Datensouveränität und KI

Datenschutz, Datensicherheit, Vertraulichkeit

Harald Wagener

- Gruppenleiter Cloud und IT,
  Zentrum für Digitale Gesundheit, BIH, Charité
  Universitätsmedizin Berlin

- Aufbau und Betrieb von Forschungs-IT
- Zunehmend mit Schwerpunkt auf Inhouse-KI-Lösungen
- Notwendig, da hochsensible Daten verarbeitet werden

“Datensouveränität”

- Politischer Begriff
- Europäische / Nationale Hegemonie



Ich ziehe den Begriff **Datenautonomie** vor

Datenautonomie

- Kontrolle darüber,
  wann welche Daten zu welchem Zweck verwendet werden
- Freie Wahl der Werkzeuge und des Speicher-Ortes
- Ein “Deutsches Amazon” erfüllt die Ziele der
  Datensouveränität, aber nicht der Datenautonomie

KI ist ein Multiplikator



- In den Händen von Fachleutenist KI ein **Multiplikator**
- KI muss **gezielt** verwendetwerden
  (Harness, Skills, etc.)
- KI braucht
  - Spezifische **Aufgaben** und
  - Spezifischen **Input** (“Kontext”)
- Je genauer der Kontext, je klarer die Aufgabenstellung,
  desto besser können die Ergebnisse sein
  ”Jedes Arbeitsergebnis ist im besten Fall so gut wie das Briefing”

Wer betreibt KI? Warum?

- Große IT Firmen mit viel Hardware
  (KI als Service)
- Große Organisationen mit eigenen Ressourcen, auch Dienstleister
- Forschungseinrichtungen
- Enthusiasten (-:



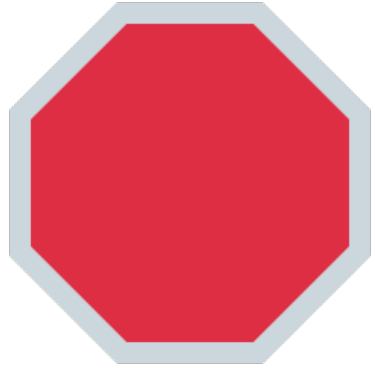
- Regulatorik, Vertraulichkeit, Kostenoptimierung

Abstrakte Risiken

- Was passiert mit meinen Daten?
  - Wie werden sie ausgewertet oder monetarisiert?
- Wem verrät die KI meine Geschäftsgeheimnisse?
  - absichtlich oder auch unabsichtlich
- Geschäftsgeheimnisse schützen?
- Geschäftsvorteile/-nachteile?



Konkrete Gefahren



- Ungesteuerter, ungeplanter Einsatz von KI (Martin #8)
- Risiko und Nutzen müssen gegeneinander abgewogen werden
- Upload vertraulicher Daten und Informationen an “Unbekannte Dritte”
- Kostenexplosion (aktuelle Abos Faktor 10-20 zu niedrig)

Nichtlösungen



- Multicloud
- Multi-KI
- EiGenVerAntWoRTuNG der Mitarbeitenden

  → KI ist auch ein **Risiko-Multiplikator**
- Risikominimierung: Beim Anbieter bleiben

  → "Wenn Deine Infrastruktur eh auf Microsoft 365 läuft, steigt das Risiko nicht, wenn Du CoPilot verwendest!"

Können KMUs KI zuhause betreiben?

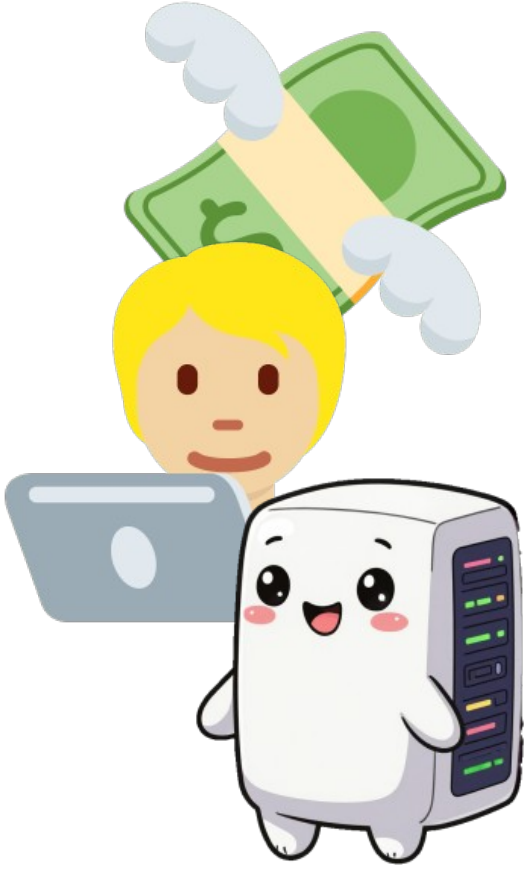
- Ende 2025: Ausgeschlossen
- Ende 2026: Ja! (Inferenz, Tuning)
- Open Weights in 2026 besser als Frontier Models in 2025

Aber: Mit Einschränkungen!



Lösungsansätze

- KI nur gezielt einsetzen
- Kontext, Tooling, Zielstellung, Meßbarkeit
- KI nur selbst betreiben, wenn man die
- Ressourcen dafür einsetzen kann und will:
  - Wissen
  - Geld
  - Betriebs Know-How



Q&A mit Martin

Alle Bilder emojipedia.org