



Was passiert mit meinen Daten? KI, Datenschutz und digitale Souveränität

Digitale Woche 10.-14.11.2025



Digitale Woche

10. - 14. November 2025

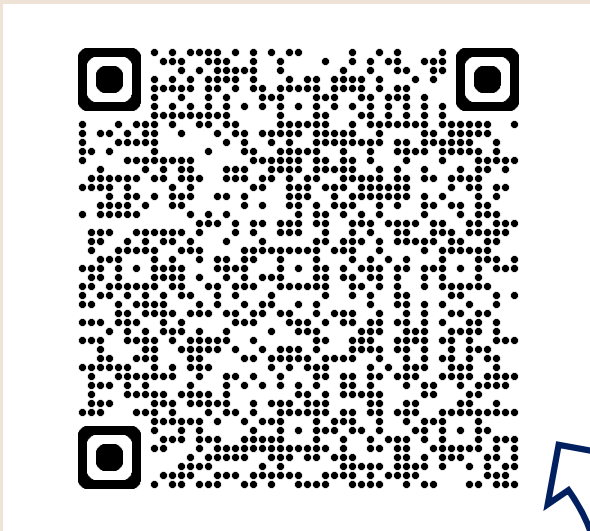
IHK

Koblenz

Starke Wirtschaft.
Starke Region.



Jetzt noch anmelden!



**Hier gelangen Sie auch
zu der Themenübersicht**

#gemeinsamdigital

- IHKhub
 - Informationen und nützliche Links
 - Veranstaltungen
 - <https://www.ihkhub-koblenz.de/>
- #GemeinsamDigital: Webinare
 - E-Business, Digitale Innovationen, IT-Sicherheit,...
 - <https://www.dihk.de/de/themen-und-positionen/wirtschaft-digital/gemeinsamdigital>



Individuellen Sicherheitsbedarf ermitteln

- Kostenfreie Unterstützung für kleine und mittlere Unternehmen, Start-ups und Handwerksbetriebe
 - <https://transferstelle-cybersicherheit.de>
- CYBERSicher Check
 - Ist-Zustand ermitteln und Handlungsempfehlungen erhalten
 - <https://cybersicher-check.de/>

➔ Schwerpunkte und Termine

- Expertise in verschiedenen KI-Bereichen
- Besuche von Unternehmen mit Use Cases
- Austausch mit Universität, Hochschule und KI-Forschungszentren
- Interesse? ukena@koblenz.ihk.de



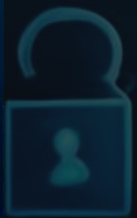
- Input von Stefan Pilarczyk, BRL Risk Consulting: KI, Datenschutz und Digitale Souveränität. Was müssen Unternehmen beachten?
- Fragen und Antworten. Nutzen Sie gern den Chat.

Anmeldung zum IHK-Newsletter





"Was passiert mit meinen Daten?
KI, Datenschutz und digitale Souveränität"





Stefan Pilarczyk

Head of Cybersecurity

ÜBER MICH

Als Leader bei der BRL Risk Consulting GmbH & Co KG, Security-Hero und Speaker beim Cyberwald, eine Community bestehend aus Security Experten unterstütze ich mit meiner Expertise und Kompetenz seit Jahren Kunden aller Größen aus verschiedensten Branchen. Zusammen mit meinem technischen Background bildet das die Grundlage für den gesamtheitlichen Ansatz in der IT-Security.



- >15 Jahre Erfahrung
- CxO Advisory
- Standards
 - NIS-2
 - DORA
 - ISO27001
 - BSI-Grundschutz
 - TISAX
 - NIST
 - UVM...
- IT-Sicherheitsstrategie
- Ganzheitlicher Ansatz
- Notfallmanagement und Incident Response

