: March 31, 2023

10.4 Customer License Grant. You agree to grant and hereby grant Zoom a perpetual, worldwide, non-exclusive, royalty-free, sublicensable, and transferable license and all other rights required or necessary to redistribute, publish, import, access, use, store, transmit, review, disclose, preserve, extract, modify, reproduce, share, use, display, copy, distribute, translate, transcribe, create derivative works, and process Customer Content and to perform all acts with respect to the Customer Content: (i) as may be necessary for Zoom to provide the Services to you, including to support the Services; (ii) for the purpose of product and service development, marketing, analytics, quality assurance, machine learning, artificial intelligence, training, testing, improvement of the Services, Software, or Zoom's other products, services, and software, or any combination thereof; and (iii) for any other purpose relating to any use or other act permitted in accordance with Section 10.3. If you have any Proprietary Rights in or to Service Generated Data or Aggregated Anonymous Data, you hereby grant Zoom a perpetual, irrevocable, worldwide, non-exclusive, royalty-free, sublicensable, and transferable license and all other rights required or necessary to enable Zoom to exercise its rights pertaining to Service Generated Data and Aggregated Anonymous Data, as the case may be, in accordance with this Agreement.

Neue Terms of Service
seit letzter Woche

Zoom does not use any of your audio, video, chat, screen sharing, attachments or other communications-like Customer Content (such as poll results, whiteboard and reactions) to train Zoom or third-party artificial intelligence models.

Einführung



KI und Urheberrecht

Mein Buch gehört mir

11. Juli 2023, 15:11 Uhr | Lesezeit: 4 min

Die Komikerin Sarah Silverman und zwei Autoren verklagen die Firma Open AI. Der Prozess könnte zum Musterfall für das Urheberrecht in Zeiten künstlicher Intelligenz werden.

KI und Urheberrecht: Autoren verklagen OpenAI - Kultur - SZ.de (sueddeutsche.de)

URHEBERRECHT

Adobe will Kunden von KI-Tools bei Klagen entschädigen

Zahlreiche Künstler klagen gegen die Anbieter von KI-Bildgeneratoren. Adobe will seine Kunden genau davor schützen.

in Pocket speichern merken

9. Juni 2023, 10:37 Uhr, Sebastian Grüner

Urheberrecht: Adobe will Kunden von KI-Tools bei Klagen entschädigen - Golem.de

Was ist Künstliche Intelligenz?

Differenzierung nach Funktionsweise

Regelbasiertes Programmieren

Programmierer gibt dem Computer Regeln vor:

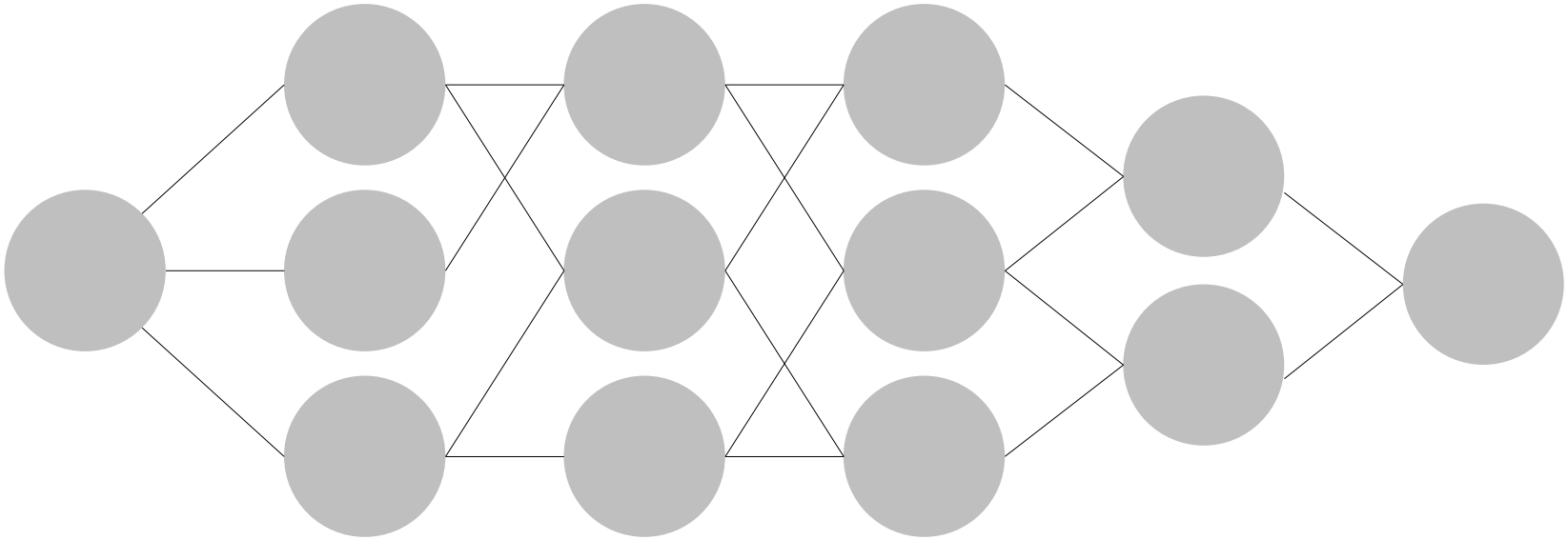
```
wenn text der email
      enthält „viagra“
      oder „Lottogewinn“
dann email == spam;
```

Erfahrungsbasiertes Lernen

Computer entwickelt die Regeln selbst:

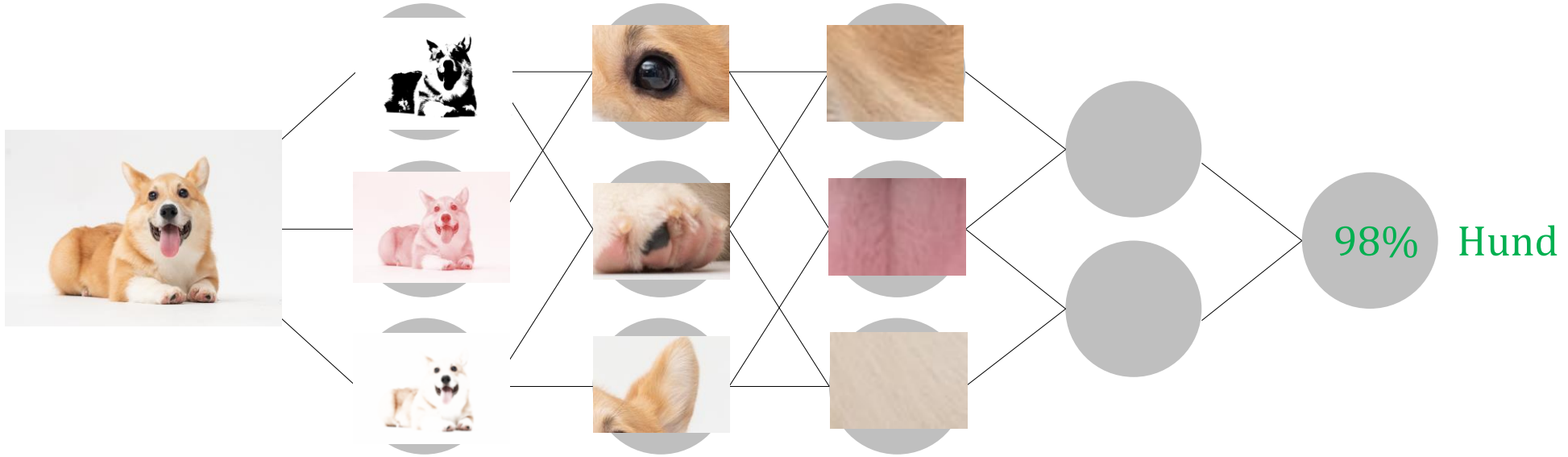
```
für bekannte spam-emails
      suche typische merkmale
      entwickle regel
wiederhole;
```

Was ist Künstliche Intelligenz?



