



Rechenzentren, Cloud & Edge:  
Strategische Infrastruktur für KI und  
datengetriebene Anwendungen

---

*Positionspapier*

*Die Stimme der Sozialen  
Marktwirtschaft*

## Einleitung

Deutschland steht vor der zentralen Herausforderung, seine Rechen- und Cloudinfrastruktur so weiterzuentwickeln, dass sie zukunftsfähig, resilient, sicher und international wettbewerbsfähig bleibt. Leistungsstarke, energieeffiziente und zuverlässige Rechenzentren — ergänzt durch moderne Cloud- und Edge-Architekturen — bilden die Grundlage für digitale Transformation, wirtschaftliche Wettbewerbsfähigkeit und datenintensive Anwendungen im Bereich der Künstlichen Intelligenz (KI).

Die deutsche Rechenzentrumslandschaft zeigt bereits heute beachtliche Leistungsfähigkeit und ein deutliches Wachstum. Laut aktuellen Analysen liegt die Gesamt-IT-Anschlussleistung aller relevanten Einrichtungen im Jahr 2024 bei rund 2.730 Megawatt (MW) und wird 2025 auf etwa 2.980 MW steigen. Besonders deutlich wächst das Segment der Co-Location-Rechenzentren: Erstmals decken sie über 50 Prozent der gesamten Kapazität ab und verzeichnen 2025 ein Wachstum von rund 17,5 Prozent.<sup>1</sup>

Ein zentraler Treiber dieses Wachstums sind Cloud- und KI-Infrastrukturen, deren IT-Anschlussleistung auf etwa 1.450 MW geschätzt wird.<sup>2</sup> Damit entfällt inzwischen fast die Hälfte der deutschen Rechenzentrumskapazitäten auf Cloud-Lösungen — im Vorjahr waren es noch 45 Prozent, 2019 lediglich 29 Prozent. Dies verdeutlicht, dass Cloud-Anwendungen mittlerweile den zentralen Wachstumstreiber darstellen. Parallel gewinnt das Segment der Edge-Rechenzentren an Bedeutung, auch wenn ihr Anteil aktuell noch moderat ist: Für 2025 wurde ihr Anteil an der Gesamt-RZ-Kapazität auf rund 8 Prozent geschätzt. Edge-Rechenzentren ergänzen zentrale Cloud-Strukturen, indem sie Rechenleistung in unmittelbare Nähe zu den Nutzern oder Anwendungen bringen und so besonders kurze Reaktionszeiten ermöglichen — eine entscheidende Voraussetzung für latenzsensitive und datenintensive Anwendungen.<sup>3</sup>

In der Gesamtschau zeigt sich ein tiefgreifender Strukturwandel: Weg von vielen kleinen, klassischen Serverräumen hin zu wenigen, leistungsstarken Co-Location-, Cloud- und Edge-Rechenzentren. Dieser Wandel spiegelt den wachsenden Bedarf an skalierbarer Rechenleistung, Cloud- und KI-Diensten sowie an latenzarmen, dezentralen Lösungen wider, die die digitale Transformation und innovative Anwendungen — insbesondere im Bereich Business AI und agentischer KI — effizient unterstützen.<sup>4</sup>

Diese strukturellen Entwicklungen sind von zentraler Bedeutung für die breite Nutzung von KI. Moderne Anwendungen — vom Training großer neuronaler Netze über Echtzeitanalysen bis zu generativen KI-Modellen — erfordern erhebliche Rechenleistung, große Speicherkapazitäten, hohe Netzwerkbandbreite und niedrige Latenzzeiten.

---

<sup>1</sup> Bundesministerium für Wirtschaft und Energie, Status and development of the German data centre landscape – Executive Summary, 31.03.2025, <https://www.bundeswirtschaftsministerium.de/Redaktion/EN/Publikationen/Digitale-Welt/status-and-development-of-the-german-data-centre-landscape-executive-summary.pdf>.

<sup>2</sup> Borderstep Institute, Rechenzentren in Deutschland – Aktuelle Marktentwicklungen und Trends, <https://www.borderstep.de/projekte/rechenzentren-in-deutschland>.

<sup>3</sup> Bitkom e.V., Rechenzentren in Deutschland, Aktuelle Marktentwicklungen 2025, <https://www.bitkom.org/sites/main/files/2025-11/bitkom-studie-rechenzentren-in-deutschland-2025.pdf>.