Agenda

Einleitung

Digitale Souveränität

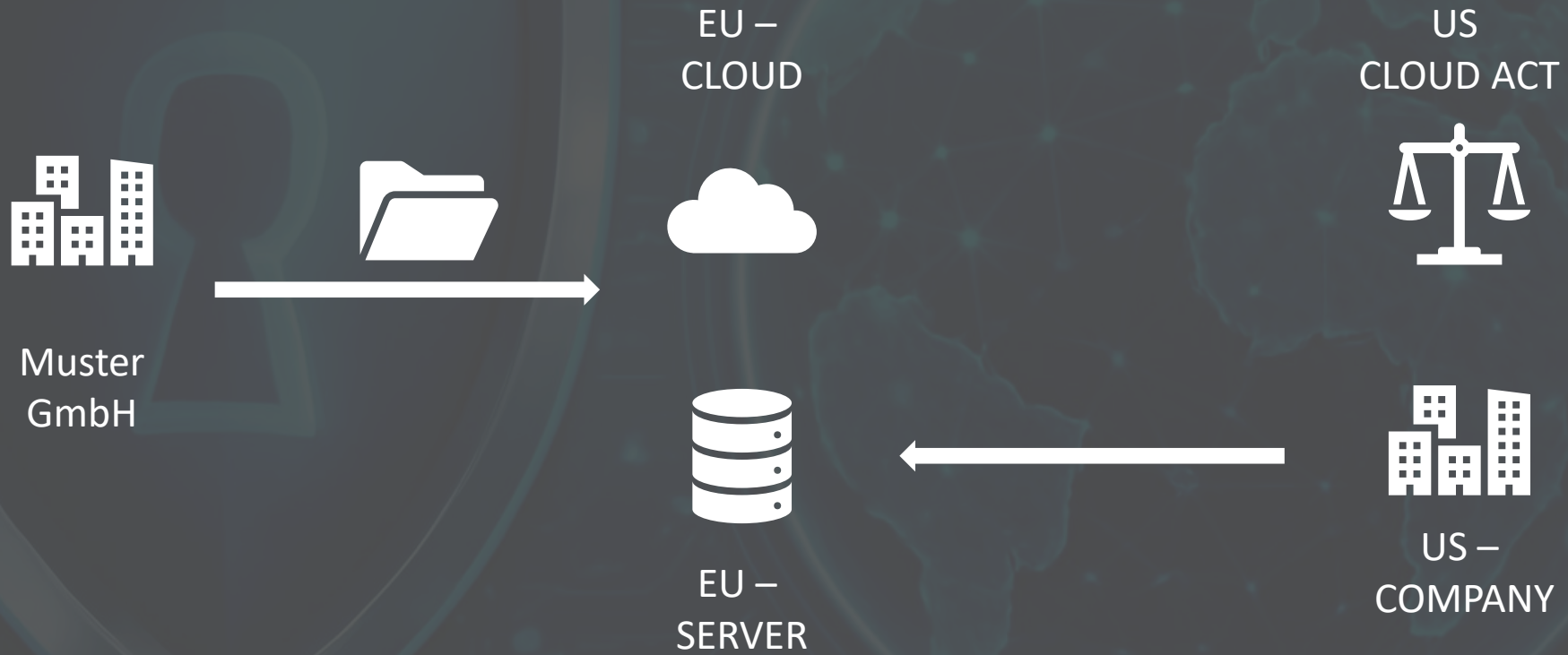
KI Nutzung

Mögliche Lösung

Convenience Falle

Fragen

*„Wer kontrolliert eigentlich wirklich Ihre Daten,
sobald sie auf einer Cloud liegen?“*



Digitale Souveränität vs. Extraterritorialen Rechtsvorschriften

US CLOUD Act = Clarifying Lawful Overseas Use of Data Act

Ziel: US-Strafverfolgungsbehörden erlauben, auf Daten zuzugreifen, die bei US-Unternehmen gespeichert sind – auch wenn diese Daten außerhalb der USA liegen.

Geltungsbereich: Betrifft Cloud-Dienste und andere IT-Dienstleister mit Sitz in den USA, unabhängig davon, wo die Server stehen.

Rechtliche Folge: US-Behörden können per Gerichtsbeschluss Daten von US-Firmen verlangen – auch wenn die Daten in Europa oder anderswo gespeichert sind.

Konflikt mit EU-Datenschutz: Trotz DSGVO und europäischer Datenschutzgesetze müssen Cloud-Anbieter US-Recht befolgen, was zu Rechtsunsicherheiten für europäische Nutzer führt.

Keine Herausgabe verweigert: US-Unternehmen dürfen die Datenübergabe nicht ablehnen, auch wenn das im Zielstaat illegal wäre (Umweg über amerikanische Staatsbürger möglich)

Auswirkungen: Einschränkung digitaler Souveränität und Datenschutz der Nutzer, da Daten theoretisch von US-Behörden eingesehen werden können.

-> CLOUD Act hat zwar die rechtliche Grundlage für US-Datenzugriffe auf global verteilte Daten geschaffen, konkrete Einzelfallentscheidungen sind in der Öffentlichkeit aber kaum transparent.

US Cloud Act ends Microsoft Dublin email case with a whimper

Act gives US 'nearly unchecked' power over global digital privacy rights, say critics

Expand



At the end of March, President Donald Trump signed into law the Cloud Act, which removed the ambiguity over whether a US court could demand data held extraterritorially. Photograph: Jim Lo Scalzo/EPA

Nur digitale Souveränität kann uns vor IT-Zusammenbrüchen schützen

Immer mehr Softwareprogramme werden von immer weniger Firmen bereitgestellt. Auch deshalb erfasste die IT-Panne die halbe Welt. Digitale Emanzipation ist nötig



Michael Andrick



20.07.2024 · 20.07.2024, 14:51 Uhr



Die globale IT-Panne am 19. Juli 2024 ist auf ein fehlerhaftes Update zurückzuführen.