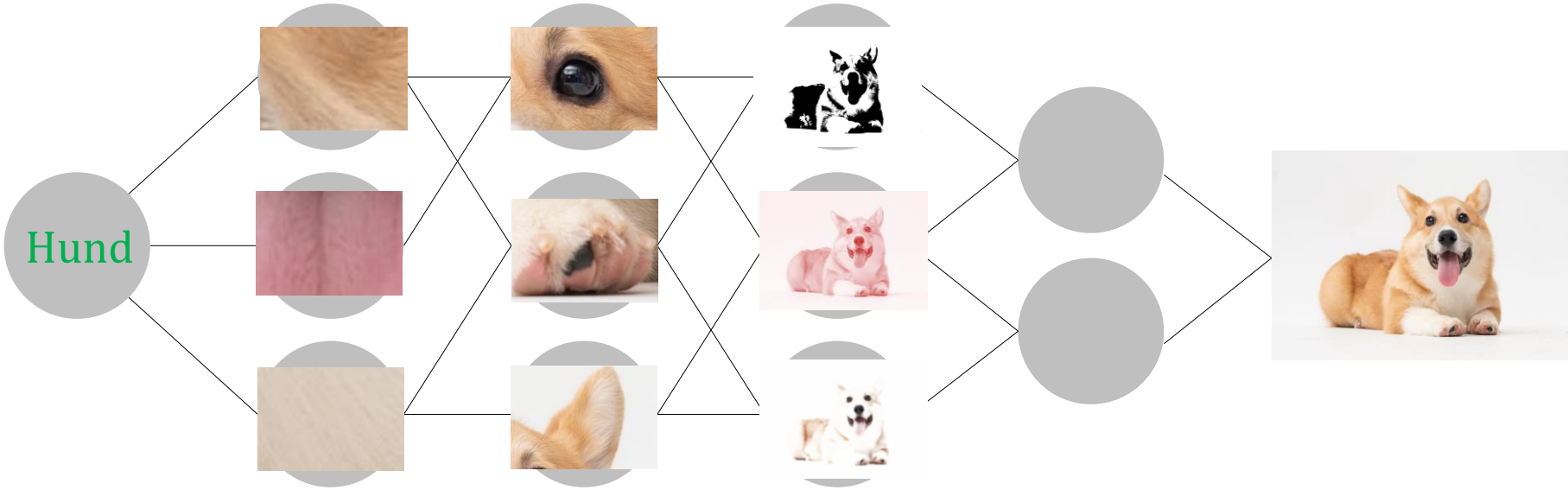
Input | **Gewinnung von Einzelinformationen („Layers“)** | **Output**

Was ist prädiktive Künstliche Intelligenz?



Input | **Gewinnung von Einzelinformationen („Layers“)** | **Output**

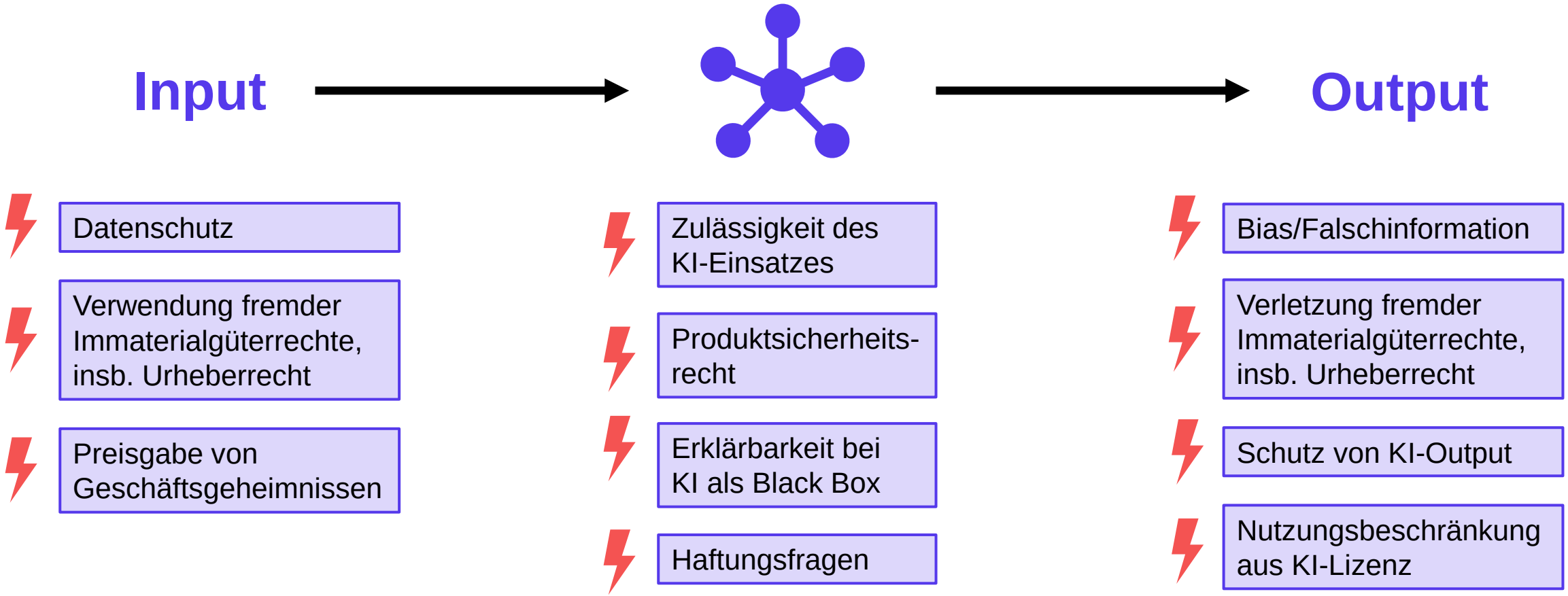
Was ist generative Künstliche Intelligenz?



Input | **Erzeugung von Einzelinformationen („Layers“)** | **Output**

Welche rechtlichen Risiken bestehen beim Einsatz von KI?

Rechtliche Risken beim Einsatz von KI



Input – Verwenden fremder Trainingsdaten

Personenbezogene Daten

↓

DSGVO zu beachten

- Vertragliche Erlaubnis (Einwilligung)
  Hohe Anforderungen an Freiwilligkeit und Informiertheit der Einwilligung, insbesondere bei sensiblen Daten
- Gesetzliche Erlaubnis
  Art. 6 lit. b DSGVO (Erfüllung des Vertragszwecks)
  Art. 6 lit. c DSGVO (rechtliche Verpflichtung)
  Anonymisierung

Geschützte Werke

↓

UrhG zu beachten

- Vertragliche Erlaubnis (Lizenz)
  Lizenzierung von Werken ist oft unpraktikabel insbesondere wegen benötigter Datenmenge
- Gesetzliche Erlaubnis
  § 44a UrhG (vorübergehende Vervielfältigung)
  § 44b UrhG (kommerzielles Text und Data Mining)
  § 60d UrhG (wissenschaftliches Text und Data Mining)

Input – Schutz eigener Daten

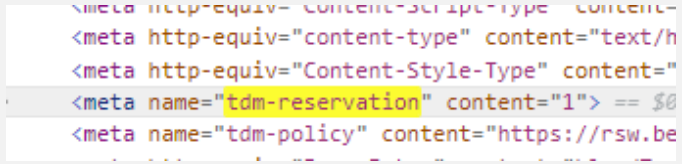
… Compliance kann auch heißen, die eigenen Daten davor zu schützen, dass sie als Trainingsdaten für fremde KI verwendet werden

Veröffentlichte Daten

↓

Nutzungsvorbehalt prüfen

- Nutzung eigener Daten für KI-Training durch Dritte ausschließen
  - § 44b Abs. 3 UrhG: „in maschinenlesbarer Form“



Vertrauliche Daten

↓

Bei Weitergabe an Dritte Daten(nutzungs)rechte klären

- Recht an Daten vertraglich zuordnen
- Datennutzungsrechts des Dritten beschränken
  z.B. Verarbeitung in KI-Systemen des Dritten durch „AI-NDA“ verhindern

Interne Geschäftsgeheimnisse

↓

Preisgabe durch eigene Mitarbeiter verhindern

- Vertragsbedingungen von eingesetzten KI-Tools prüfen
  Welche Daten werden verarbeitet?
  Zu welchem Zweck?
- Ggf. On-Premise-Lösungen anbieten, um Kontrolle über Daten zu behalten

Input – Schutz eigener Daten

Interne Geschäftsgeheimnisse

↓

Preisgabe durch eigene Mitarbeiter verhindern

Compliance-Risiko:
Sonst droht der Verlust des Geheimnisschutzrechts wegen fehlender Geheimhaltungsmaßnahmen

Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG)

§ 2 Begriffsbestimmungen

Im Sinne dieses Gesetzes ist

1. Geschäftsgeheimnis

   eine Information

   a) die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich ist und daher von wirtschaftlichem Wert ist und

   b) die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und

   c) bei der ein berechtigtes Interesse an der Geheimhaltung besteht;

– Zulässigkeit des Einsatzes von KI-Systemen

- Bereits heute ist der Einsatz von KI für bestimmte Zwecke oder in bestimmten Bereichen unzulässig bzw. unterliegt gewissen Voraussetzungen

- **Allgemeine Einschränkungen und Anforderungen:**

  - **Art. 22 DSGVO** (Automatisierte Entscheidungen im Einzelfall)
    - Verbot von vollautomatisierten Entscheidungen mit rechtlicher Wirkung
    - Relevant insbesondere beim Einsatz von Automatic Decision Making Systems für Kreditgewährung