<sup>4</sup> Data Center Impact Report Deutschland 2024, [https://www.germandatacenters.com/fileadmin/images/DCIRD-24/Data-Center-Impact-Report-Deutschland-2024\\_EN.pdf](https://www.germandatacenters.com/fileadmin/images/DCIRD-24/Data-Center-Impact-Report-Deutschland-2024_EN.pdf).

Nur eine skalierbare, zuverlässige und leistungsfähige Infrastruktur ermöglicht, dass solche Workloads effizient und sicher ausgeführt werden können.

Gleichzeitig bringt die Entwicklung Herausforderungen mit sich: Die starke Konzentration auf wenige Regionen erhöht das Risiko von Anbieter- oder Standortabhängigkeiten. Hinzu kommen Fragen der Energieversorgung, Netz- und Strominfrastruktur, Nachhaltigkeit und Umweltbelastung — insbesondere angesichts des hohen Energie- und Kühlbedarfs moderner Rechenzentren.

Datenschutz, Sicherheitsstandards und Cyber-Resilienz müssen konsequent berücksichtigt werden, vor allem bei sensiblen oder kritischen KI- und Datenanwendungen. Darüber hinaus ist die Schaffung allgemeiner Planungssicherheit für die Weiterentwicklung der bestehenden Rechenkapazität eine zentrale Aufgabe, die eine enge und effektive Zusammenarbeit zwischen Wirtschaft, Politik und Verwaltung erfordert.

Daraus folgt: Deutschland benötigt eine robuste, diversifizierte und souveräne Rechenzentrumslandschaft, die sowohl Co-Location- als auch Hyperscale-Infrastrukturen umfasst und zugleich gegenüber dem wachsenden und sich verändernden Bedarf an Rechenleistung weiterentwickelt wird. Co-Location-Rechenzentren bieten insbesondere kleinen und mittelständischen Unternehmen einen kosteneffizienten Zugang zu moderner IT-Infrastruktur, sicheren Netzwerken und Cloud-Integrationen. Hyperscale-Rechenzentren liefern die erforderliche Leistung für hochskalierbare Anwendungen, Cloud-Dienste und das Training großer KI-Modelle und sind damit für die internationale Wettbewerbsfähigkeit unverzichtbar. Diese komplementäre Struktur bildet das Fundament für eine langfristige strategische Vision bis 2050: eine hyper-distribuierte Edge-Cloud-Architektur, in der zentrale Hyperscale-Standorte mit einer Vielzahl von Micro- und Nano-Rechenzentren in urbanen Räumen, Industrieanlagen und kritischen Infrastrukturen intelligent vernetzt sind. In einem solchen Ökosystem erfolgt Datenverarbeitung weitgehend lokal mit niedrigen Latenzzeiten, während autonome Load-Balancing-Cluster und softwaredefinierte Netzwerke Rechenlast dynamisch, effizient und resilient verteilen.

KI wird dabei nicht nur als Anwendungsfall auftreten, sondern integraler Bestandteil des Rechenzentrumsbetriebs sein: KI-gestützte Ressourcenallokation, automatisierte Fehlerdiagnose, Predictive Maintenance, energieoptimierte Workload-Steuerung und intelligente Sicherheitsüberwachung steigern Effizienz, Resilienz und Nachhaltigkeit gleichermaßen. Gleichzeitig müssen Rechenzentren schrittweise in ein nachhaltiges Energiesystem integriert werden — durch sektorübergreifende Kopplung, flexible Laststeuerung, Abwärmenutzung auf Quartiersebene sowie die direkte Anbindung an erneuerbare Energiequellen.

Nur wenn Deutschland die heutige Infrastrukturvielfalt konsequent weiterentwickelt und mit einer solchen langfristigen Architekturvision verbindet, kann es seine Wettbewerbsfähigkeit sichern und sich dauerhaft als Standort für KI-Innovationen, datengetriebene Geschäftsmodelle und technologische Zukunftsfähigkeit positionieren.

## 1. Anforderungen an Infrastruktur für KI-Entwicklung und Anwendung

Die erfolgreiche Entwicklung und Anwendung von KI ist eng mit der Verfügbarkeit einer leistungsfähigen, skalierbaren und resilienten Infrastruktur verbunden. Diese bildet die Grundlage für die Verarbeitung der enormen Datenmengen, die für das Training und den operativen Einsatz von KI-Modellen und Business-Anwendungen erforderlich sind. Es ist von entscheidender Bedeutung, die unterschiedlichen technischen Anforderungen nach Bedarf anzupassen – das Training und die operative Anwendung – klar zu differenzieren, da sie jeweils spezifische infrastrukturelle Ansätze verlangen.

### a) Leistungsstarke Rechenressourcen für die KI-Modellentwicklung

Das Training großer KI-Modelle, insbesondere neuronaler Netze, ist nur durch den Einsatz hochleistungsfähiger Rechenressourcen und spezialisierter Hardware wie GPUs und TPUs möglich. Diese Technologien sind notwendig, um die für das Training erforderlichen großen Datenmengen in kurzer Zeit effizient und parallel zu verarbeiten.

Gleichzeitig ist eine gut strukturierte Dateninfrastruktur unerlässlich. Um KI-Modelle effizient zu trainieren, müssen Daten in strukturierten Datenpools (wie z.B. Data Lakes) vorgehalten werden. Die Datenqualität, ihre Verfügbarkeit sowie die Einhaltung von Datenschutz- und Sicherheitsanforderungen sind zentrale Faktoren für die Leistungsfähigkeit und Akzeptanz von KI-Anwendungen. Fehlen solche gut organisierten und gesicherten Datenpools, wird der gesamte Trainingsprozess ineffizient und das Vertrauen in KI-Anwendungen kann erheblich beeinträchtigt werden. Daher sollte die europäische Datenstrategie eng mit der Infrastrukturpolitik verknüpft sein.

### b) Infrastruktur für operative KI-Anwendungen: Edge Computing und On-Premise-Lösungen

Für den operativen Einsatz von KI, insbesondere in zeitkritischen Anwendungen wie autonomem Fahren oder industrieller Automatisierung, sind die Anforderungen an die Infrastruktur besonders hoch, insbesondere hinsichtlich niedriger Latenzzeiten. In solchen Szenarien ist Edge Computing von zentraler Bedeutung: Die Datenverarbeitung findet direkt an der Quelle statt – also nahe an den Sensoren oder Endgeräten – was schnelle Reaktionszeiten ermöglicht und gleichzeitig Bandbreitenressourcen schont. Dies ist besonders wichtig für Anwendungen, die Echtzeitentscheidungen erfordern.

Ein weiteres Schlüsselement für die KI-Infrastruktur sind On-Premise-Lösungen. Diese ermöglichen es Unternehmen, ihre Daten intern zu verarbeiten, wodurch sie höchsten Datenschutz- und Sicherheitsanforderungen gerecht werden. Besonders für sensible Daten – etwa aus der Gesundheitsversorgung oder sicherheitskritischen Bereichen – ist der Einsatz von On-Premise-Infrastrukturen unverzichtbar.

Diese Lösungen gewährleisten nicht nur die Einhaltung von regulatorischen Vorgaben, sondern können für den Mittelstand auch eine kostengünstige Möglichkeit darstellen, KI-Technologien ohne Abhängigkeit von externen Cloud-Diensten zu integrieren. Dies stärkt die Resilienz und gibt den Unternehmen mehr Kontrolle über ihre sensiblen Daten.

Für eine langfristig erfolgreiche KI-Strategie ist daher eine multifunktionale Infrastruktur erforderlich, die sowohl **Cloud-** als auch **Edge-Technologien** sowie **On-Premise-Lösungen** integriert. Hybride Infrastrukturen, die diese verschiedenen Architekturtypen kombinieren, bieten eine hohe Flexibilität und können den unterschiedlichen Anforderungen der KI-Anwendungen in verschiedenen Sektoren gerecht werden. Sie ermöglichen es, sowohl große Rechenzentren für das Modelltraining als auch kleinere, spezialisierte Modelle für die Inferenz direkt im Unternehmen oder am Rand des Netzwerks zu betreiben.

#### **c) Skalierbarkeit der Rechenkapazitäten und Wachstumschancen für Unternehmen**

Die KI-Infrastruktur muss skalierbar sein, um den stetig wachsenden Anforderungen gerecht zu werden, die durch die zunehmende Nutzung von KI-Anwendungen entstehen. Die Potenziale von KI liegen für die Wirtschaft in Europa und Deutschland vor allem im spezifischen Branchenwissen, das durch Business-AI-Anwendungen und agentische KI nutzbar gemacht und automatisiert wird. Ein zentrales Element hierbei ist die Fähigkeit der Rechenzentren, mit der steigenden Nachfrage nach Rechenleistung Schritt zu halten. Ein Netzwerk europäischer Rechenzentren, das sowohl großflächige **KI-Gigafactories** als auch kleinere, lokal betriebene Rechenzentren umfasst, bietet eine doppelte Sicherheit: Sie gewährleisten nicht nur eine stabile und leistungsfähige Infrastruktur, sondern schützen auch vor einer übermäßigen Abhängigkeit von wenigen großen Cloud-Anbietern. Diese Vielfalt an Infrastrukturmodellen ermöglicht es, die Rechenkapazitäten flexibel und bedarfsorientiert zu skalieren, was die Resilienz und Wettbewerbsfähigkeit der europäischen Unternehmen stärkt.

#### **d) Interdependenzen bei der Entwicklung der Rechenzentrumslandschaft in Europa**

Die erfolgreiche Skalierung von Rechenzentren zur Förderung der Entwicklung und Anwendung von KI setzt voraus, dass Rechenzentren, Cloud- und Edge-Infrastrukturen nicht nur leistungsfähig und resilient, sondern auch grenzüberschreitend vernetzt sind. Eine solche Infrastruktur muss so konzipiert werden, dass Unternehmen und Forschungseinrichtungen europaweit jederzeit auf die benötigte Rechenkapazität zugreifen können – unabhängig von ihrer geografischen Lage. Nur durch eine nahtlose und grenzübergreifende Vernetzung wird eine effiziente Nutzung der verfügbaren Ressourcen möglich, die notwendig ist, um mit den dynamischen Anforderungen der KI-Entwicklung Schritt zu halten.

Die grenzüberschreitende Vernetzung von Rechenzentren, deren Bau und Nutzung, ist jedoch nicht nur eine technische Herausforderung, sondern auch eine rechtliche Hürde in Europa. Die rechtlichen Rahmenbedingungen, die die Nutzung von Cloud-Diensten und die Kommunikation zwischen Rechenzentren regeln, sind in Europa sehr komplex und variieren oft je nach Mitgliedstaat. Dies kann

die Effizienz und Flexibilität der grenzüberschreitenden Infrastruktur erheblich einschränken. Ein integriertes europäisches Rechenzentrumsnetzwerk würde es Unternehmen in ganz Europa hingegen ermöglichen, auf eine zuverlässige und skalierbare Infrastruktur zuzugreifen, die den ständig wachsenden Anforderungen der KI-Entwicklung gerecht wird.

Ein zentraler Baustein für die erfolgreiche grenzüberschreitende Nutzung von Rechenzentren und KI-Infrastrukturen ist die Schaffung eines harmonisierten rechtlichen Rahmens innerhalb der EU. Diese Harmonisierung der rechtlichen Rahmenbedingungen würde nicht nur die Effizienz der Infrastruktur steigern, sondern auch das Vertrauen europäischer Unternehmen in diese Infrastruktur und den europäischen Binnenmarkt langfristig stärken.

## 2. Herausforderungen für den Rechenzentrumsstandort Deutschland

### a) Infrastrukturlücken und Energiebedarf als zentrale Herausforderung

Eine der zentralen Herausforderungen für den digitalen Fortschritt in Deutschland liegt in den bestehenden **Infrastrukturlücken**, die die Einführung und Nutzung von KI erheblich hemmen. Der steigende Energiebedarf KI-basierter Rechenzentren bringt die bestehende Energieinfrastruktur zunehmend an ihre Kapazitätsgrenzen. So wird die IT-Lastkapazität deutscher Rechenzentren von derzeit rund 2.980 MW (2025) bis 2030 voraussichtlich auf etwa 5.000 MW steigen.<sup>5</sup> Ohne eine nachhaltige, dauerhaft verfügbare und skalierbare Energieversorgung drohen Engpässe, die den Betrieb rechenintensiver KI-Anwendungen behindern werden.

Parallel erschweren **Konnektivitätsdefizite** und langwierige Genehmigungsverfahren beim Ausbau digitaler Netze den flächendeckenden Zugang zu leistungsfähigen Breitband- und Glasfasernetzen. In ländlichen Regionen verfügen lediglich 37 Prozent der Haushalte über Glasfaseranschlüsse, während in Städten mehr als 85 Prozent der Haushalte versorgt sind<sup>6</sup>. Latenz- und Bandbreitenengpässe können insbesondere Echtzeitanwendungen, Edge-Computing und KI-gestützte Analysen stark einschränken.

Gleichzeitig zeigt sich eine deutliche **Konzentration der IT-Last auf einzelne Hotspots**: So liegt im Raum Frankfurt am Main eine erhebliche IT-Load — mit rund 745 MW live Capacity, 542 MW im Bau und 383 MW in Planung.<sup>7</sup> Diese Konzentration verdeutlicht einerseits die Attraktivität zentraler Standorte — etwa wegen guter Netz- und Stromanbindung und Infrastruktur — andererseits aber auch potenzielle Risiken hinsichtlich regionaler Diversität und Abhängigkeit von wenigen Ballungsräumen.

---

<sup>5</sup> Mordor Intelligence, Germany Data Center Market Size & Share Analysis - Growth Trends And Forecast (2025 - 2030), <https://www.mordorintelligence.com/industry-reports/germany-data-center-market>.

<sup>6</sup> Bundesnetzagentur, Bundesnetzagentur publishes new data on broad band cover age in the Broadband Atlas, 2024, [https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2024/20240619\\_BBA.html](https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2024/20240619_BBA.html).

<sup>7</sup> JLL, Insight - German Data Center Market, <https://www.jll.com/en-de/insights/german-data-center-market-addressing-rising-demand>.

Der **steigende Energiebedarf** im Zusammenhang mit der Expansion von Rechenzentren stellt eine wachsende Herausforderung dar, die dringend eine frühzeitige Klarheit in mehreren Bereichen erfordert. Insbesondere müssen Netzanschlüsse, die langfristige Versorgungssicherheit, stabile Strompreise und klare Genehmigungsprozesse gewährleistet werden, um Investitionen in die Rechenzentrumsinfrastruktur nicht unnötig auszubremsen.

Ein zentrales Problem besteht darin, dass Unsicherheiten bei der Verfügbarkeit von Energie sowie unklare oder langwierige Genehmigungsverfahren potenzielle Investoren abschrecken und die schnelle Skalierung von Rechenzentren behindern können.

Hierfür ist ein entschlossener **Bürokratieabbau** erforderlich, insbesondere bei Genehmigungsprozessen und den regulatorischen Vorgaben für den Betrieb von Rechenzentren. Vereinfachte, transparente und standardisierte Verfahren würden nicht nur die Investitionsbereitschaft erhöhen, sondern auch die Realisierung neuer Rechenzentren deutlich beschleunigen. Zugleich könnten sie dazu beitragen, eine ausreichende und stabile Energieversorgung sicherzustellen, die für den zuverlässigen Betrieb unerlässlich ist. Planbare und wettbewerbsfähige Strompreise würden darüber hinaus die Betriebskosten langfristig senken. Ein klarer, effizienter und zukunftsfähiger regulatorischer Rahmen wird damit zu einem entscheidenden Faktor für Wettbewerbsfähigkeit und Skalierbarkeit der europäischen Rechenzentrumslandschaft.

#### **b) Nutzerstruktur & KMU-Lücke**

Neben infrastrukturellen Engpässen ist auch die gegenwärtige Nutzerstruktur von Rechenzentrums- und Cloud-Diensten zu berücksichtigen. Während große Unternehmen und Konzerne Cloud- und Co-Location-Angebote bereits intensiv nutzen, zeigen sich bei kleinen und mittleren Unternehmen weiterhin deutliche Zurückhaltung und strukturelle Defizite. Häufig fehlen grundlegende technische Voraussetzungen wie Virtualisierung, Containerisierung oder moderne IT-Architekturen. Hinzu kommen begrenzte personelle und finanzielle Ressourcen sowie Unsicherheiten hinsichtlich regulatorischer Anforderungen.

Da **KMU das Rückgrat der deutschen Wirtschaft** bilden, stellt diese Nutzungslücke ein strategisches Risiko für die Wettbewerbsfähigkeit dar. Gefragt sind daher niedrigschwellige Transformationsprogramme für KMU, standardisierte Migrationsleitfäden, modulare Cloud-Bausteine mit klarer Compliance-Zertifizierung sowie gezielte Förderprogramme zur Modernisierung bestehender Unternehmensrechenzentren.

Nur wenn die Breite der Wirtschaft – insbesondere der industrielle Mittelstand – in die Nutzung moderner Rechen- und KI-Infrastrukturen eingebunden wird, kann die digitale Transformation volkswirtschaftlich wirksam werden.

### c) Cybersicherheit als systemkritische Herausforderung

Mit dem schnellen Ausbau von Rechen-, Cloud- und KI-Infrastrukturen steigt die Verwundbarkeit digitaler Systeme erheblich. Rechenzentren, Cloud-Plattformen und KI-Modelle sind zunehmend Ziel komplexer Angriffe, die weit über klassische IT-Bedrohungen hinausgehen.

Laut Bundesamt für Sicherheit in der Informationstechnik (BSI) befindet sich die IT-Bedrohungslage in Deutschland weiterhin auf einem anhaltend hohen Niveau, insbesondere aufgrund professioneller Cyberkriminalität, Ransomware-Angriffen und zunehmend automatisierter Angriffswerkzeuge (siehe den BSI-Lagebericht 2023/2024)<sup>8</sup>.

Hinzu kommen KI-spezifische Angriffsvektoren:

- **Datenvergiftung (Data Poisoning):** gezielte Verfälschung von Trainingsdaten, um Modelle zu manipulieren
- **Model Extraction & Model Inversion:** Angriffe, die Rückschlüsse auf Trainingsdaten oder interne Modellparameter erlauben
- **Adversariale Manipulationen:** minimale Eingriffe in Input-Daten führen zu Fehleinschätzungen der Modelle
- **Supply-Chain-Angriffe auf Software- und Hardwareabhängigkeiten** (z. B. Firmware, Library Dependencies), die laut der EU-Cybersicherheitsagentur ENISA 2024 weiter an Bedeutung gewinnen

Für Rechenzentren und Cloud-Infrastrukturen entstehen dadurch Sicherheitsanforderungen, die klassische Schutzkonzepte – Firewalls, Netzwerksegmentierung oder reine Compliance-Maßnahmen – nicht mehr ausreichend abdecken. Stattdessen werden notwendig:

- Zero-Trust-Architekturen,
- KI-basierte Anomalie- und Angriffserkennung,
- transparente Modell-Governance,
- Härtung der Lieferketten,
- sowie zertifizierte Sicherheitsstandards (u. a. ISO 27001, C5, EUCS).

Cybersicherheit wird damit nicht nur zu einer technischen, sondern zu einer strategischen Schlüsselkompetenz für den Standort Deutschland.

### d) Fachkräftemangel als strukturelle Wachstumsbremse

Parallel wirkt der anhaltende Fachkräftemangel als erhebliche Hürde für den Ausbau und den sicheren Betrieb deutscher Rechen- und KI-Infrastrukturen, besonders in den folgenden Bereichen:

---

<sup>8</sup> Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2024, [https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/Archiv-Lageberichte/2024/lagebericht\\_2024\\_node.html](https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/Archiv-Lageberichte/2024/lagebericht_2024_node.html).

- Cloud-Architektur und DevOps,
- Cybersicherheit,
- Data Engineering,
- KI-Entwicklung und MLOps,
- Rechenzentrumsbetrieb und Energie-/Gebäudetechnik.

Diese Lücke führt zu spürbaren Auswirkungen:

- **Verzögerte Realisierung neuer Rechenzentren**, da Planungs-, Bau- und Betriebsprozesse hochspezialisiertes Personal erfordern (RZ-Planung, Kühl- und Energieexpertise, Netzwerktechnik).
- **Engpässe beim Betrieb sicherheitskritischer Systeme**, da Cybersecurity-Teams unterbesetzt sind und Angriffe oft nicht schnell genug erkannt oder abgewehrt werden können.
- **Erschwerte Skalierung von KI-Anwendungen**, da insbesondere Data-Engineering- und MLOps-Kompetenzen fehlen, die für stabile Datenpipelines und den produktiven KI-Einsatz zentral sind.
- **Wachsende Kosten für Unternehmen**, da die Nachfrage nach spezialisierten Fachkräften weit über dem Angebot liegt und damit Löhne und Beratungsaufwände steigen.

Der Fachkräftemangel verstärkt somit die ohnehin hohen Sicherheitsrisiken und beeinträchtigt direkt die Wettbewerbsfähigkeit des Standorts Deutschland – insbesondere im internationalen Vergleich, wo Länder wie die USA, Kanada oder Singapur aggressive Strategien zur Talentgewinnung verfolgen.

#### **e) Regulatorische Komplexität als Innovationsbremse**

Ein zentrales Hemmnis für den schnellen Ausbau und die internationale Wettbewerbsfähigkeit des Rechenzentrums- und Cloud-Standorts Deutschland ist die hohe regulatorische Komplexität. Unternehmen, Betreiber und öffentliche Einrichtungen sehen sich mit einem vielschichtigen Geflecht aus nationalen Regelungen, EU-Vorschriften, sektoralen Normen und regionalen Zuständigkeiten konfrontiert, die häufig nicht aufeinander abgestimmt sind. Dies führt zu erheblichen Verzögerungen bei Planung, Betrieb und Skalierung digitaler Infrastruktur.

#### Divergierende Vorschriften und nationale Sonderwege

In Deutschland gelten für Rechenzentren und Cloud-Infrastrukturen zahlreiche Regelwerke aus den Bereichen:

- Datenschutz (DSGVO + nationale Ergänzungen)
- IT-Sicherheit (BSIG, KRITIS-Verordnung, BSI-C5)
- Energieeffizienz und Gebäudestandards (EnEV, GEG, Energieeffizienzgesetz)
- Genehmigungs- und Bauvorschriften (Landesbauordnungen, Emissionsschutz, Standortauflagen)
- Telekommunikationsrecht (TKG, Vorratsdatenspeicherung – obwohl ausgesetzt)

Viele dieser Regelungen gehen über europäische Vorgaben hinaus oder unterscheiden sich zwischen Bundesländern. So benötigen Rechenzentren in manchen Ländern mehrstufige Umwelt- oder Energieeffizienznachweise, während in anderen Regionen ähnliche Anlagen deutlich schneller genehmigt werden. Die Folge ist ein ungleicher Regulierungsraum, der Investitionen regional verzerrt oder sogar verhindert. Um Investitionen zu vereinfachen und Bauvorhaben zu beschleunigen, muss daher einer Harmonisierung des deutschen Rechts mit den europäischen Vorgaben und eine Vereinheitlichung des Baurechts auf nationaler Ebene erfolgen.

#### Hemmnisse für grenzüberschreitenden Datenaustausch und Cloud-Nutzung

Mit dem europäischen Cloud-Regulierungsrahmen (GAIA-X, EUDIS, EUCS) soll eigentlich ein einheitlicher digitaler Binnenmarkt entstehen. In der Praxis wird die Nutzung jedoch erschwert durch:

- inkonsistente Zertifizierungen (z. B. nationale Anforderungen über EU-Standards hinaus)
- Unsicherheiten über Datenlokalisierung und Datenhoheit
- unterschiedliche Sicherheitsanforderungen für kritische Infrastrukturen
- restriktive Interpretationen der DSGVO durch deutsche Aufsichtsbehörden.

Dies führt dazu, dass international konkurrenzfähige Cloud-Dienste in Deutschland oft langsamer ausgerollt oder nur eingeschränkt genutzt werden können.

#### Verzögerte Einführung neuer Technologien

Regulatorische Komplexität wirkt sich besonders negativ auf Zukunftstechnologien aus:

- **Beim Ausbau von KI-Infrastrukturen:** KI-Anwendungen unterliegen gleichzeitig Datenschutz-, IT-Sicherheits-, Wettbewerbs-, Urheber- und zunehmend KI-spezifischen Regelungen (KI-VO). Fehlende Klarheit darüber, wie diese Normen zusammenspielen, führt zu regulatorischer Unsicherheit und einem Compliance-Albtraum – einem der zentralen Innovationsrisiken für Unternehmen.
- **Bei Rechenzentren und Cloud-Betrieb:** Komplexe Bau- und Umweltauflagen verlängern Genehmigungsverfahren häufig auf 18–36 Monate, während vergleichbare Standorte in den Niederlanden, UK oder den nordischen Ländern zum Teil unter 12 Monaten bleiben.
- **Bei Edge-Infrastrukturen:** Hier fehlen vielfach klare Richtlinien zu Platzierung, baurechtlicher Einordnung oder Sicherheitsanforderungen. Das erschwert den Einsatz edge-basierter Anwendungen in Industrie, Verkehr oder Gesundheitswesen.
- **Steigende administrative Kosten und Investitionshemmnisse:** Die Vielzahl von Auflagen führt zu hohen Compliance-Kosten, insbesondere für mittelständische Unternehmen und Betreiber kleiner Rechenzentren.

Wenn Deutschland Planung, Bau und Betrieb digitaler Infrastruktur durch regulatorische Komplexität verlangsamt, führt das zu drei Risiken:

- Abwanderung von Investitionen in Rechenzentren, KI-Fabriken und Cloud-Services
- Wachstumsverlangsamung von KI-Startups und deutschen Cloud-Anbietern
- Technologische Abhängigkeit von außereuropäischen Anbietern, wenn europäische Alternativen zu spät skalieren

### 3. Chancen für den Rechenzentrumsstandort Deutschland

Trotz bestehender Herausforderungen eröffnen sich für Deutschland erhebliche Chancen, seine Position als führender Standort für Rechenzentren, Cloud-Dienste und KI-Infrastrukturen auszubauen. Diese Chancen ergeben sich aus technologischen Entwicklungen, politischen Weichenstellungen, Markttrends und der wachsenden globalen Nachfrage nach digitaler Souveränität, KI-Fähigkeiten und resilienten Dateninfrastrukturen.

Deutschland besitzt aktuell erhebliche Potenziale, seine Rolle als führender Standort für Rechenzentren, Cloud- und KI-Infrastruktur deutlich auszubauen.

Ein zentraler Ansatz liegt im **Aufbau leistungsfähiger KI-Infrastrukturen**. Der steigende Bedarf an Rechenleistung — befeuert durch neue Anforderungen durch agentische KI, KI-Workloads, Cloud-Dienste und Industrie 4.0 — eröffnet die Möglichkeit, sogenannte „AI-Factories“ oder modulare GPU-/HPC-Cluster zu errichten. Dadurch kann Deutschland seine technologische Souveränität stärken und einen europäischen Tech-Standort mit hoher Wettbewerbsfähigkeit etablieren. Neben globalen Cloud-Anbietern könnten so daten- und KI-intensive Anwendungen lokal, rechtssicher und datenschutzkonform betrieben werden — ein Vorteil insbesondere für Unternehmen und Organisationen, die auf Regulierung, Compliance und Datenschutz achten müssen.

Zeitgleich eröffnet der wachsende Energiebedarf durch Ausbau der Rechenzentren eine strategische Chance für eine **Modernisierung und Nachhaltigkeitswende der Energieinfrastruktur**. Studien zeigen, dass deutsche Rechenzentren ihre Energieeffizienz in den letzten Jahren deutlich verbessert haben — der durchschnittliche Power-Usage-Effectiveness-Wert (PUE) liegt mittlerweile bei etwa 1,46.<sup>9</sup>

Gleichzeitig ergeben sich durch Konzepte wie **Abwärmenutzung, Integration in Fernwärmesysteme oder Nutzung erneuerbarer Energien** Möglichkeiten, Rechenzentren als Teil eines nachhaltigen Energiesystems zu etablieren. So kann Deutschland bei „Green Compute“ und klimafreundlicher Cloud-Infrastruktur eine Vorreiterrolle einnehmen.

---

<sup>9</sup> Bundesministerium für Wirtschaft und Klimaschutz, Stand und Entwicklung des Rechenzentrumsstandorts Deutschland, 17.01.2025, [https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Publikationen/Technologie/stand-und-entwicklung-des-rechenzentrumsstandorts-deutschland.pdf?\\_\\_blob=publicationFile&\\_\\_amp%3Bv=10&utm](https://www.bundeswirtschaftsministerium.de/Redaktion/DE/Publikationen/Technologie/stand-und-entwicklung-des-rechenzentrumsstandorts-deutschland.pdf?__blob=publicationFile&__amp%3Bv=10&utm).

Gleichzeitig steigt der **Bedarf an Cybersicherheit und Sicherheitstechnologien** — mit ihm eröffnen sich neue Marktchancen. Der Ausbau von Cloud-, Edge- und KI-Infrastruktur verlangt robuste Sicherheitsarchitekturen, Zero-Trust-Konzepte und kontinuierliche Überwachung, um Datenintegrität, Verfügbarkeit und Resilienz gegen Cyberangriffe zu gewährleisten. Anbieter, die entsprechende Sicherheits- und Compliance-Lösungen entwickeln, können Deutschland als sicheren, vertrauenswürdigen Standort für kritische Infrastruktur positionieren.

Ein weiterer, entscheidender Vorteil entsteht aus der Möglichkeit, europäische und nationale **Standards sowie Regularien für Cloud, Datenschutz und IT-Sicherheit** voranzubringen. Wenn Deutschland gemeinsam mit europäischen Partnern Harmonisierung und klare Regelwerke umsetzt, kann das Land zur Drehscheibe für souveräne, rechtskonforme und interoperable Cloud- und Datenservices in Europa werden.

Darüber hinaus bietet der Ausbau einer modernen Rechenzentren- und Cloud-Infrastruktur die Chance, **neue Geschäftsfelder und Innovationen in Bereichen wie Industrie 4.0, Edge-Computing, Smart Cities oder digitale Verwaltung** zu fördern. Unternehmen, Forschungseinrichtungen und öffentliche Institutionen erhalten Zugriff auf skalierbare, leistungsfähige und datenschutzkonforme Infrastruktur. