

TeleTrust-Konferenz

Berlin, 26.06.2026

Digitale Souveränität

Dr. André Kudra, esatus / TeleTrust-Vorstand

Zwei Arten von Abhängigkeit

⚠ **Ärgerlich: Verfügbarkeit**

- Juli 2025: Microsoft-Cloud fällt 19 Stunden aus
- Oktober 2025: Azure-Front-Door – halb Europa betroffen
- Lösbar: Redundanz, bessere SLAs

🚨 **Gefährlich: Souveränität**

- Mai 2026: Microsoft übermittelt interne Kommunikation niederländischer DSA-Behörden ans US-Repräsentantenhaus – ungeschwärzt
- Kein CLOUD-Act-Fall: parlamentarische Vorladung für Microsofts eigene Korrespondenz
- Strukturelle Abhängigkeit – nicht durch individuelle Hygiene lösbar

Data residency ≠ Data sovereignty

Lagebild: Drei Zahlen

1 – Technologiebasis

- > 4/5 der genutzten Kerntechnologien in Europa sind importiert
- Nur 4 der 50 größten Tech-Unternehmen weltweit sind europäisch (Draghi 2024)
- Investitionslücke: 800 Mrd. € jährlich laut Draghi-Report (Digitalisierung, Green Tech, Verteidigung)

2 – Schadensentwicklung

- DE: 220 Mrd. € (2021) → ~280–300 Mrd. € (2025) – wir werden teurer, nicht sicherer

3 – Hardware-Abhängigkeit

- Chips: TSMC und ASML dominieren – Volumenfertigung weitgehend außerhalb Europas
- EU Chips Act: Ziel 20 % Weltmarktanteil 2030 – aktueller Stand: ~10 %
- KI-Chips: Nvidia ~80 % Marktanteil; kein europäischer Hersteller wettbewerbsfähig

KI: Eine tiefere Abhängigkeit besteht

Rechenkapazität ist nur der Anfang

- EU: ~5 % globale KI-Rechenkapazität | USA: ~75 % (Epoch AI, Mai 2025)
- 5 Hyperscaler besitzen > 2/3 davon – kein einziges europäisches Unternehmen (Epoch AI, April 2026)

Verfügbarkeit der Modelle

- 12. Juni 2026: US-Regierung erlässt Exportkontrolle
 - Anthropic sperrt Frontier-Modelle (wie Fable) weltweit für Nicht-US-Bürger
- EU-Finanzminister hatten Zugang zu Mythos für Bankensicherheit beantragt – Washington: Nein
- Eine ausländische Regierung kann Werkzeuge abschalten, die in europäischen Unternehmen, Universitäten und Behörden verankert sind

„Wer Daten, Rechenleistung und Zieldefinition kontrolliert, entscheidet, was diese Technologie mit Menschen macht.“

– Paolo De Rosa, Policy Officer, EU-Kommission

Das Spannungsfeld auf den Punkt gebracht

Das Bewusstsein ist da. Die Investitionsbereitschaft fehlt.

- Deutlich steigende Unternehmensinsolvenzen in Deutschland
- IT-Budgets unter Druck – keine Risikokapazität für Wechselprojekte
- Rationale Reaktion auf schwierige Wirtschaftslage

Aber: Was kostet die Abhängigkeit?

- KI-Infrastruktur als geopolitische Verhandlungsmasse
- Organisationen können Vertraulichkeit ihrer Kommunikation nicht mehr garantieren
- Modellzugang kann per Dekret über Nacht entzogen werden – wie am 12. Juni geschehen

Souveränität ist teuer. Abhängigkeit ist teurer. Die Rechnung kommt später.

Drei Forderungen

1 Souveränität ist Steuerungsleistung – kein Label, kein Standort

- Schlüsselfrage: Wer kann das System zum Sprechen bringen – auf wessen Anweisung?
- Server Frankfurt + US-Anbieter = lokaler Server mit amerikanischem Schlüssel
- Bei KI: Trainingsdaten, Zieldefinitionen, Auditierbarkeit ebenso entscheidend

2 Staat als Ankerkunde – mit verbindlichen Kriterien

- BMDS 16.06.2026: Deutschland-Stack positioniert Staat als Ankerkunden
- Versprechen ≠ Beschaffungsauftrag: Security by Design, BoM, KI-Auditierbarkeit

3 „Governed Interdependence“ statt ertragener Abhängigkeit

- Nicht Autarkie – souveräne Bedingungen als Beschaffungsvoraussetzung
- Gilt auch für KI-Modelle: Zugangsbedingungen vertraglich und regulatorisch absichern – stets Alternativen schaffen
- „Anspruchsvoll in der Kontrolle, mutig in der Nutzung“ (De Rosa)

Was möglich und verfügbar ist

Verfügbare Optionen heute

- IONOS + Nextcloud Workspace (4.6.2026): M365-Alternative, deutsche Infrastruktur
- STACKIT: BMDS-KI-Plattform-Zuschlag (Mai 2026), EU-Kommissions-Ausschreibung
- Telekom Industrial AI Cloud (Feb. 2026): 80 % Kernfunktionsparität
- govdigital gd.Cloud-Broker: Bund, Länder, 85 % Kommunen
- KI-Modelle: Mistral (FR) + Aleph Alpha/Cohere (DE/CA, April 2026) – europäische Frontier-Alternativen entstehen

Die Richtung stimmt.

- Konsistenter politischer Wille in Beschaffung, Regulierung, Förderung fehlt noch

Ehrliche Einschränkungen

- Leistungsabstand zu US-Hyperscalern bei KI-Integration real
- Migrationen aufwändig – nicht jeder Workload gleichwertig substituierbar
- Markt fragmentiert – „Souveränität“ als Marketingbegriff weit verbreitet

„Es wäre möglich gewesen. Es gab eine Chance – und wir haben es nicht einmal versucht.“

– Europe 2031, eine dystopische Szenario-Studie

<https://europe2031.ai>

Überblick: Dimensionen Digitaler Souveränität

Technisch-kryptografisch

- Manipulationssichere Verarbeitung (Laufzeitintegrität)
- Verifizierbarkeit / Remote Attestation
- Schlüsselhoheit (eigene Krypto-Schlüssel)
- Hardware-Sicherheitsankerpunkt

Kontroll- und Governance-Ebene

- Datenkontrolle (wer hat Zugang, wo gespeichert)
- Wechselfähigkeit / Vendor-Lock-in-Vermeidung
- Souveränität als Steuerungsleistung (nicht als Label)
- Residency ≠ Sovereignty (Standort ≠ Kontrolle)
- Hardware-Sicherheitsankerpunkt

Rechtlich-regulatorisch

- Rechtliche Autonomie / eigene Gesetzgebung
- Zertifizierungsrahmen (BSI C5, EUCS, AUDITOR)

Strategisch-ökonomisch

- Technologische Unabhängigkeit / europäische Anbieter
- Nachhaltigkeit / CO₂ als Souveränitätsdimension
- Individuelle / nutzerorientierte Souveränität

Operationalisierung / Messbarkeit

- Stufenmodell / Klassifizierungsschema
- Marktfähige Produktumsetzung heute

Digitale Souveränität

TeleTrust arbeitete schon daran, als sonst noch niemand davon geredet hat. Ich lade Sie ein, mitzumachen.

Dr. Andre Kudra | andre.kudra@teletrust.de