  - **Mitwirkungs- und Informationsrechte des Betriebsrates**
    - Pflicht zur Information des Betriebsrates über „Arbeitsverfahren und Arbeitsabläufen einschließlich des Einsatzes von Künstlicher Intelligenz“ nach § 90 Abs. 1 Nr. 3 BetrVG
    - Recht zur Einbeziehung von Sachverständigen gemäß § 80 Abs. 3 S. 2 BetrVG
    - Mitbestimmungsrecht, z.B. § 95 Abs. 2a BetrVG, § 87 Abs. 1 Nr. 6 BetrVG
    - Ggf. Betriebsänderung gemäß §§ 111, 112 f. BetrVG

– Zulässigkeit des Einsatzes von KI-Systemen

➢ Sektorspezifische Einschränkungen und Anforderungen:

Automobilindustrie

- **§ 1a StVG i.V.m. AFGBV**

  Zulassung und Typengenehmigung für hoch- oder vollautomatisierte Kraftfahrzeuge
- **§ 63a StVG**

  Datenverarbeitung bei hoch- oder vollautomatisierten Kraftfahrzeugen

Banken/Finanzdienstleister

- **MaRisk Modul AT 4.3.5**

  Data Governance und „Human in the loop“
- **BaFin Prinzipienpapier für den Einsatz von Algorithmen in Entscheidungsprozessen**

  Fairness und Nachvollziehbarkeit beim Einsatz von KI

Versicherungen

- **§ 37 BDSG**

  Zulässigkeit von (stattgebenden) automatisierten Versicherungsentscheidungen
- **EIOPA Governance Principles for Artificial Intelligence**

  Transparenz, Belastbarkeit und menschliche Aufsicht von KI

Medizinproduktehersteller

- **MDR und IVDR**

  Sicherheit und Leistungsfähigkeit von Algorithmen, Wiederholbarkeit und Nachprüfbarkeit der Ergebnisse
- **IG-NB Fragenkatalog Künstliche Intelligenz bei Medizinprodukten**

Output – Nutzung und Verwertung von KI-Output

KI-generierte „Werke“ sind nach deutschem Urheberrecht grds. nicht schutzfähig und gemeinfrei

- Risiko: Kunden und Wettbewerber können KI-Output kopieren und selbst nutzen
  - Bedeutung von Geheimhaltung steigt, wenn KI-Output kommerziell verwertet werden sollen

- Risiko: „Exklusive Rechte“ an gemeinfreiem KI-Output einzuräumen, ist unmöglich
  - Verträge prüfen, wenn Dritte KI-Output liefern (inbound)
  - Verträge prüfen, wenn KI-Output nach außen geliefert wird (outbound)
  - Abläufe prüfen, wenn Mitarbeiter KI-Tools nutzen

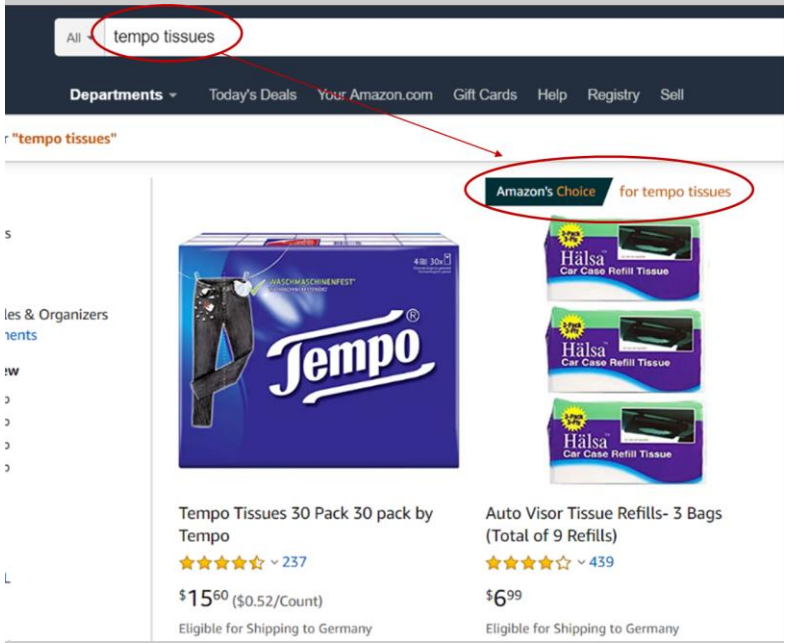
- Risiko: Nutzungsvorgaben für KI-Output wirken oft nur sehr beschränkt
  - „Lizenz“ stellt eigentlich eine schuldrechtliche Beschränkung der Nutzungsmöglichkeit dar
  - Nutzungsvorgaben für KI-Output sind nur inter partes durchsetzbar

Output – Rechtsverletzung durch KI

GitHub Copilot

Kopie durch KI
z.B. Übernahme von fremden Trainingsdaten im KI-Output

Kartell durch KI
z.B. koordinierte automatisierte Preissetzung durch Einsatz von KI



Markenverletzung durch KI
z.B. Empfehlung (oder automatischer Kauf) von Produkten des Wettbewerbers

Ausblick auf die Compliance-Anforderungen nach der zukünftigen KI-VO

KI-VO: Risikobasierte Regulierung

Anwendungsbereich

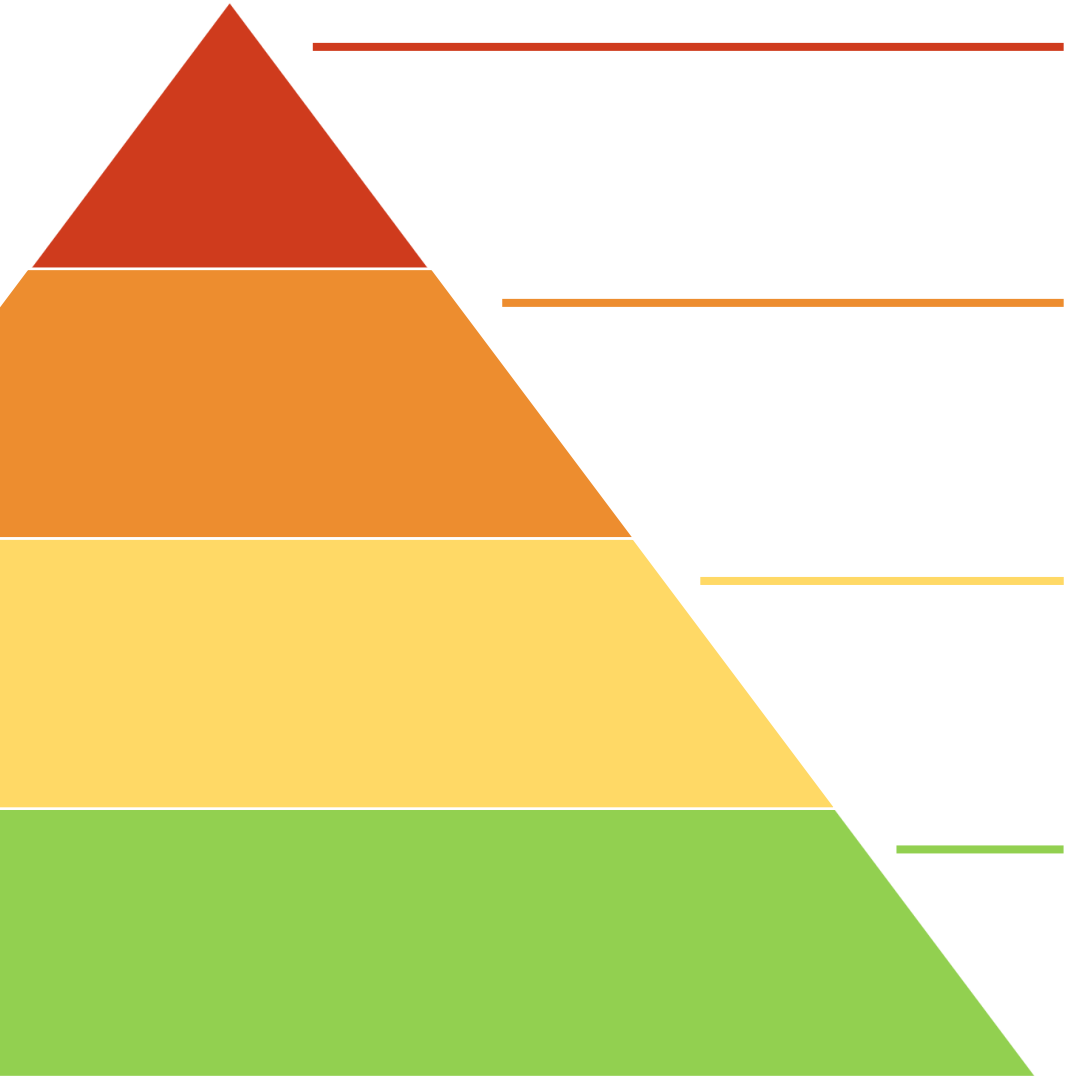
Gilt für alle KI-Systeme, die in der EU entwickelt oder verwendet werden (Marktortprinzip wie in der DSGVO)

Adressaten: Entwickler und berufliche Nutzer von KI, private Nutzer bisher ausgenommen

Risikobasierter Ansatz

Es muss künftig präventiv geprüft werden, welche Risiken von KI-Anwendungen ausgehen können. Je nach Befund ist ein unterschiedliches Maß an Schutzvorkehrungen notwendig.