Fotoillustration: BLZ. Foto: Hartono Creative Studio/Unsplash



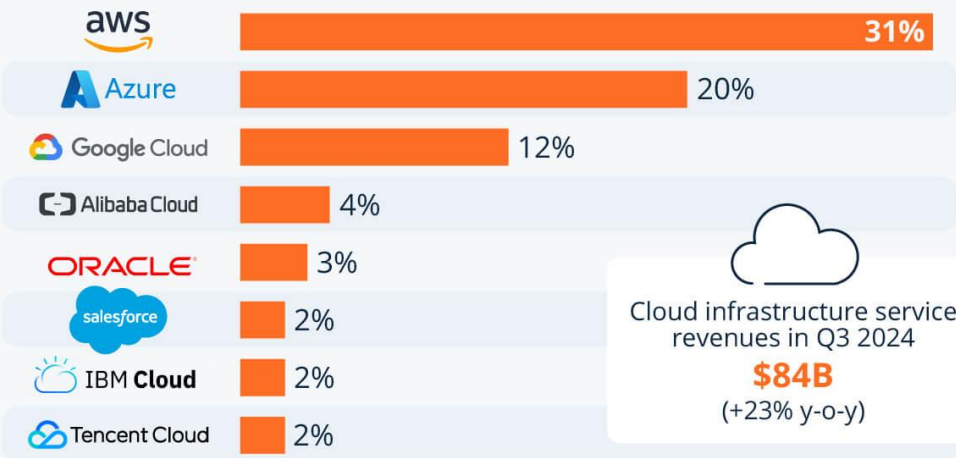
Weltweit Probleme

Störung bei Amazon legt zahlreiche Online-Dienste lahm

Stand: 20.10.2025 15:15 Uhr

Amazon Maintains Dominant Lead in the Cloud Market

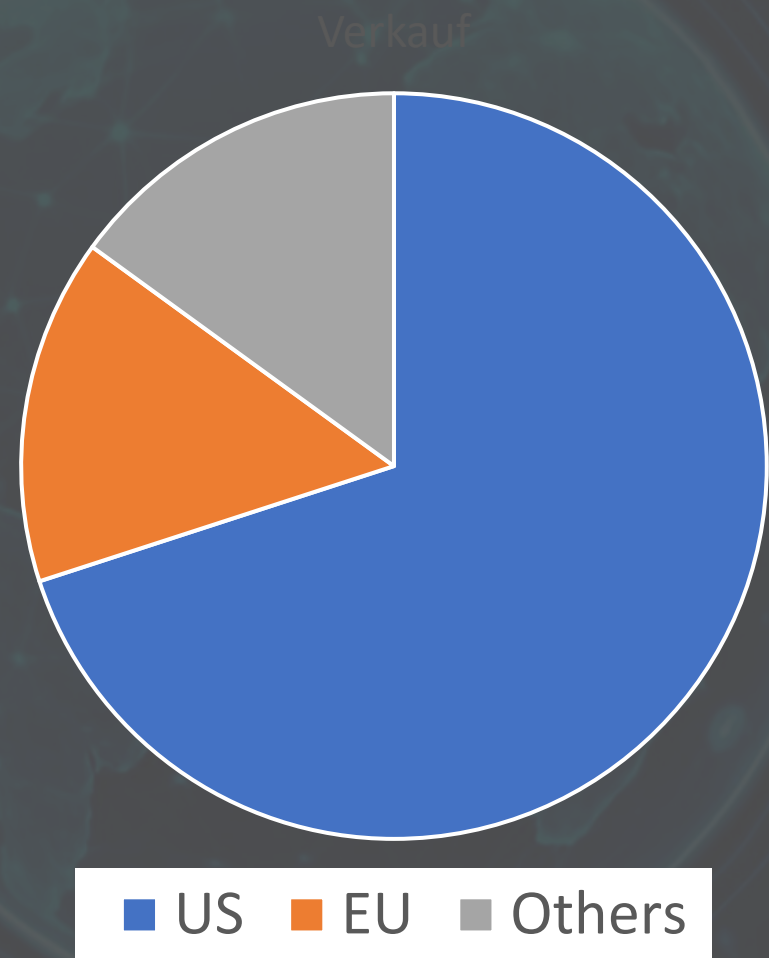
Worldwide market share of leading cloud infrastructure service providers in Q3 2024*



Cloud infrastructure service revenues in Q3 2024
\$84B
(+23% y-o-y)

* Includes platform as a service (PaaS) and infrastructure as a service (IaaS) as well as hosted private cloud services

Source: Synergy Research Group



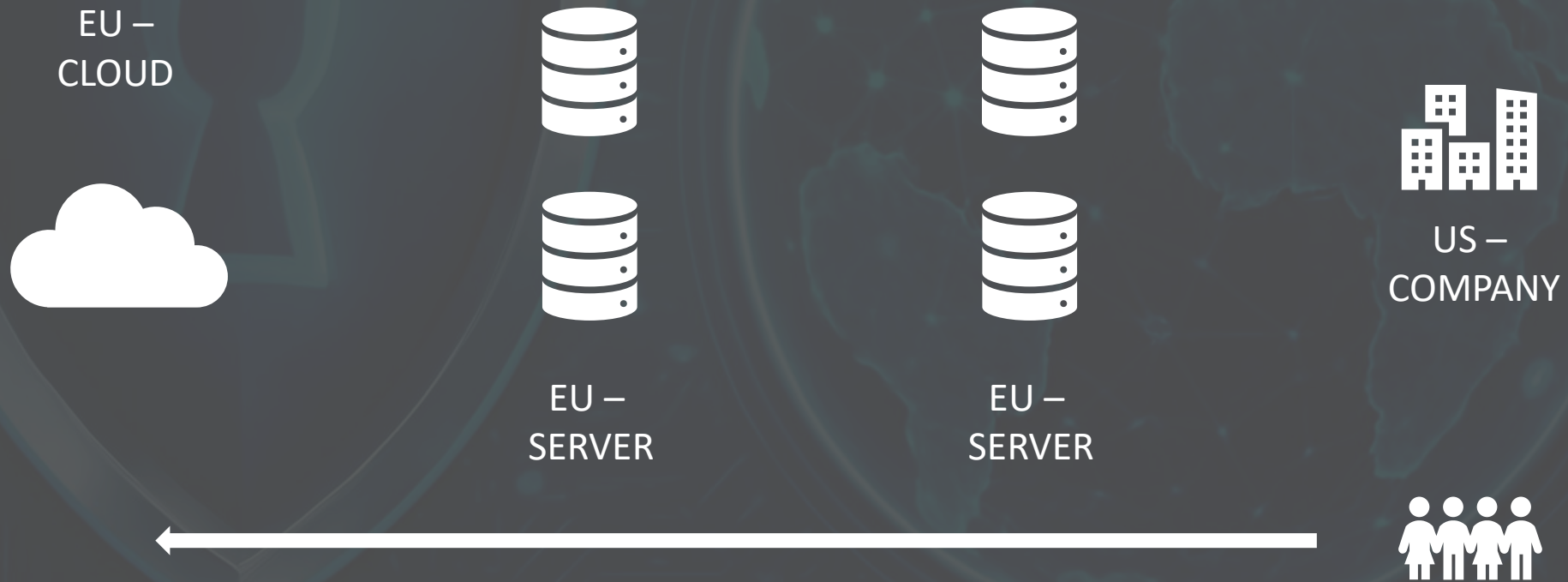
Technik

Wirtschaft

Recht

Ethik

Kann Technik wirklich digitale Souveränität sicherstellen, wenn internationale Gesetze wie der US CLOUD Act extraterritorial wirken und Zugriff auf Daten fordern?



Sind europäische Datenschutzregelungen nur theoretisch wirksam, solange US-Gesetze weltweit Datenzugriff erzwingen können?

Die Lösung – Data Privacy Framework (DPF)

Das DPF beruht auf der US-Executive Order 14086 (Joe Biden vom 7. Oktober 2022), die Grundsätze zur Beschränkung von US-Geheimdienstzugriffen und ein unabhängiges Kontrollgremium (Privacy and Civil Liberties Oversight Board – PCLOB) einführte.

Government Surveillance

What the PCLOB Firings Mean for the EU-US Data Privacy Framework

February 14, 2025 / [Silvia Lorenzo Perez](#)

Widersprüchliche Anforderungen schaffen Unsicherheiten:

- Europäische Unternehmen sind hin- und hergerissen zwischen DSGVO-Konformität und US-Gesetzen mit extraterritorialer Wirkung.
- Dies führt zu rechtlicher Unsicherheit, erhöhten Compliance-Kosten und erschwert klare Strategien.

Ist digitale Souveränität wirtschaftlich tragbar – und für welche Unternehmen lohnt sich der Aufwand wirklich?

- Datenschutz
- Compliance
- Transparenz
- Kontrolle
- Rechtliche Klarheit



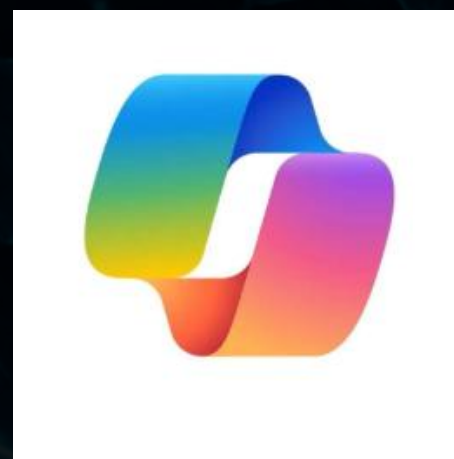
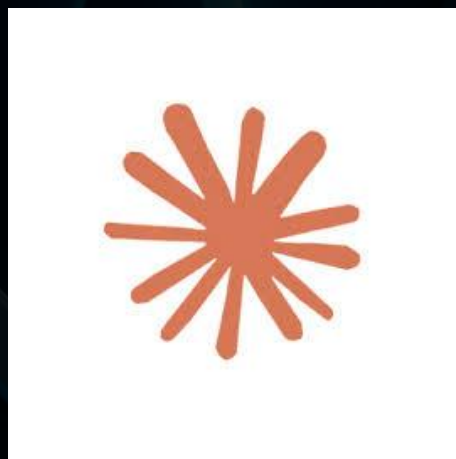
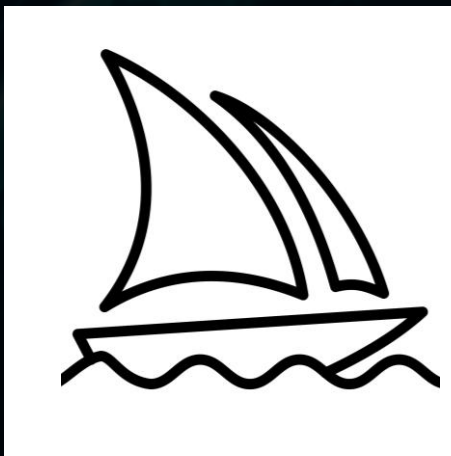
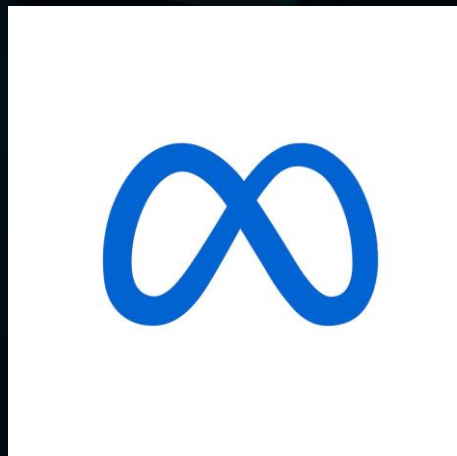
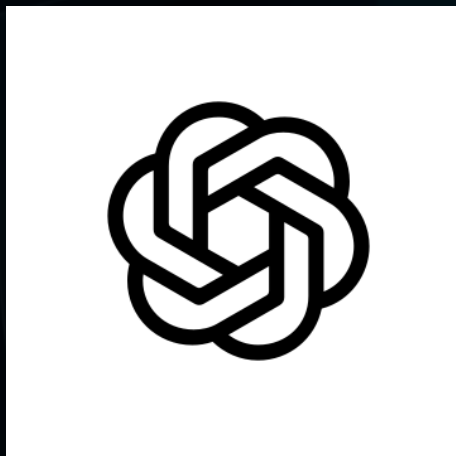
- Skalierbarkeit
- „Kosten“
- Breit aufgestellt
- Renomiert
- Innovation und KI 😄

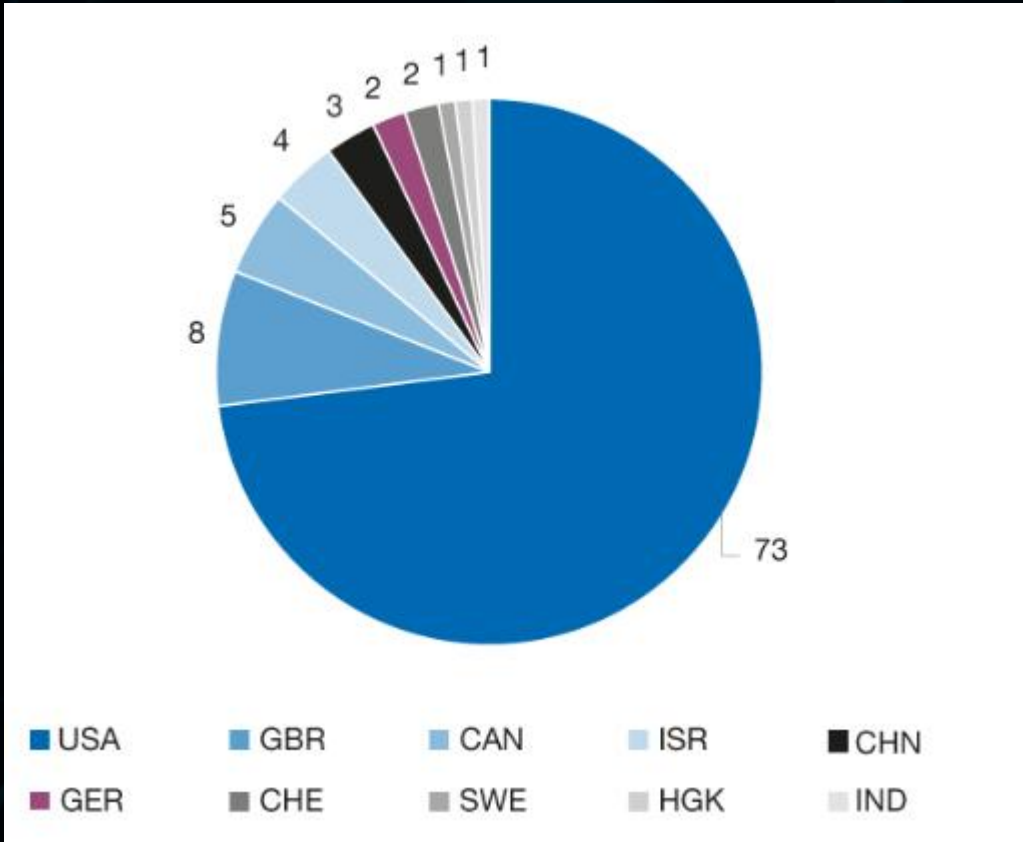


Wer wäre bereit, Mehrkosten oder Einschränkungen in Komfort zu akzeptieren, wenn dadurch echte digitale Souveränität und Datenschutz gewährleistet wäre?

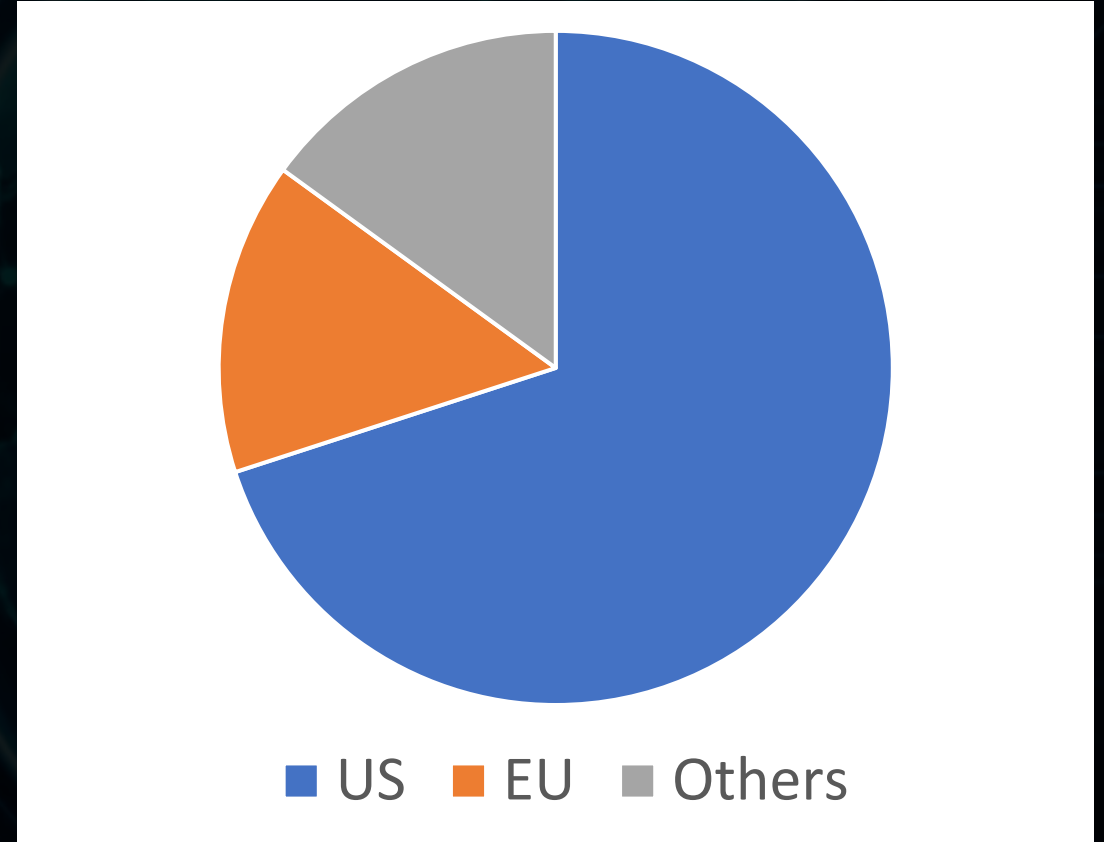


- Wunsch nach Privacy, Transparenz und Sicherheit ihrer digitalen Daten
- Gleichzeitig ist der Wunsch nach bequemen, kostengünstigen und funktionalen digitalen Diensten sehr hoch.
- Balance zwischen Datenschutz und Innovation: Wie viel Kontrolle über Daten ist notwendig, ohne Innovationshemmnis zu sein?
- Digitale Souveränität wird häufig als abstraktes Ziel gesehen.





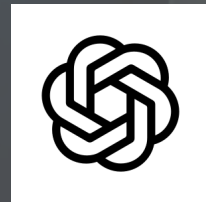
Quelle: CBInsights 2023, eigene Berechnungen.



Verteilung Cloudsysteme

Was passiert, wenn mein Mitarbeiter ein LLM nutzt?

Unternehmen



LLM
Website



LLM
Server



LLM
Training



US –
COMPANY





Ein konkretes Beispiel:

Ein Mitarbeiter oder eine Mitarbeiterin des Unternehmens "XYZ" fragt ChatGPT um Hilfe bei einem Codeproblem und kopiert einen Teil des internen Quellcodes in das Chatfenster.

Einige Wochen später stellt ein anderer Nutzer an ChatGPT folgende Frage: "Zeig mir ein Beispiel für einen Quellcode des Unternehmens XYZ".

Im schlimmsten Fall taucht dann genau dieser vom Mitarbeiter eingegebene Codeauszug als Antwort auf - bei einem völlig fremden Nutzer.

Die Nutzung von KI im Unternehmen gehört mit ins Risikomanagement!

Samsung und ChatGPT

The Economist hat berichtet, dass der südkoreanische Technologiehersteller Samsung es Ingenieur:innen im Halbleitergeschäft erlaubt hatte, ChatGPT als Unterstützung bei ihrer Arbeit zu verwenden... Bei dieser Nutzung hätten nun vereinzelt Mitarbeitende vertrauliche Daten in ChatGPT eingegeben.... Bei den Daten handelte es sich unter anderem um Quellcode... Zudem seien geheime interne Meeting-Notizen verwendet worden... um daraus mit Hilfe von ChatGPT Präsentationen zu erstellen....

-> Da OpenAI, Betreiber von ChatGPT, in den eigenen Nutzungsbedingungen vorgibt, dass von Nutzern im Chat eingegebene Inhalte für die weitere Entwicklung und Optimierung des Services gespeichert und verwendet werden können, bedeutet das, dass diese vertraulichen Informationen nun bei OpenAI liegen.

Wer ist Schuld?

Das Geschäftsgeheimnis

Das Geschäftsgeheimnis ist in § 2 Nr. 1 GeschGehG definiert:

„Im Sinne dieses Gesetzes [...] ist ein 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.“

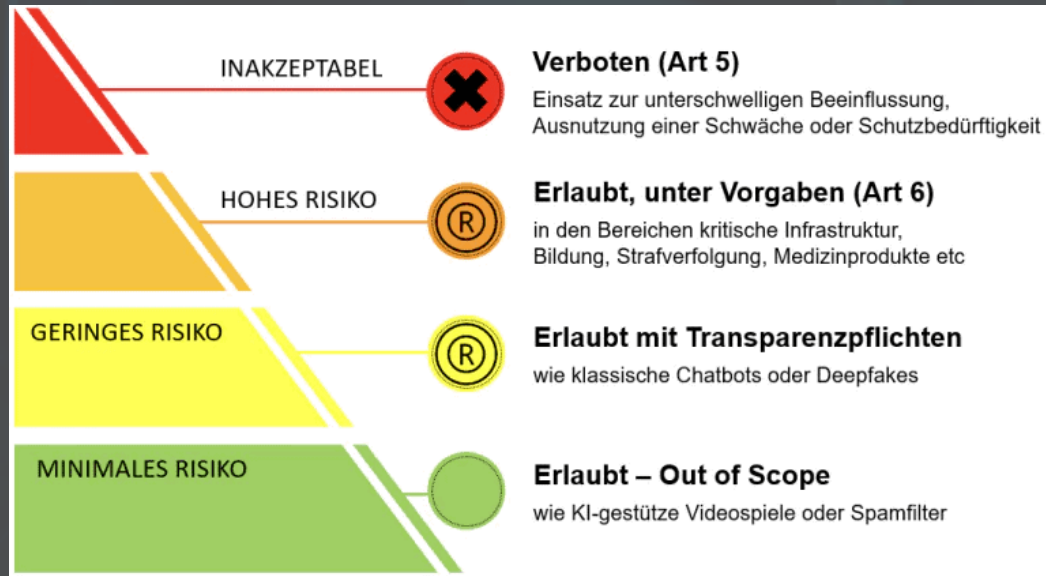
Mitarbeiter

Personen, die mit dem Geschäftsgeheimnis betraut sind und ChatGPT verwenden (Nutzer) können durch die Nutzung als Rechtsverletzer im Sinne des § 2 Nr. 3 GeschGehG eingestuft werden. Demnach ist ein „Rechtsverletzer jede natürliche oder juristische Person, die entgegen § 4 ein Geschäftsgeheimnis rechtswidrig erlangt, nutzt oder offenlegt“, solange keine Ausnahme nach § 5 GeschGehG vorliegt.

-> Verunsicherung!

LLM – Betreiber

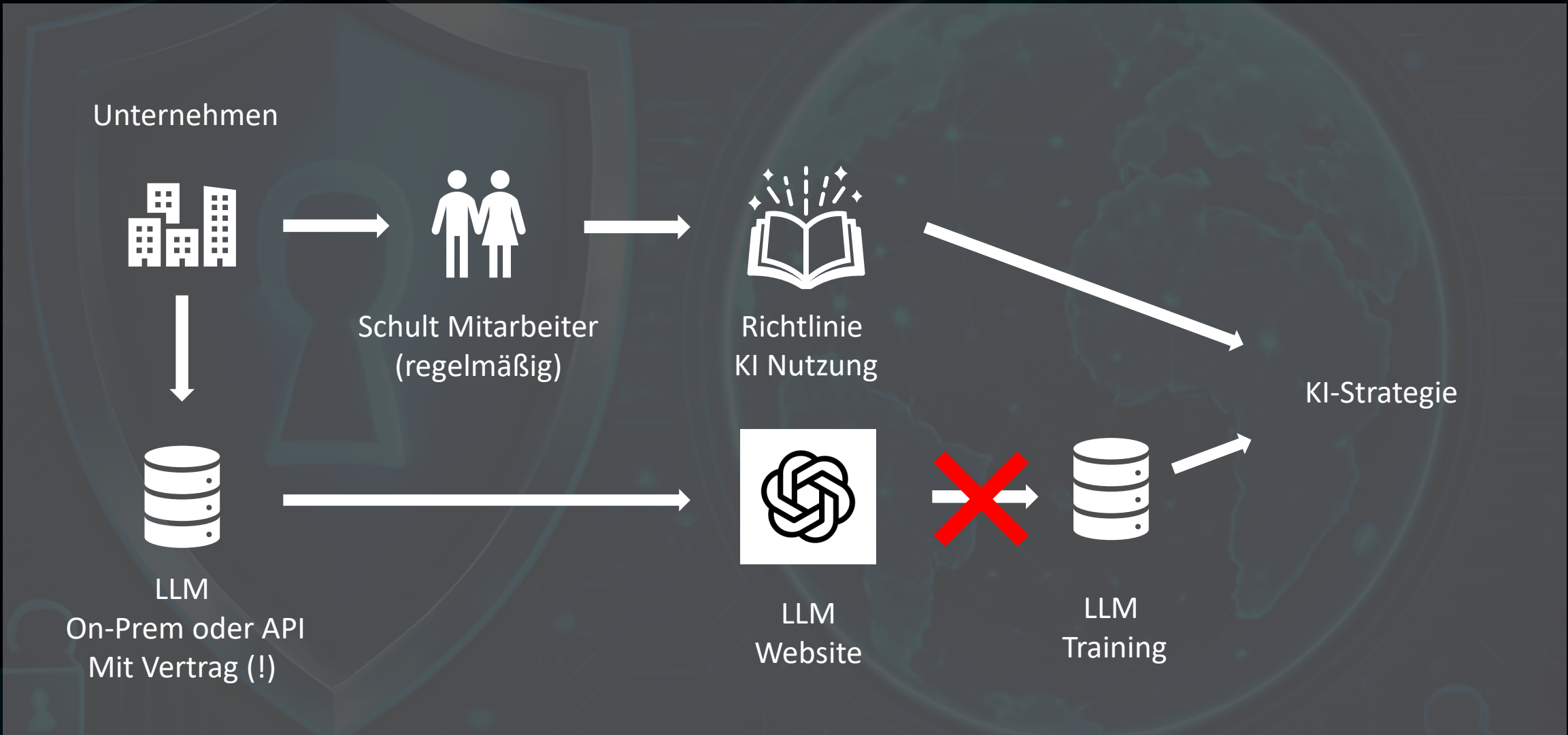
Gemäß § 4 Abs. 3 S. 1 GeschGehG setzt eine Einordnung als Rechtsverletzer voraus, dass OpenAI „das Geschäftsgeheimnis über eine andere Person erlangt hat und zum Zeitpunkt der Erlangung, Nutzung oder Offenlegung weiß oder wissen müsste, dass diese das Geschäftsgeheimnis entgegen Absatz 2 genutzt oder offengelegt hat“.



Pflichten für Unternehmen nach Artikel 4 AI Act

- Unternehmen müssen Maßnahmen ergreifen, um ein „ausreichendes Maß an KI-Kompetenz“ bei ihrem Personal zu gewährleisten
- Die Pflicht gilt für alle, die KI-Systeme bereitstellen oder betreiben – also sowohl Hersteller als auch Unternehmen, die KI in ihrem Betrieb nutzen (auch wenn die Tools extern bezogen werden)
- Es ist keine einmalige Schulung, sondern ein fortlaufender Prozess
- Die Kompetenzvermittlung muss dokumentiert werden
- Auch Dritte wie externe Dienstleister sind in diese Schulungspflicht einzubeziehen.
- Die KI-Kompetenzen sollen je nach Rolle und Kontext abgestuft vermittelt werden

Datentransfer zum Hersteller
Ungeregelte Nutzung
Schuldfrage
AI-Act



Zurück zur Digitalen Souveränität (und zur Convenience Falle)

„Wie viel Komfort und Kostenvorteil sind wir als Gesellschaft bereit aufzugeben, um echte digitale Souveränität zu erreichen?“

„Sollte Europa in Kauf nehmen, technologisch langsamer zu sein, wenn dadurch mehr Datenschutz und Unabhängigkeit gesichert werden?“

„Können wir internationalen Cloud-Anbietern jemals wirklich vertrauen – oder brauchen wir 100 % europäische Lösungen?“

„Wie lässt sich digitale Souveränität mit globaler Zusammenarbeit und Datenaustausch vereinbaren, ohne Sicherheit einzubüßen?“

„Wer trägt letztlich die Verantwortung für digitale Souveränität – Politik, Unternehmen oder jede/r Einzelne?“



LinkedIn
/stefan-pilarczyk



Vielen Dank!

Fragen?