




KI und Haftung – Ein Überblick

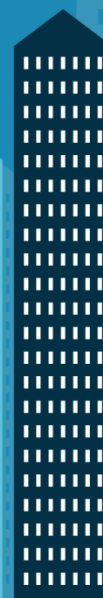
Christoph Y. Pitzer, LL.M. oec.
Dr. Johannes Ballestrem, LL.M.

18. Oktober 2023

Private & Confidential



Helping you
succeed in
tomorrow's
world.



“

Warum ist die KI der beste Anwalt? Weil sie immer auf Daten zugreifen kann, ohne jemals Kaffee zu benötigen, um wach zu bleiben!

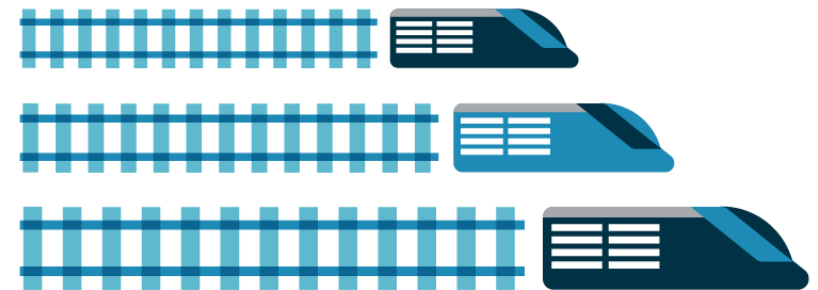
– ChatGPT (released November 2022)

”



Agenda

1. Überblick: Rechtliche Risiken beim Einsatz von KI
2. Einblicke: KI Regulierung
3. Ausblick: Wie geht es weiter?



1

Überblick: Rechtliche Risiken



Input Risiken: Trainingsdaten

- Voreingenommenheit (“bias”) und Diskriminierung:
 - Ggf. Verstoß gegen gesetzliche Verbote, jedenfalls aber birgt es Risiken für die Tauglichkeit des Systems mit potentiellen Folgerisiken
- Datenschutz:
 - Persönliche Daten dürfen nur verarbeitet werden, wenn es eine rechtliche Basis dafür gibt
 - Zusätzliche Voraussetzungen, wo automatisierte Entscheidungen getroffen werden (Einstellungsprüfung, Kreditvergabe)
 - Muss transparent sein, muss dem User leicht möglich sein, menschliche Prüfung zu erreichen bzw. die Entscheidung anzufechten und es bedarf regelmäßiger Checks, dass das System wie intendiert funktioniert
- IP-Risiken
 - Trainingsdaten können IP-rechtlich geschützt sein

Input Risiken: User Input

- Geschäftsgeheimnisse und Geheimhaltungspflichten
 - Was passiert mit den Daten, die von Verwenderseite eingegeben werden? Werden sie ggf. für weiteres Training genutzt oder gar individuell Input und Output ausgewertet?
- Bewusste Falscheingaben

KI und Geschäftsgeheimnisse

- Für erfolgreiches "maschinelles Lernen" müssen KI-Tools mit Daten gefüttert werden
- Die Präzision der Problemlösung hängt von der Quantität und Qualität der gesammelten Daten ab
- KI lernt und verbessert sich anhand dieser Trainingsdaten

KI und Geschäftsgeheimnisse

Kann die Eingabe von Geschäftsgeheimnissen in KI-Tools zur Ermittlung des **Standes der Technik** zu deren **Offenlegung** und in der Folge zur Zurückweisung einer Patentanmeldung führen?

KI und Geschäftsgeheimnisse

§ 3 Deutsches Patentgesetz / Art. 54 EPÜ

(1) Eine Erfindung gilt als neu, wenn sie **nicht zum Stand der Technik gehört**. Als Stand der Technik gelten **alle Kenntnisse, die der Öffentlichkeit** vor dem für den Anmelde- oder Prioritätstag maßgeblichen Tag durch schriftliche oder mündliche Beschreibung, durch Benutzung oder in sonstiger Weise **zugänglich gemacht worden sind**.

(2) ...

(3) ...

(4) ...

(5) ...

KI und Geschäftsgeheimnisse

§ 2 GeschGehG

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)

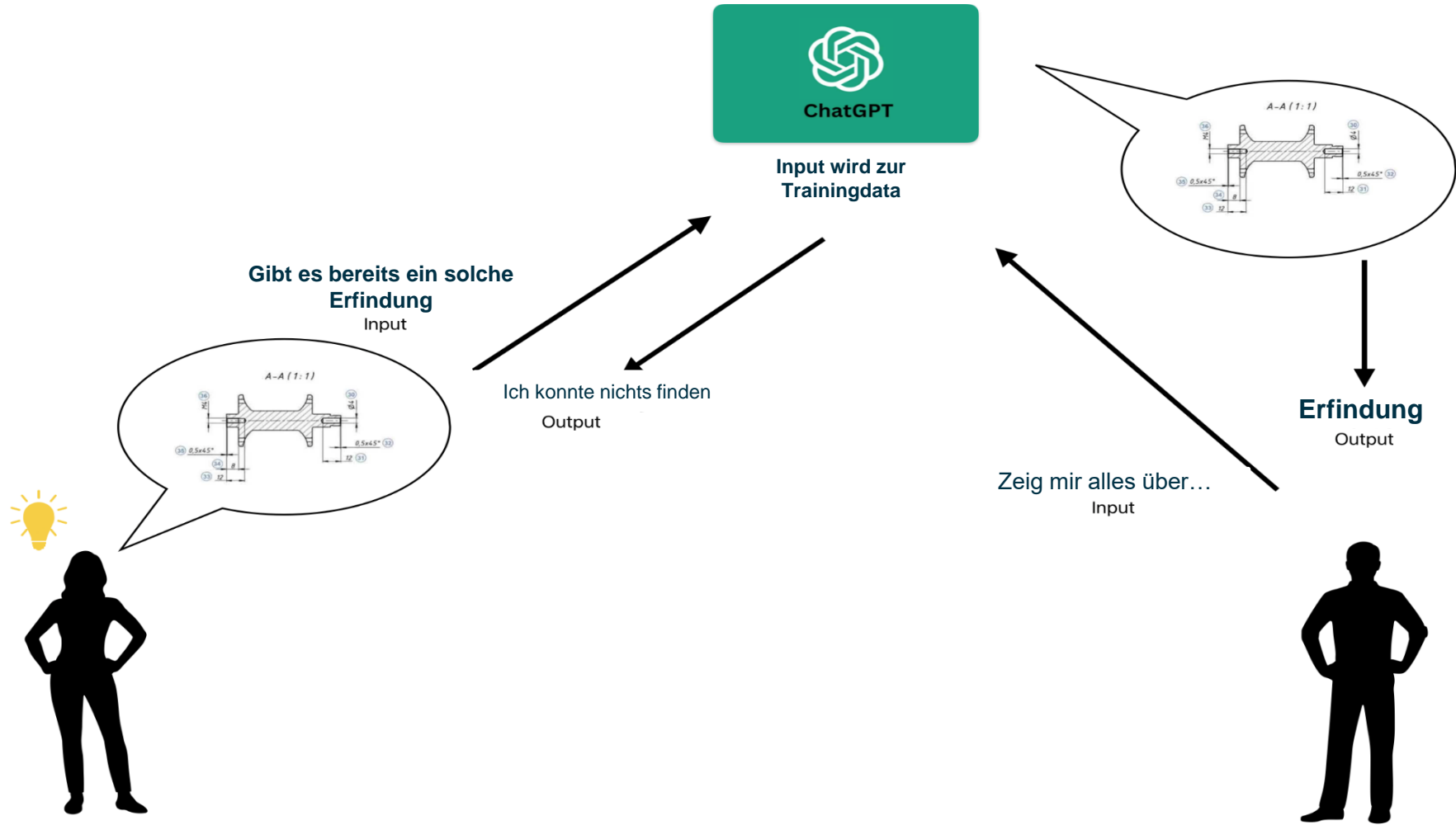
bei der ein berechtigtes Interesse an der Geheimhaltung besteht;

KI und Geschäftsgeheimnisse

Der Samsung-Vorfall und andere sicherheitsrelevante Bugs

- Samsung erlaubte seinen Mitarbeitern, ChatGPT für berufliche Zwecke zu nutzen
- Der gesamte Quellcode einer Anwendung wurde zu Debugging-Zwecken in ChatGPT eingegeben
- ChatGPT wurde von Samsung-Mitarbeitern genutzt, um Sitzungsnotizen zusammenzufassen und eine Präsentation zu erstellen
- In einem anderen Fall wurden ChatGPT-Benutzern aufgrund eines Fehlers, der die Anfragen / Aufforderungen offenlegte, Anfragen von anderen Benutzern angezeigt
- Alle Vorfälle sind öffentlich bekannt geworden

KI und Geschäftsgeheimnisse



KI und Geschäftsgeheimnisse



Compare ChatGPT plans

Free

\$0 per person/month

Try it now ↗

- ✓ GPT-3.5
- ✓ Regular model updates

Plus

\$20 per person/month

Upgrade now ↗

Everything in Free, and:

- ✓ GPT-4*
- ✓ Advanced Data Analysis*
- ✓ Plugins*
- ✓ Early access to beta features

Enterprise

Contact sales

Everything in Plus, and:

- ✓ Unlimited high-speed GPT-4*
- ✓ Longer inputs with 32k token context
- ✓ Unlimited Advanced Data Analysis
- ✓ Internally shareable chat templates
- ✓ Dedicated admin console
- ✓ SSO, domain verification, and analytics
- ✓ API credits to build your own solutions
- ✓ Enterprise data is not used for training

*Usage capped at 50 messages every three hours

*Actual speed varies depending on utilization of our systems



KI und Geschäftsgeheimnisse - <https://search.projectpq.ai/>

pqai

Vision Get Involved Resources Blog

Try Patent Searching

Shaping the future of patent searching through AI

A collaborative, not-for-profit initiative to build an open-source ecosystem of AI components to drive innovation and improve patent quality.

Try Patent Search

An initiative by AT&T



Vision

Patent Quality Artificial Intelligence

KI und Geschäftsgeheimnisse

How PQAI maintains user privacy?

By [PQAI Staff](#) | In [FAQ](#) | [Leave a comment](#)

When you use PQAI for running prior-art searches, you can rest assured that PQAI **provides you complete privacy.**

Unlike most search engines, which track everything you do, **PQAI never tracks or saves your search data.** We believe that it is very much needed for a platform like PQAI, which is used by many inventors to validate the novelty of their ideas.

When you enter a search query on PQAI, it goes to our server in the cloud on a secure, encrypted link. The server finds the results matching your query from its database, and sends them off back your way. **After this, no traces of your query are left on the server.**

(This policy of never storing user search queries is also mentioned on PQAI's [search page](#) – see the link at the bottom of the page.)

Please note even though we don't track user data, we do store few anonymous traffic statistics such as number of requests. This helps us scale our servers appropriately to handle the traffic, deter abuse, and understand how people find value on our platform.

How do we train our AI?

Another question is whether our AI learns from user behavior? The answer is – no. The fact that we don't track or save search data makes it impossible for us to train our AI on it.

But that leads to another question: how do we train it then? The answer is: patent office examination data.

We download the examination data that is routinely published by the USPTO on their website, then we process it to create training datasets for our AI. Many contributors from the open source community have helped us in this process.

KI und Geschäftsgeheimnisse

All Prior Art

Algorithmically generated prior art

Prior Art **Publications** About Contact

Publications

Publications, each of 10,000 inventions

Current total:

4,220,000 inventions

[Current torrent](#)

[All Prior Art Volume 1](#)

[All Prior Art Volume 2](#)

[All Prior Art Volume 3](#)

[All Prior Art Volume 4](#)

[All Prior Art Volume 5](#)

[All Prior Art Volume 6](#)

[All Prior Art Volume 7](#)

[All Prior Art Volume 8](#)

[All Prior Art Volume 9](#)

[All Prior Art Volume 10](#)

[All Prior Art Volume 11](#)

[All Prior Art Volume 12](#)

Search ... 

All The Claims

Algorithmically generated claims as prior art

Claims About Publications Contact

1461189017-69dc6a61-7dae-4dd5-b591-5a18c6996c0e

Search ... 

1. A filtering chip conveyor comprising:
a conveyor tank arranged to retain cutting fluid containing chips,
a continuous conveyor belt at least partly disposed inside the conveyor tank, the belt being arranged to rotate and to turn at a tail end and at a discharge end, with a space between upper and lower flights of the belt, so as to transport chips on the upper flight towards the discharge end, to be discharged off the conveyor,
at least one filter box arranged between the upper and the lower flights of the belt,
at least one filter plate arranged in the filter box, the filter plate comprising a filtration region having a plurality of openings for permitting cutting fluid to pass through the filter plate while not permitting chips whose smallest sectional chip dimension is larger than a predetermined maximum chip dimension, to pass through the filter plate,
wherein:
the at least one filter plate has a thickness of less than 0.3 mm,
the openings include an array of profiled orifices etched through the filter plate, the etched orifice profile being such that the smallest sectional

Output Risiken: IP-Risiken bezüglich generierter Inhalte

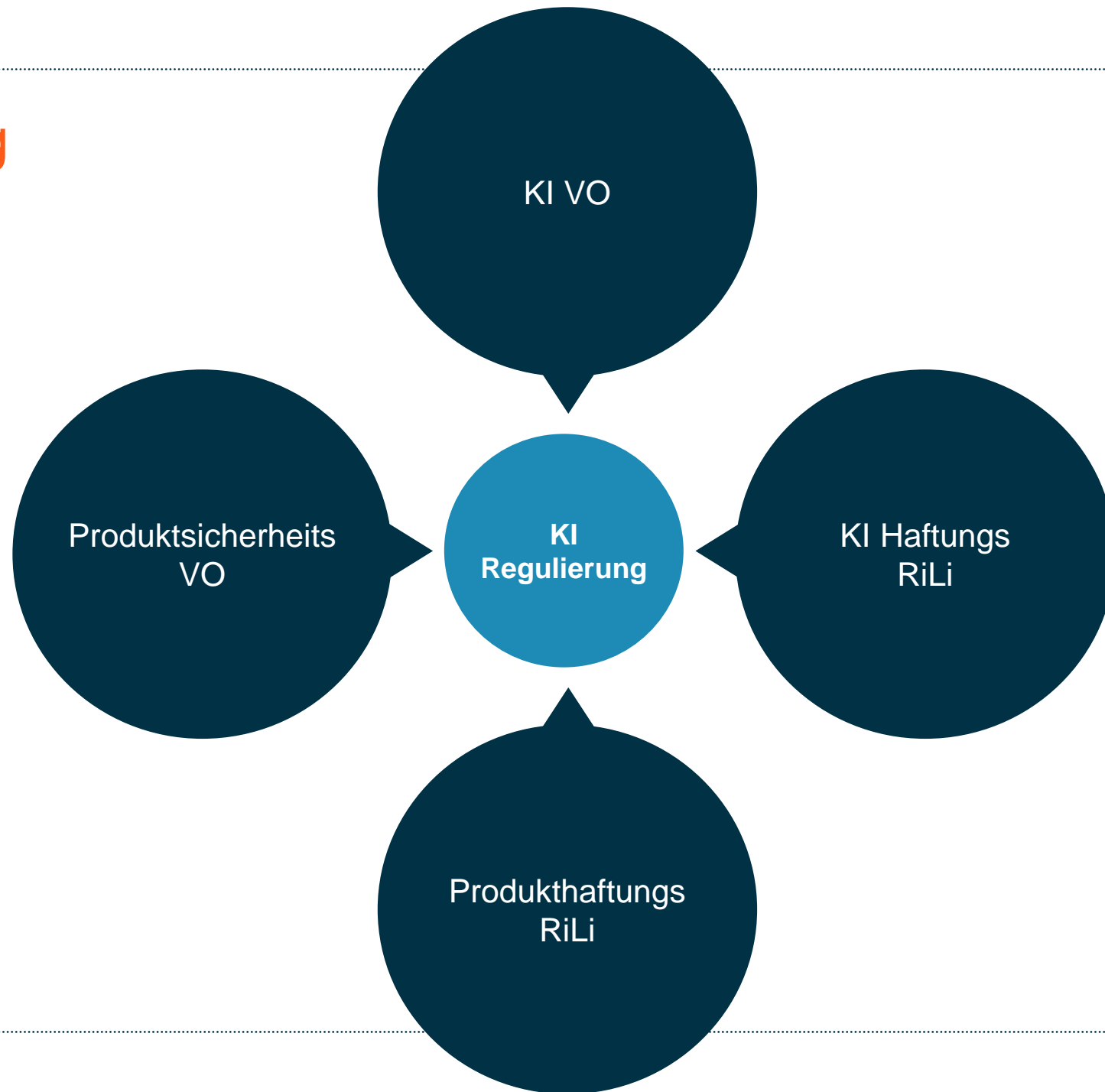
- Patentrecht
 - KI Systeme können zwar Erfindungen generieren
 - KI Systeme können jedoch nicht Erfinder sein
- Urheberrecht
 - Grundsätzlich urheberrechtlicher Schutz beim Urheber selbst bzw. Nutzungsrechte beim Arbeitgeber. Beim Einsatz von KI könnte dies anders zu bewerten sein: Allenfalls Zuhilfenahme, nicht aber vollautomatisierter Einsatz.
- Verletzung fremder IP-Rechte (Haftungsfreistellung!)

Output Risiken: Genauigkeit, Halluzinationen und Bias

„Halluzinationen“ von generativen KI-Systemen sind ein bekanntes Risiko, das sich aus der Tatsache ergibt, dass maschinelle Lernsysteme Antworten vorhersagen, anstatt sie zu erforschen.

- Kann die Genauigkeit der Ergebnisse Auswirkungen auf die Produktsicherheit oder -qualität haben?
- Wenn die KI mithilfe personenbezogener Daten trainiert wurde, sind Verpflichtungen zur Beseitigung oder Korrektur ungenauer Daten über Personen denkbar

KI Regulierung



2

Einblicke: Wo stehen wir?

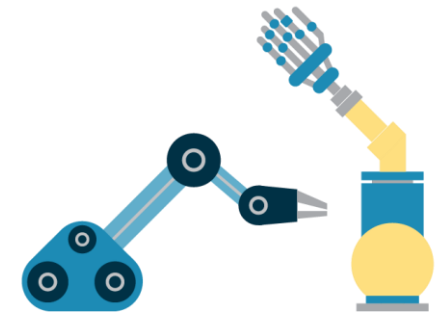


ProduktsicherheitsVO

- VO (EU) 2023/988
- In Kraft seit 12. Juni 2023
- Gilt ab dem 13. Dezember 2024

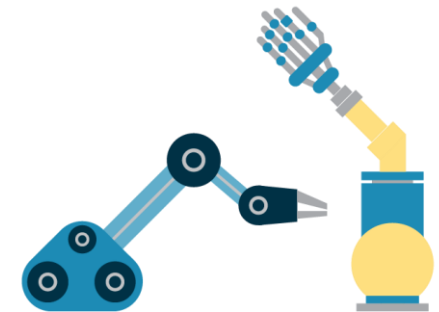
ProduktsicherheitsVO: Worum geht es?

- Sicherheit von Verbraucherprodukten
- Erweiterung der Verpflichteten: Fulfillment-Dienstleister sowie Anbieter von Online-Marktplätzen
- Klarstellung zu Remanufacturing (wesentliche Veränderung)
- Rückrufpflichten wurden verschärft
- Software im (unmittelbaren) Anwendungsbereich?
- Kriterien für „sicheres Produkt“ werden verschärft:
 - Wirkung anderer Produkte und mögliche Beeinflussung sicherheitsrelevanter Eigenschaften
 - Aspekte der Cybersicherheit
 - Sich entwickelnde, lernende und prädikative Funktionen des Produkts



ProduktsicherheitsVO: Neue Dokumentationspflichten

- Hersteller müssen für jedes Produkt
 - eine interne Risikoanalyse durchführen und
 - technische Unterlagen erstellen, die mindestens eine allgemeine Beschreibung des Produkts und seiner für die Bewertung seiner Sicherheit relevanten wesentlichen Eigenschaften enthalten
 - Sofern dies angesichts der möglicherweise mit dem Produkt verbundenen Risiken angemessen ist, umfassen die (...) genannten technischen Unterlagen, soweit anwendbar, außerdem a) eine Analyse der möglicherweise mit dem Produkt verbundenen Risiken und der gewählten Lösungen zur Beseitigung oder Minderung dieser Risiken, einschließlich der Ergebnisse aller Berichte über Tests, die der Hersteller durchgeführt hat oder von einem Dritten hat durchführen lassen, und b) eine Aufstellung aller einschlägigen europäischen Normen nach Artikel 7 Absatz 1 Buchstabe a und der anderen Elemente nach Artikel 7 Absatz 1 Buchstabe b oder Artikel 8, die angewandt wurden, um dem allgemeinen Sicherheitsgebot gemäß Artikel 5 zu entsprechen



ProduktsicherheitsVO

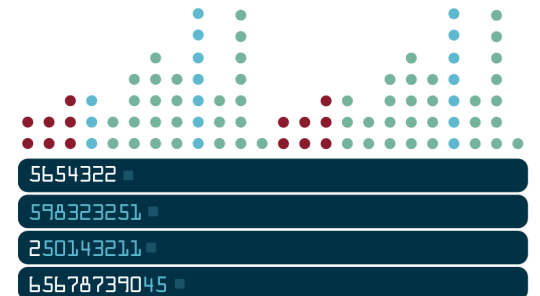
- VO (EU) 2023/988
- In Kraft seit 12. Juni 2023
- Gilt ab dem 13. Dezember 2024

KI VO

- COM (2021) 206
- Nach Beschluss des EP am 14. Juni 2023 nun im Trilog
- Verabschiedung Ende 2023?
- Inkrafttreten 2026

Regelungsziele

- **Technologieneutrale, einheitliche Definition für KI**, die auf zukünftige KI-Systeme angewendet werden könnte
- In der EU eingesetzte KI-Systeme sollen sicher, transparent, nachvollziehbar, nicht diskriminierend und umweltfreundlich sein
- **Überwachung von KI-Systemen durch Menschen und nicht von der Automatisierung**, um schädliche Ergebnisse zu verhindern



”

‘artificial intelligence system’ (AI system) means a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments;

”

Kern des Regelwerks der KI-Verordnung ist eine auf die Inverkehrgabe von künstlicher Intelligenz durch den Hersteller ausgerichtete Konformitätsbewertung, die Mindestanforderungen an Systeme künstlicher Intelligenz definiert.

Adressaten sind insbesondere Anbieter von künstlicher Intelligenz, aber auch deren gewerbliche Verwender sowie Hersteller von Produkten, die wiederum künstliche Intelligenz beinhalten.

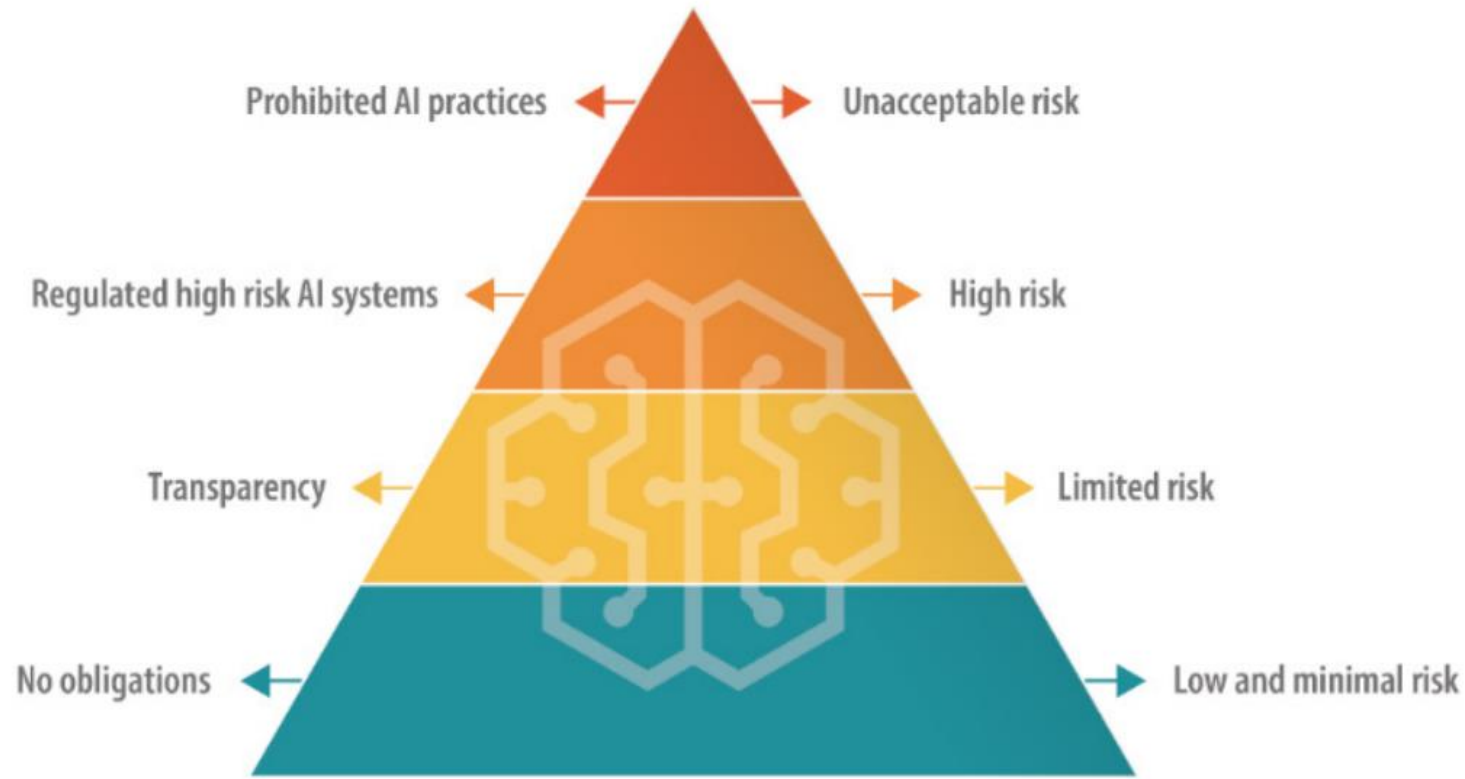


Risikobasierter Ansatz:

- bestimmte künstliche Intelligenz wird verboten
- Hochrisiko-KI wird unter besondere Voraussetzungen gestellt
- Für General Purpose AI gibt es gewisse Anforderungen



Pyramid of risks



KI Anwendungen sollen nur so weit reguliert werden, wie es für die Bewältigung bestimmter Risiken unbedingt erforderlich ist.

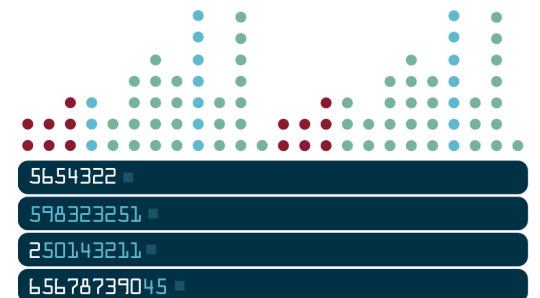
Data source: [European Commission](https://ec.europa.eu/commission/presscorner/detail/en/ip19_1911).

Unterschiedliche Risk Levels: Unacceptable Risks

KI-Systeme, die als Bedrohung für Menschen gelten und verboten werden.

- Kognitive Verhaltensmanipulation von Menschen oder bestimmten gefährdeten Gruppen
- Soziales Scoring: Klassifizierung von Menschen aufgrund von Verhalten, sozioökonomischem Status oder persönlichen Merkmalen
- Biometrische Identifikationssysteme in Echtzeit und aus der Ferne, z.B. Gesichtserkennung

Einige Ausnahmen können zulässig sein: So werden beispielsweise "post"-biometrische Fernidentifizierungssysteme, bei denen die Identifizierung erst mit erheblicher Verzögerung erfolgt, zur Verfolgung schwerer Straftaten zugelassen, allerdings nur nach gerichtlicher Genehmigung.



Was fällt unter High Risk?

Datenbank

1. Biometrische Identifizierung und Kategorisierung natürlicher Personen
2. Verwaltung und Betrieb kritischer Infrastrukturen
3. Allgemeine und berufliche Bildung
4. Beschäftigung, Personalmanagement und Zugang zur Selbstständigkeit
5. Zugänglichkeit und Inanspruchnahme grundlegender privater und öffentlicher Dienste und Leistungen
6. Strafverfolgung
7. Migration, Asyl und Grenzkontrolle
8. Rechtspflege und demokratische Prozesse

Was fällt unter High Risk?

KI-Systeme, die in Produkten verwendet werden, die unter die Produktsicherheitsvorschriften der EU fallen.

Zum Beispiel:

- Maschinen
- Spielzeug
- Luftfahrt
- Autos
- medizinische Geräte
- Aufzüge

Anforderungen High Risk: Konformitätsbewertung

- Registrierung der KI Systeme in einer von der Kommission verwalteten EU-weiten Datenbank, bevor sie auf den Markt gebracht oder in Betrieb genommen werden
- Alle KI-Produkte und -Dienstleistungen, die unter die Produktsicherheitsgesetzgebung unterliegen, fallen unter die bereits bestehenden Konformitätsregelungen für Dritte, die die bereits gelten (z. B. für Medizinprodukte)
- Anbieter von KI-Systemen, die derzeit nicht unter die EU Gesetzgebung unterliegen, müssen ihre eigene Konformitätsbewertung (Selbstbewertung) durchführen, die zeigt dass sie die neuen Anforderungen erfüllen und die CE-Kennzeichnung verwenden können
- Nur KI-Systeme mit hohem Risiko die für die biometrische Identifizierung verwendet werden, würden eine Konformitätsbewertung durch eine "benannte Stelle" erfordern

Weitere Anforderungen: High Risk

- Anforderungen an Risikomanagement (System), Tests, technische Robustheit, Daten und Datengovernance, Protokollierung, Transparenz, menschliche Aufsicht und Cybersicherheit, Qualitätsmanagement
- Betrifft Anbieter, Importeure, Händler und Nutzer von KI-Systemen mit hohem Risiko
- Anbieter von außerhalb der EU benötigen einen bevollmächtigten Vertreter in der EU, der (u.a.), die Konformitätsbewertung zu gewährleisten, ein System zur Überwachung nach dem Inverkehrbringen einzurichten und bei Bedarf Korrekturmaßnahmen Maßnahmen zu ergreifen

Anforderungen: Limited Risk

- KI-Systeme, die mit Menschen interagieren (z. B. Chatbots), Systeme zur Erkennung von Emotionen, biometrische Kategorisierungssysteme und KI-Systeme, die Bild-, Audio- oder Videoinhalte erzeugen oder manipulieren (z. B. Deepfakes)
 - Transparenz
 - Design des Modells, dass es keine illegalen Inhalte erzeugen kann
 - Offenlegung einer Übersicht, welche urheberrechtlich geschützten Inhalte zum Training verwendet wurden

Low and minimal Risk

- Keine Beschränkung, aber es sind (freiwillige) codes of conduct angedacht. Diese können dann indirekt Verbindlichkeit entwickeln (z.B. aufgrund interner Compliance-Ziele, freiwillige Selbstverpflichtung von Industrien, oder Einhaltung wird vertraglich zur Auflage gemacht)

ProduktsicherheitsVO

- VO (EU) 2023/988
- In Kraft seit 12. Juni 2023
- Gilt ab dem 13. Dezember 2024

KI VO

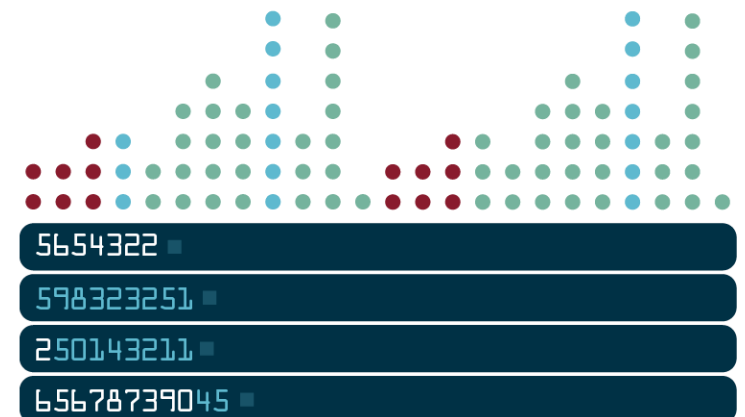
- COM (2021) 206
- Nach Beschluss des EP am 14. Juni 2023 nun im Trilog
- Verabschiedung Ende 2023?
- Inkrafttreten 2026

KI HaftungsRiLi

- COM (2022) 496
- Vor erster Lesung im EP

KI HaftungsRiLi: Worum geht es?

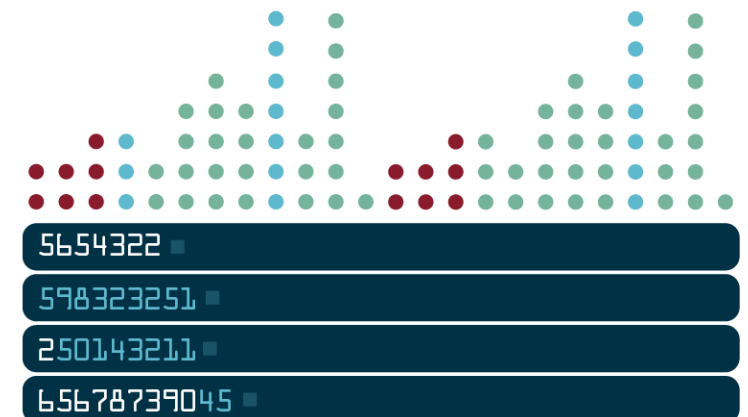
- Ersatz für Schäden durch Systeme künstlicher Intelligenz
- Nichtvertragliche, verschuldensabhängige Schadensersatzansprüche
- B2B und B2C
- Beweiserleichterung für Geschädigte:
 - Kausalitätsvermutung, die die Opfer von der Pflicht entbindet, ausführlich zu erläutern, wie der Schaden durch ein bestimmtes Verschulden oder Versäumnis verursacht wurde, und
 - der Zugang zu Beweismitteln im Besitz von Unternehmen oder Anbietern, wenn es um Hochrisiko-KI geht



KI HaftungsRiLi: Kausalitätsvermutung

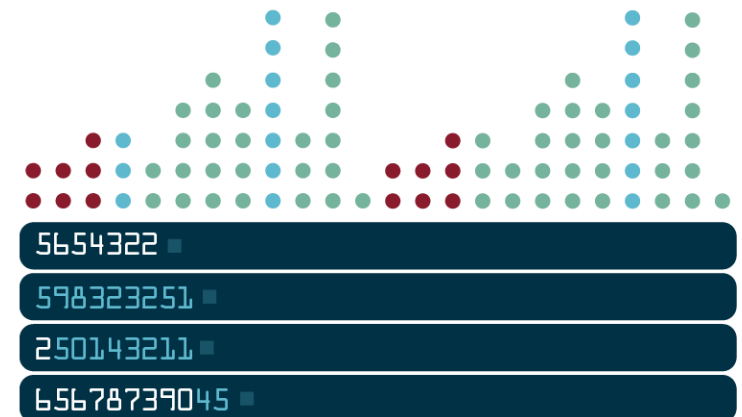
Voraussetzungen der Kausalitätsvermutung:

1. Nachweis des Geschädigten, dass der vom KI-System erzeugte Output (oder das Fehlen) zu dem konkreten Schaden geführt hat
2. Verletzung einer Sorgfaltspflicht, die vor dem eingetretenen Schaden schützen soll (Vermutung bei Hochrisiko-KI-Systemen, wenn der Anspruch auf Zugang zu bestimmten Beweismitteln unberechtigt verweigert wurde)
3. Hinreichende Wahrscheinlichkeit, dass der Fehler den vom KI-System erzeugten Output (oder dem Fehlen) beeinflusst hat



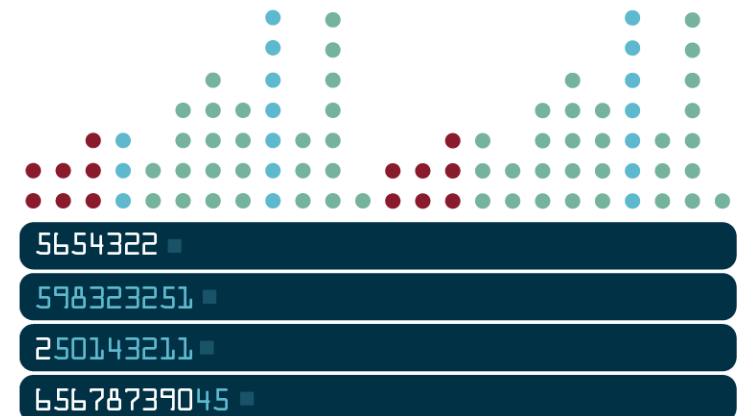
KI HaftungsRiLi: Sorgfaltspflichten des Anbieters

- a) Bei dem KI-System werden Techniken eingesetzt, bei denen Modelle mit Daten trainiert werden, und das System wurde nicht anhand von Trainings-, Validierungs- und Testdatensätzen entwickelt, die den in (...) genannten Qualitätskriterien entsprechen
- b) das KI-System wurde nicht so konzipiert und entwickelt, dass es den in (KI VO) festgelegten Transparenzanforderungen entspricht
- c) das KI-System wurde nicht so konzipiert und entwickelt, dass es (...) während der Dauer seiner Verwendung von natürlichen Personen wirksam beaufsichtigt werden kann
- d) das KI-System wurde nicht so konzipiert und entwickelt, dass es (...) im Hinblick auf seine Zweckbestimmung ein angemessenes Maß an Genauigkeit, Robustheit und Cybersicherheit erreicht, oder
- e) es wurden nicht unverzüglich die erforderlichen Korrekturmaßnahmen ergriffen, um das KI-System mit den in (KI VO) festgelegten Anforderungen in Einklang zu bringen oder das System gegebenenfalls (...) zurückzunehmen oder zurückzurufen.



KI HaftungsRiLi: Sorgfaltspflichten des Anbieters

- a) seiner Pflicht zur Verwendung oder Überwachung des KI-Systems entsprechend der beigefügten Gebrauchsanweisung oder gegebenenfalls zur Aussetzung oder Unterbrechung seiner Verwendung (KI VO) nicht nachgekommen ist, oder
- b) Eingabedaten, die seiner Kontrolle unterliegen, auf das KI-System angewandt hat, die der Zweckbestimmung des Systems (KI VO) nicht entsprechen



ProduktsicherheitsVO

- VO (EU) 2023/988
- In Kraft seit 12. Juni 2023
- Gilt ab dem 13. Dezember 2024

KI VO

- COM (2021) 206
- Nach Beschluss des EP am 14. Juni 2023 nun im Trilog
- Verabschiedung Ende 2023?
- Inkrafttreten 2026

KI HaftungsRiLi

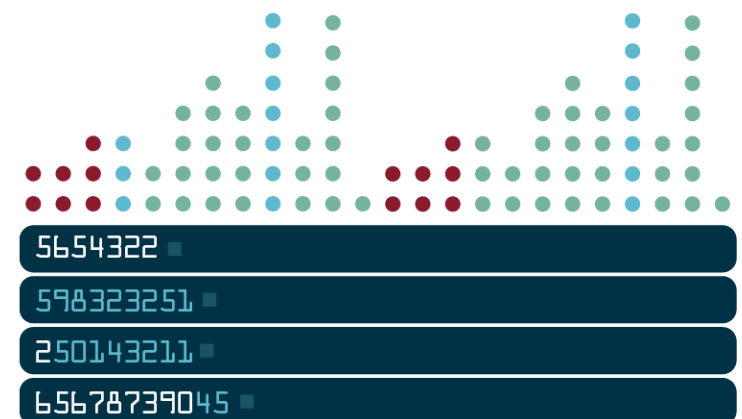
- COM (2022) 496
- Vor erster Lesung im EP

ProdukthaftungsRiLi

- COM (2022) 495
- Vor erster Lesung im EP

ProdhaftungsRiLi: Worum geht es?

- Ersatz für Schäden durch Produkte - zukünftig ausdrücklich Software
- Nichtvertragliche, verschuldensunabhängige Schadensersatzansprüche
- Nur B2C
- Beschränkung auf psychische, physische Schäden, Sachschäden und Datenverluste (keine Vermögensschäden)
- Beweiserleichterung für Geschädigte:
 - Kausalitätsvermutung, die die Opfer von der Pflicht entbindet, ausführlich zu erläutern, wie der Schaden durch ein bestimmtes Verschulden oder Versäumnis verursacht wurde, und
 - der Zugang zu Beweismitteln im Besitz von Unternehmen oder Anbietern



3

Ausblick: Wie geht es weiter?



ProduktsicherheitsVO

- VO (EU) 2023/988
- In Kraft seit 12. Juni 2023
- Gilt ab dem 13. Dezember 2024

KI VO

- COM (2021) 206
- Nach Beschluss des EP am 14. Juni 2023 nun im Trilog
- Verabschiedung Ende 2023?
- Inkrafttreten 2026

KI HaftungsRiLi

- COM (2022) 496
- Vor erster Lesung im EP

ProdukthaftungsRiLi

- COM (2022) 495
- Vor erster Lesung im EP

Vielen Dank für Ihre Aufmerksamkeit!



Dr. Johannes Ballestrem

Partner
Germany

+49 221 5108 4394

johannes.ballestrem@osborneclarke.com



Christoph Y. Pitzer, LL.M. oec.

Senior Counsel
Germany

+49 221 5108 4278

christoph.pitzer@osborneclarke.com





Vielen Dank für die Aufmerksamkeit!


Osborne Clarke ist der Firmenname für ein internationales Rechtsanwaltsbüro und die damit verbundenen Abteilungen.

Alle Einzelheiten dazu hier: osborneclarke.com/verein

Diese Materialien werden nur zu allgemeinen Informationszwecken geschrieben und bereitgestellt. Sie sind nicht vorgesehen und sollten nicht als Ersatz für Rechtsberatung verwendet werden. Bevor Sie sich mit einem der folgenden Themen befassen, sollten Sie sich rechtlich beraten lassen.

© Osborne Clarke Rechtsanwälte Steuerberater Partnerschaft mbB

September 2023



Helping you
succeed in
tomorrow's
world.