KI-VO: Risikobasierte Regulierung



KI-Verbote (Art. 5) – Unannehmbares Risiko

= verboten (darf nicht in der EU angeboten oder genutzt werden)

Hochrisiko-KI (Art. 6 – 51) – Hohes Risiko

= präventives Risikomanagement vor Einsatz verpflichtend

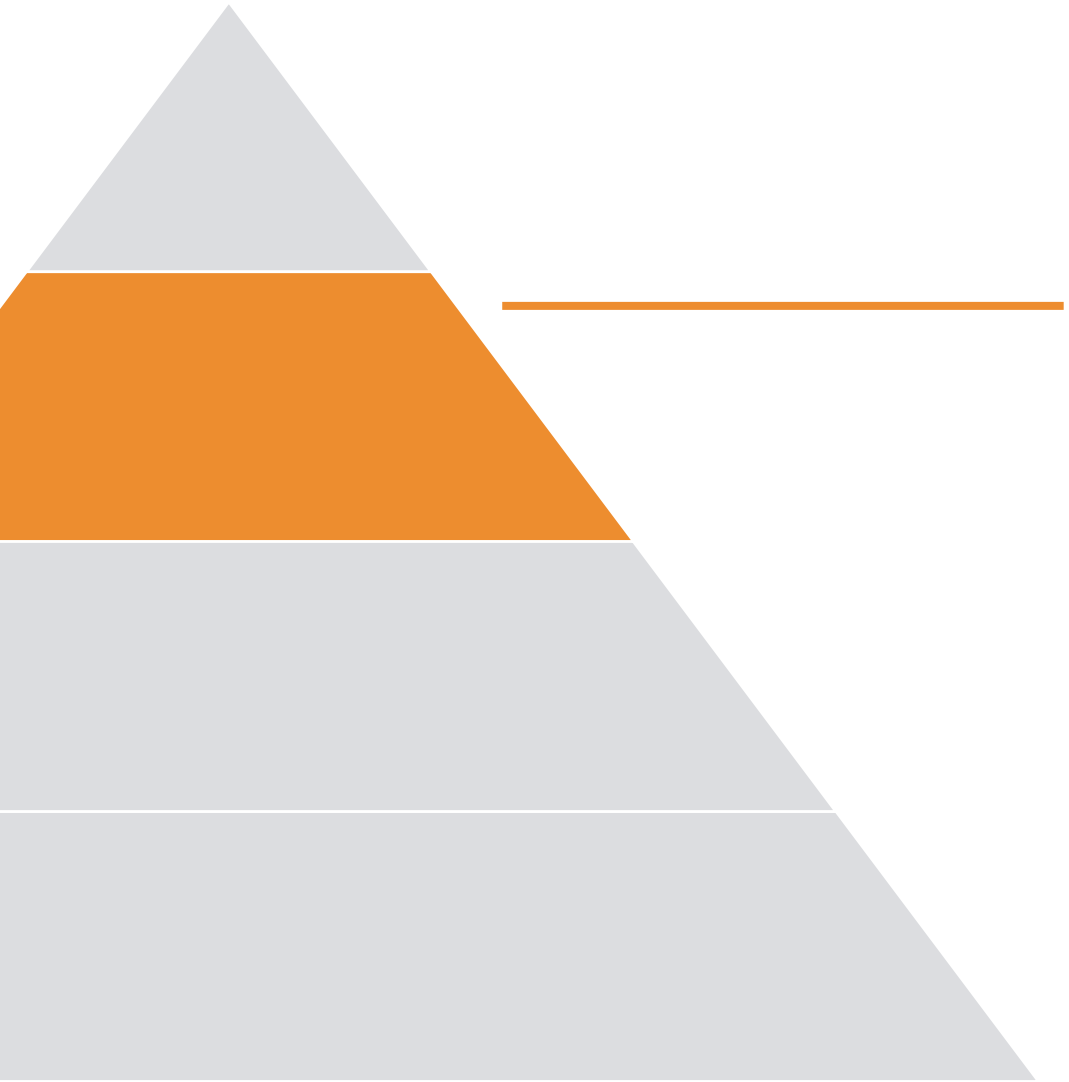
Besondere Transparenzpflichten (Art. 52) – Mittleres Risiko

= Hinweis an Menschen, wenn sie mit KI interagieren

Voluntary Code of Conduct (Art. 69) – Minimales Risiko

= ohne Einschränkungen erlaubt

Pflichten bei Hochrisiko-KI

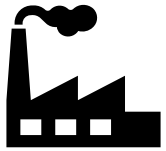


Hochrisiko-KI (Art. 6 - 51) – Anwendungsbereich

- KI als **Produkt oder sicherheitsrelevante Komponente** von regulierten Produkten nach Annex II, die bereits heute einer Zulassungspflicht unterliegen
  - Industriemaschinen und Schutzausrüstung
  - Spielzeuge
  - Verkehrsmittel (Autos, Motorräder, Schiffe, Flugzeuge, Züge)
  - Medizinprodukte
  - Funkgeräte und Kabel

- Einsatz von KI in **besonders sensiblen Bereichen** nach Annex III
  - Biometrische Identifikation
  - Kritische Infrastruktur
  - Zugang zu Bildung und staatlichen Leistungen
  - Bewertung von Prüfungen oder Arbeitsleistungen
  - Einstellung und Entlassung von Arbeitnehmern
  - Prüfung der Kreditwürdigkeit
    (Parlament und Rat: sowie Abschluss und Preis von Kranken- und Lebensversicherungen)
  - Strafverfolgung und Migration
  - Unterstützung von Gerichten

Adressaten der Pflichten nach der KI-Verordnung



Anbieter

Nutzer / Betreiber

Bevollmächtigter

Einführer

Händler

„eine natürliche oder juristische Person, Behörde, […], die ein KI-System **entwickelt oder entwickeln lässt**, um es **unter ihrem eigenen Namen** oder ihrer eigenen Marke – **entgeltlich oder unentgeltlich** – in Verkehr zu bringen oder in Betrieb zu nehmen“

Adressaten der Pflichten nach der KI-Verordnung

Anbieter

Nutzer / Betreiber

„eine natürliche oder juristische Person, Behörde, […], die ein **KI-System in eigener Verantwortung verwendet**, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet“

Bevollmächtigter

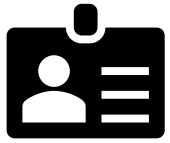
Einführer

Händler

Adressaten der Pflichten nach der KI-Verordnung

Anbieter

Nutzer / Betreiber



Bevollmächtigter

„eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, **die vom Anbieter eines KI-Systems schriftlich dazu bevollmächtigt wurde,** in seinem Namen die in dieser Verordnung festgelegten **Pflichten zu erfüllen bzw. Verfahren durchzuführen**“

Einführer

Händler

Adressaten der Pflichten nach der KI-Verordnung

Anbieter

Nutzer / Betreiber

Bevollmächtigter

Einführer

„eine in der Union ansässige oder niedergelassene natürliche oder juristische Person, die ein **KI-System, das den Namen oder die Marke einer außerhalb der Union ansässigen oder niedergelassenen natürlichen oder juristischen Person trägt**, **in der Union in Verkehr bringt oder in Betrieb nimmt**“

Händler

Adressaten der Pflichten nach der KI-Verordnung

Anbieter

Nutzer / Betreiber

Bevollmächtigter

Einführer

Händler

„eine natürliche oder juristische Person in der Lieferkette, die ein KI-System **ohne Änderung seiner Merkmale auf dem Unionsmarkt bereitstellt**, mit Ausnahme des Herstellers oder des Einführers“

Pflichten des Anbieters (Art. 16 KI-VO)

Anbieter | Nutzer / Betreiber | Bevollmächtigter | Einführer | Händler

Vorgelagerte Compliance

Data und Data Governance, Art. 10
Technische Dokumentation, Art. 11

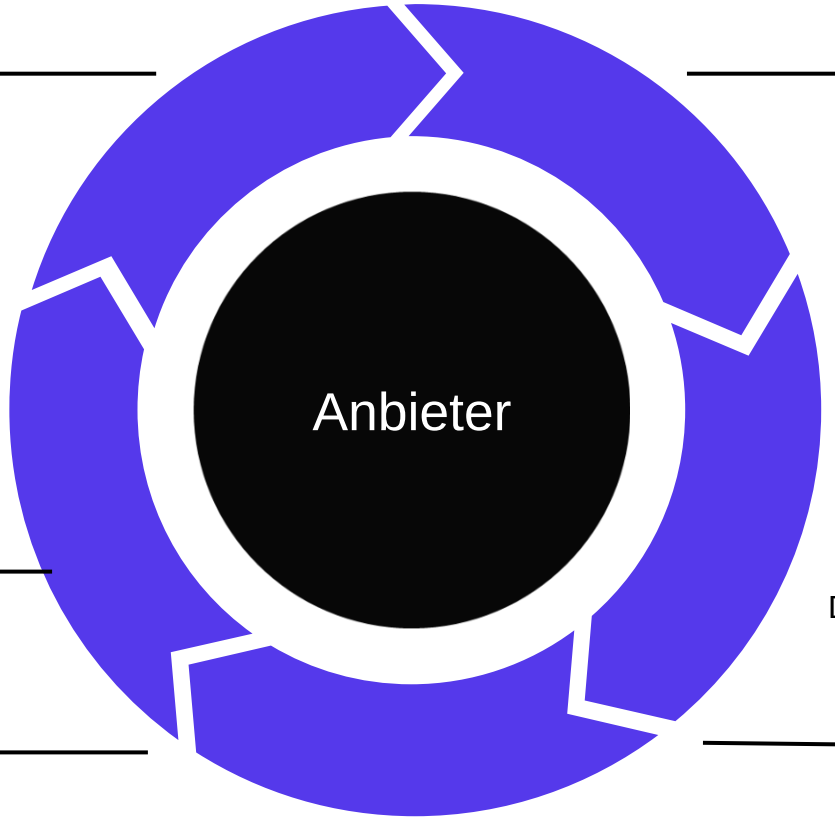
Einsatz des KI-Systems

Protokollierung, Art. 12
Transparenz, Art. 13
Menschliche Aufsicht, Art. 14
Genauigkeit, Robustheit, Cybersecurity, Art. 15

Allgemeine Pflichten

Ethische Grundsätze, Art. 4a Abs. 1, 2
KI-Kompetenz, Art. 4b Abs. 2

KI-Basismodelle



QM- und Risikomanagement

QM-System, Art. 17
Risikomanagementsystem, Art. 9
Beobachtungspflichten, Art. 17, 61

Pflichten bzgl. Aufsicht

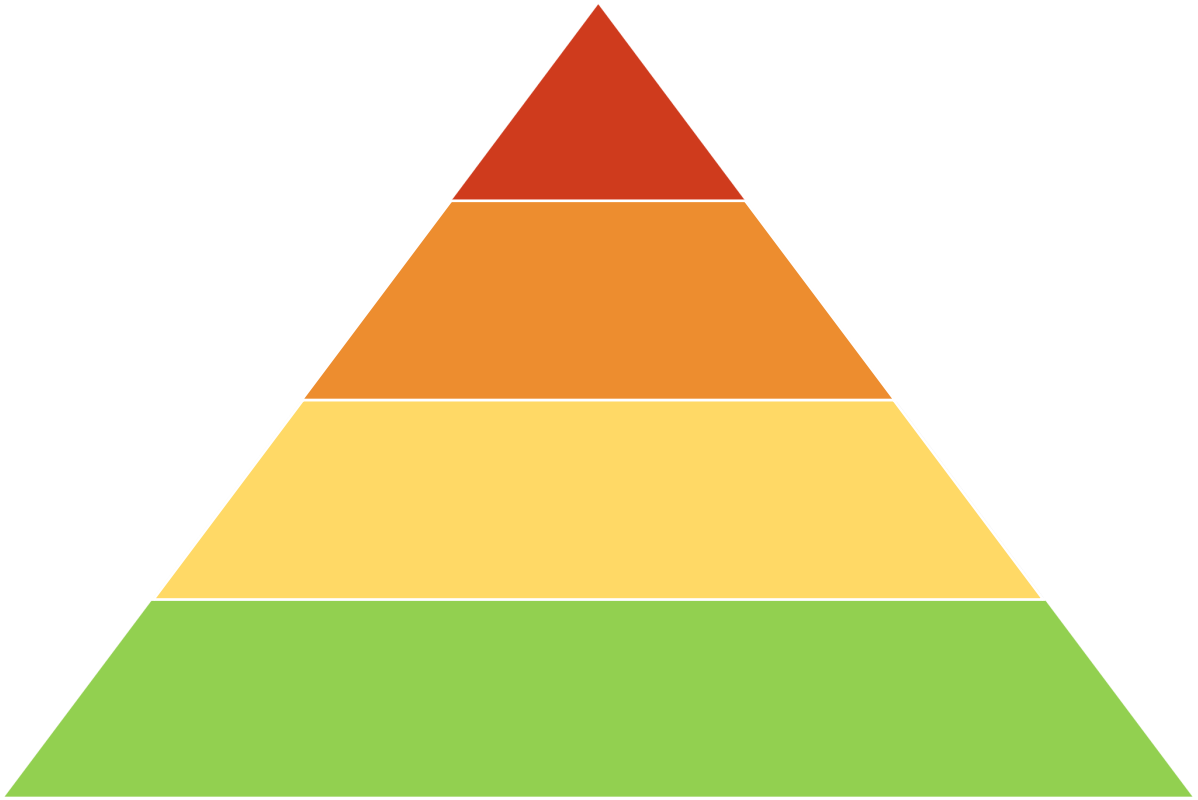
Registrierung, Art. 16 lit. f, 51
Konformitätsbewertungsverf, Art.43
CE-Kennzeichnung, Art. 49
Meldepflicht, Art. 16 lit. h
Korrekturmaßnahmen, Art. 16 lit. g
Dokumentation/Kooperation, Art. 16 lit. j

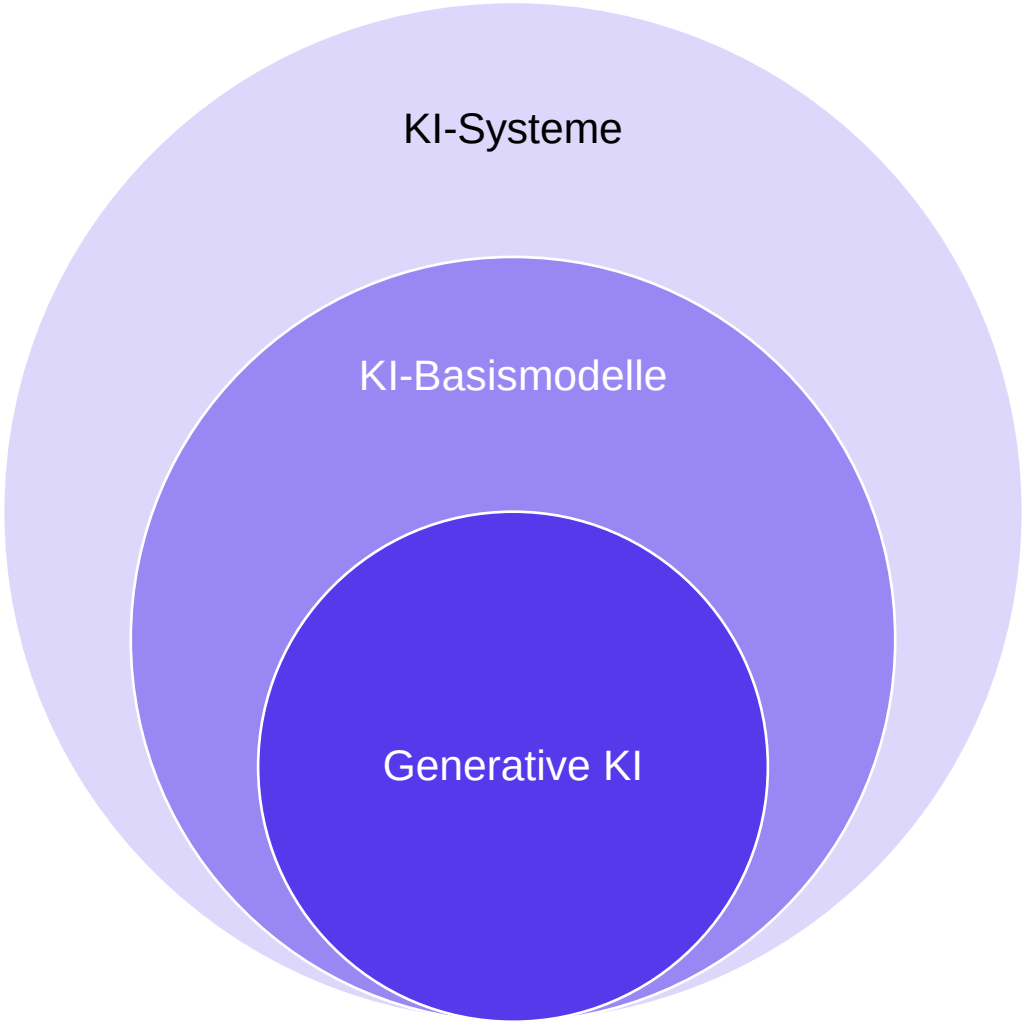
Generative KI

NOERR

Pflichten im Fall von KI-Basismodellen sowie generativer KI

Regelungsstruktur nach dem Änderungsentwurf des Parlaments





Pflichten des Anbieters (Art. 16 KI-VO)

Anbieter | Nutzer / Betreiber | Bevollmächtigter | Einführer | Händler

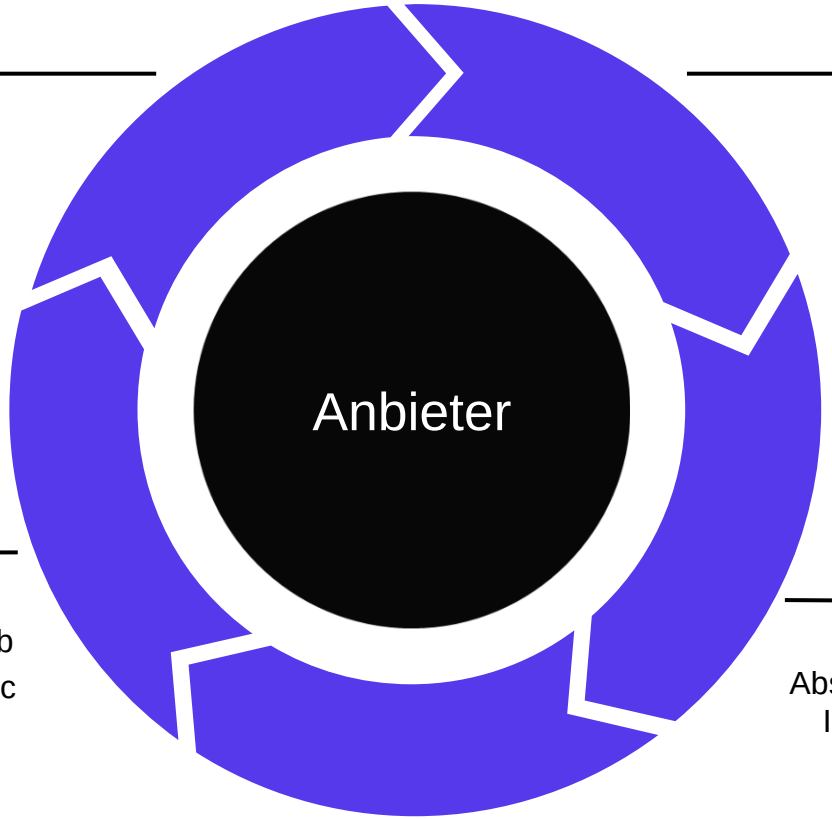
Vorgelagerte Compliance

QM- und Risikomanagement

Einsatz des KI-Systems

Pflichten bzgl. Aufsicht

Allgemeine Pflichten



KI-Basismodelle

Risikominimierung, Art. 28b Abs. 2 lit. a
Data-Governance-Maßnahmen, Art. 28b Abs. 2 lit. b
Sicherstellung der Performance, Art. 28b Abs. 2 lit. c
Nachhaltige Entwicklung, Art. 28b Abs. 2 lit. d
Dokumentation, Art. 28b Abs. 2 lit. e
Qualitätsmanagement, Art. 28b Abs. 2 lit. f
Registrierungspflicht, Art. 28b Abs. 2 lit. g

Generative KI

Transparenzpflichten, Art. 28b Abs. 4 lit. a
Absicherung gegen illegale Inhalte, Art. 28b Abs. 4 lit. b
Informationspflicht bzgl. urheberrechtlich geschützter Trainingsdaten, Art. 28b Abs. 4 lit. c

NOERR

Adressaten der Pflichten nach der KI-Verordnung

Anbieter

Nutzer / Betreiber

Bevollmächtigter

Einführer

Händler

- Art. 4a KI-VO: Ethische Grundsätze
- Art. 4b KI-VO: KI-Kompetenz
- **TOM zur Einhaltung der Gebrauchsanweisung**, Art. 29 Abs. 1 KI-VO
- Bei Kontrolle über das System (Art. 29 Abs. 1a KI-VO)
  - Sicherstellung der menschlichen Aufsicht (Art. 14 KI-VO)
  - Sicherstellung der Kompetenz des Personals
  - Sicherstellung der Maßnahmen zur Robustheit (Art. 15 KI-VO)

  → **Verlagerung der betriebsbezogenen Pflichten**
- **Eingabedaten** „relevant und ausreichend repräsentativ“ (nicht fehlerfrei!), Art. 19 Abs. 3 KI-VO
- **Informationspflicht** ggü. Anbieter, Art. 29 Abs. 4 KI-VO
- **Protokollierungspflicht**, Art. 29 Abs. 5 KI-VO
- **Konsultierung der Arbeitnehmervertreter**, Art. 29 Abs. 5a KI-VO
- **Für bestimmte Systeme**: Risikofolgeabschätzung, Art. 29 Abs. 6a, 29a KI-VO

Adressaten der Pflichten nach der KI-Verordnung

Anbieter

Nutzer / Betreiber

Bevollmächtigter

Einführer

Händler

- Formelle Prüfpflicht, Art. 26 Abs. 1 KI-VO
  - **Konformitätsbewertungs-verfahren**
  - Technische Dokumentation
  - Bevollmächtigter Vertreter
- Absehen von Inverkehrbringen bei Zweifeln an Konformität
- Angabe des Handelsnamen, Art. 26 Abs. 3 KI-VO

Adressaten der Pflichten nach der KI-Verordnung

Anbieter

Nutzer / Betreiber

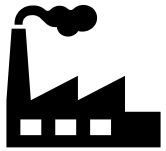
Bevollmächtigter

Einführer

Händler

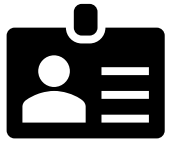
- Formelle Prüfpflicht, Art. 27 Abs. 1 KI-VO
  - CE-Kennzeichnung
  - Dokumentation/Gebrauchs-anweisung
  - Erfüllung der Pflichten nach KI-VO durch Anbieter/Einführer
- Keine Bereitstellung bei Vermutung eines Compliance-Verstoßes
- Korrekturpflicht zur Herstellung der Konformität mit KI-VO, Art. 27 Abs. 4 KI-VO

Übertragung der Anbieterpflichten auf andere Akteure



Anbieter

Nutzer / Betreiber



Bevollmächtigter

Einführer

Händler

Parlamentsentwurf, Art. 28 KI-VO:

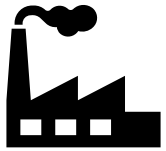
„In den folgenden Fällen gelten **Händler, Einführer, Betreiber oder sonstige Dritte als Anbieter** eines Hochrisiko-KI-Systems für die Zwecke dieser Verordnung und unterliegen den Anbieterpflichten gemäß Artikel 16:

a) wenn sie **ihren Namen oder ihr Markenzeichen** auf ein Hochrisiko-KI-System setzen, das bereits in Verkehr gebracht oder in Betrieb genommen wurde;

b) wenn sie eine **wesentliche Änderung an einem Hochrisiko-KI-System vornehmen**, das bereits in Verkehr gebracht oder in Betrieb genommen wurde, und zwar so, dass es weiterhin ein Hochrisiko-KI-System im Sinne von Artikel 6 bleibt;

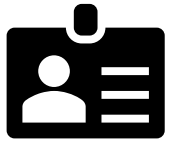
c) wenn sie ein **KI-System**, einschließlich eines KI-Systems für allgemeine Zwecke, das nicht als Hochrisiko-KI-System eingestuft wurde und bereits in Verkehr gebracht oder in Betrieb genommen wurde, **so wesentlich verändern, dass das KI-System zu einem Hochrisiko-KI-Syste**m im Sinne von Artikel 6 wird.“

Übertragung der Anbieterpflichten auf andere Akteure



Anbieter

Nutzer / Betreiber



Bevollmächtigter

Einführer

Händler

Parlamentsentwurf, Art. 28 KI-VO:

„In den folgenden Fällen gelten **Händler, Einführer, Betreiber oder sonstige Dritte als Anbieter** eines Hochrisiko-KI-Systems für die Zwecke dieser Verordnung und unterliegen den Anbieterpflichten gemäß Artikel 16:

a) wenn sie **ihren Namen oder ihr Markenzeichen** auf ein Hochrisiko-KI-System setzen, das bereits in Verkehr gebracht oder in Betrieb genommen wurde;
→ Abgrenzungsfragen bei Einbindung fremder KI-Systeme in eigene Produkte/Services (Art. 24 KI-VO)

b) wenn sie eine **wesentliche Änderung an einem Hochrisiko-KI-System vornehmen**, das bereits in Verkehr gebracht oder in Betrieb genommen wurde, und zwar so, dass es weiterhin ein Hochrisiko-KI-System im Sinne von Artikel 6 bleibt;
→ Wesentliche Änderung (Art. 3 Nr. 23 KI-VO, Erwägungsgrund 66): Vorhersehbarkeit der Änderung

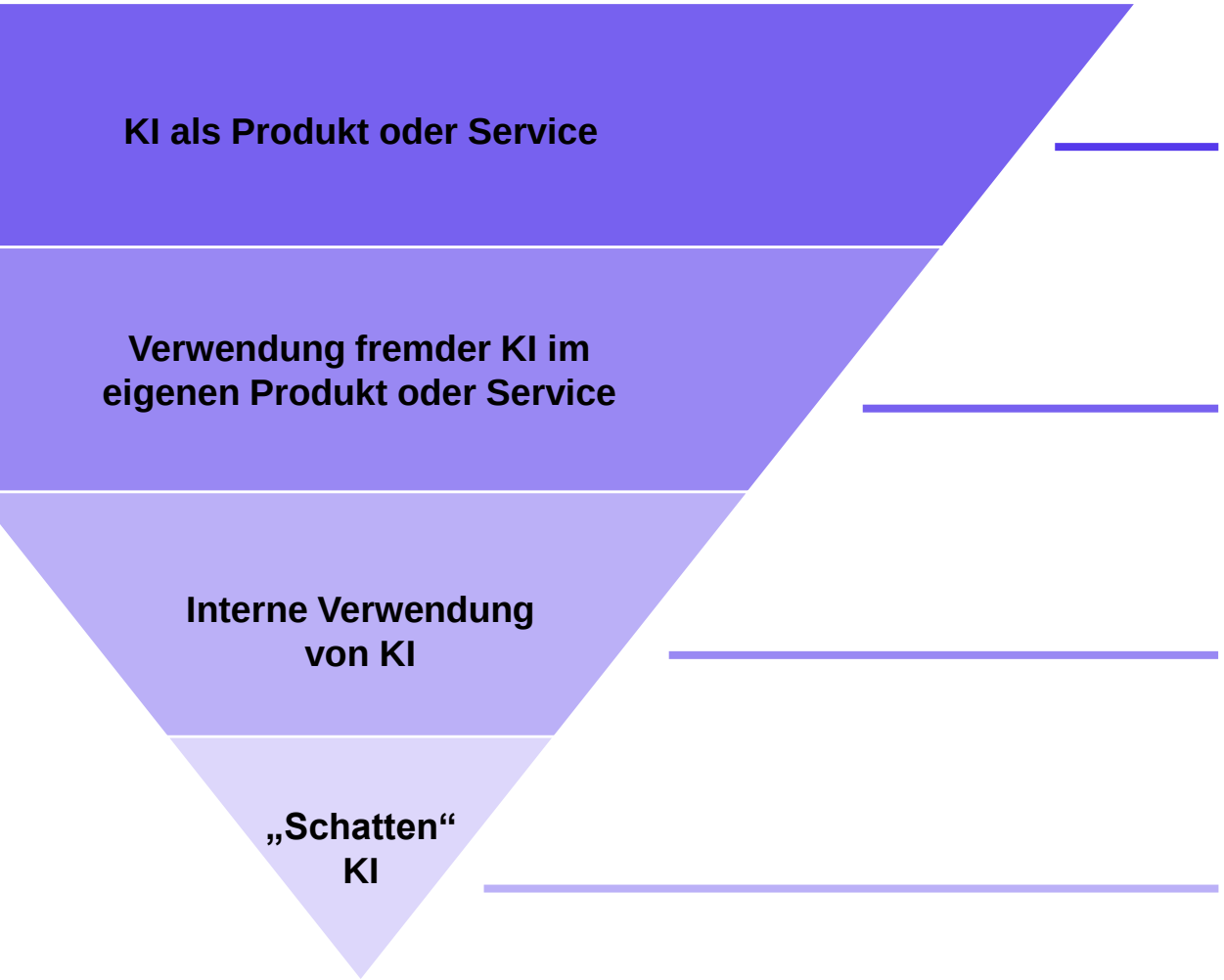
c) wenn sie ein **KI-System**, einschließlich eines KI-Systems für allgemeine Zwecke, das nicht als Hochrisiko-KI-System eingestuft wurde und bereits in Verkehr gebracht oder in Betrieb genommen wurde, **so wesentlich verändern, dass das KI-System zu einem Hochrisiko-KI-Syste**m im Sinne von Artikel 6 wird.“

KI-VO: Aktueller Stand

Grundzüge eines KI Compliance Management Systems

Wesentliche Bausteine eines Compliance-Systems

Umfang der Compliance Pflichten – Risikoanalyse



Anbieter von KI

Nutzer von fremder KI, z.B. als Komponente oder für Kundensupport

Nutzung von KI in der Produktion oder in internen Abläufen ohne Kontakt nach außen

Kein offizieller Einsatz von KI, aber Mitarbeiter und Dienstleister nutzen dennoch KI

Mit Umfang des KI-Einsatzes wachsen die Pflichten

Überblick über Anforderungen aus der KI-VO

- Ethische Grundsätze beim Einsatz von KI, Art. 4a Abs. 1, 2 KI-VO („Leitlinien“)
- Aufbau von KI-Kompetenz im Unternehmen, Art. 4b KI-VO (vgl. Erwägungsgrund 72b: KI-Entwickler)
- Menschliche Aufsicht, Art. 14 KI-VO
- Risikomanagementsystem (eingegliedert in ein Qualitätsmanagementsystem), Art. 17 Abs. 1 KI-VO
- Anpassung der Größe und Organisation von QM und Risikomanagement an Größe und Organisation des Anbieters, Art. 17 Abs. 2 KI-VO
- Fortlaufende Pflicht zur Risikobewertung, Monitoring (Produktbeobachtung) und Reporting (insb. Einhaltung der Meldepflichten nach der KI-VO)

Compliance-Richtlinien

(1) Erste Kommunikation zum KI-Einsatz an Mitarbeiter als Sofortmaßnahme

- Abdeckung der größten wirtschaftlichen und rechtlichen Risiken
  - Geschäftsgeheimnisse
  - Verletzung der Rechte Dritter
  - Datenschutz
- „Tone from the top“ zeigt Bedeutung von KI – und Bewusstsein für Risiken des KI-Einsatzes

(2) Modulartiger Aufbau von Guidelines/Richtlinien anhand konkreter Use Cases

- Definition von Use Cases anhand unterschiedlicher Einsatzbereiche im Unternehmen
  - z.B. Entwicklung (Dokumentation, Code, Review)
  - z.B. Präsentationen (intern, Teil des Marketings)
- Für neue Use Cases: Abfrageliste

Zuständigkeit für die Einhaltung von Compliance-Pflichten im Unternehmen

Nutzung **bestehender Strukturen** durch **Erweiterung der Zuständigkeit**

Datenschutzbeauftragter

IT-Sicherheits-Beauftragter

Allgemeiner Compliance-Officer

+

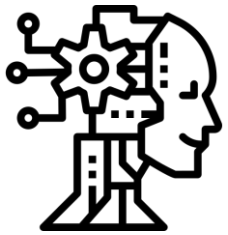
- **Schnittpunkte** zwischen den verschiedenen Themengebieten
  → KI-Projekte kommen häufig mit der Verarbeitung personenbezogener Daten und Cybersicherheit in Berührung
- Erfahrung und **Kenntnis unternehmensspezifischer Spezifika**

−

- Gefahr der **Überfrachtung** der Positionen
- KI geht als Querschnittsmaterie über einzelne Verantwortlichkeitsbereiche hinaus
- **Compliance-Verantwortlichkeit von Vorstand/Geschäftsleitung** kann nur bei klarer Verantwortlichkeit delegiert werden

Zuständigkeit für die Einhaltung von Compliance-Pflichten im Unternehmen

Einführung einer **neuen KI-spezifischen Zuständigkeit**



KI Compliance Officer

- Hohe **technische und rechtliche Komplexität** von KI
- Bündelung von Wissen und Aufbau von Know-how
- Einheitlicher **Ansprechpartner** für interne und externe Zwecke (einschließlich Aufsichts-behörden und ggf. zukünftiger KI-Behörden)
- Förderung des Aufbaus von KI-Kompetenz im Unternehmen, vgl. Art. 4b KI-VO

Zuständigkeit für die Einhaltung von Compliance-Pflichten im Unternehmen

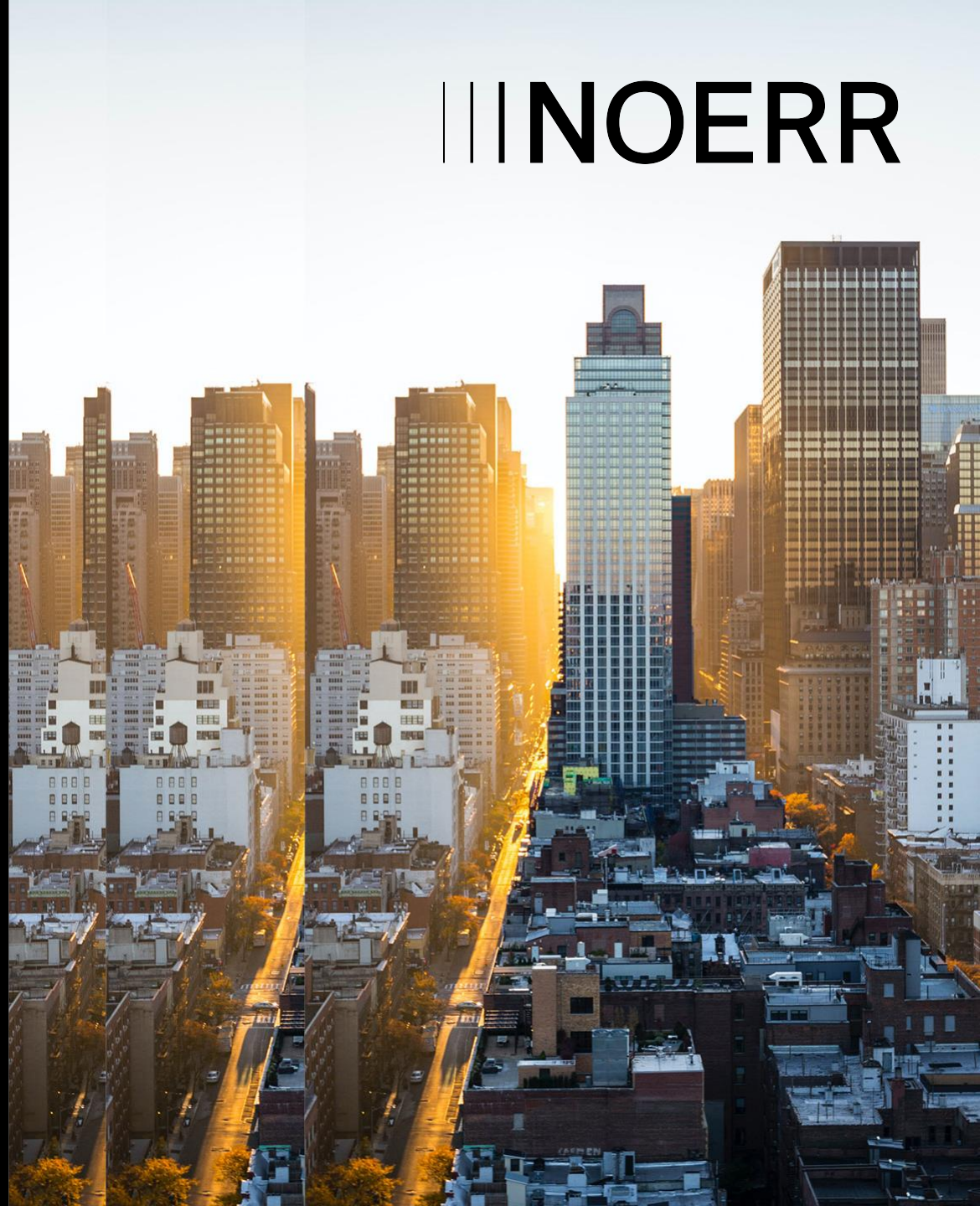
Vorgaben der **KI-VO**

- Keine Pflicht zur Benennung eines KI-Beauftragten durch Unternehmen gegenüber Aufsichtsbehörden, um die Compliance Aufgaben nach der KI-VO wahrzunehmen
- KI-VO sieht keinen zwingenden Posten für KI-Compliance vor
- KI-VO enthält umfassende Pflichten zu fortlaufendem Risikomanagement, die das Unternehmen und letztverantwortlich Vorstand/Geschäftsleitung treffen

KI Compliance Officer – Start der Umsetzung?

Zeitpunkt für KI Compliance

- Bereits jetzt (de lege lata) erhebliche wirtschaftliche und rechtliche Risiken
- Aufbau von Ressourcen und Strukturen ist kosten- und zeitintensiv
- KI-VO steht vor der Tür – keine Umgehungsmöglichkeit wegen Marktortprinzip und hohe Bußgelder
- Frühzeitige Sensibilisierung, Schulung und Weiterbildung der Mitarbeiter im Umgang mit KI aus Compliance-Sicht notwendig, aber auch für wirtschaftlichen Erfolg sinnvoll



info@noerr.com
noerr.com

Save the date

NOERR

Digital Talks

Im September geht es weiter mit einer Einführung in das Thema Cybersecurity.

Den Termin und die Agenda veröffentlichen wir in Kürze auf unserer Webseite.

Wenn Sie auch weiterhin Einladungen zu unseren Webinaren, Veranstaltungen und für Sie relevanten Rechtsthemen erhalten möchten, registrieren Sie sich bitte auf www.noerr.com/noerr-news, soweit Sie dies noch nicht getan haben.

Marieke Luise Merkle

Marieke Merkle
Rechtsanwältin
Senior Associate

+49 89 28628 227
marieke.merkle@noerr.com

Marieke Merkle ist spezialisiert auf die rechtliche Beratung im Bereich Data Economy (insbesondere Cloud-Computing, Datennutzungsverträge, KI) sowie auf die rechtliche Beratung im Zusammenhang mit Digitalisierungsprojekten nationaler und internationaler Mandanten (insbesondere Automatisierung von Unternehmensprozessen, IT-Projekte, IT-Outsourcings) und Softwareurheberrecht (einschließlich Open Source Software). Marieke Merkle ist Lehrbeauftragte an der LMU München für IT-Recht.

Publikationen

- Outbound-Compliance: Aktive Beteiligung an Open-Source-Projekten, MMR 2022, 251
- Der Entwurf des Data Acts, Recht Digital RDi 2022, 168 (zusammen mit Dr. David Bomhard)
- Regulation of Artificial Intelligence – The EU Commission's proposal of an AI Act, EuCML 2021, 257 (zusammen mit Dr. David Bomhard)
- Europäische KI-Verordnung: Der aktuelle Kommissionsentwurf und praktische Auswirkungen, Recht Digital RDI 2021, 276-283 (zusammen mit Dr. David Bomhard)
- Regelmäßige Beiträge in ROBOTIK UND PRODUKTION

Dr. Niklas Maamar

Dr. Niklas Maamar
Rechtsanwalt

+49 30 20942178
niklas.maamar@noerr.com

Dr. Niklas Maamar ist Rechtsanwalt im Berliner Büro bei Noerr. Er berät zu Rechtsfragen rund um digitale Produkte und Geschäftsmodelle. Ein Fokus seiner Arbeit liegt auf dem Einsatz von künstlicher Intelligenz sowie rechtlichen und strategischen Fragen der Plattformökonomie. Daneben ist Dr. Niklas Maamar im allgemeinen IT- und Vertragsrecht tätig und unterstützt Unternehmen bei verbraucherschutzbezogenen Fragen der Digitalisierung.

Publikationen

- Urheberrechtliche Fragen beim Einsatz von generativen KI-Systemen, in: ZUM 2023, 481
- Wem gehört, was eine Künstliche Intelligenz geschaffen hat?, in: IU Mag 7, 2023, S. 10-14
- Sorgfaltspflichten der Anbieter von Vermittlungsdiensten, in Kraul (Hrsg.), Das neue Recht der digitalen Dienste. Digital Services Act (DSA), S. 92-168, Nomos 2023
- Verträge über NFTs, in: GRUR-Prax 2023, 60 (mit Dr. Marvin Bartels)
- Computer als Schöpfer – Der Schutz von Werken und Erfindungen künstlicher Intelligenz, Mohr Siebeck 2021
- Künstliche Intelligenz als Erfinder?, in: CR-online.de Blog, 30.01.2020
- Copyright in artifically generated works, AIPPI 2019 Study Report Germany (Mitarbeit)
- Social Scoring – Eine europäische Perspektive auf Vebraucher-Scores zwischen Big-Data und Big-Brother, in: CR 2019, S.820-828 und Singer/Zhang, Verbraucherschutz in der digitalen Wirtschaft, S. 83-102, Berliner Wissenschaftsverlag 2021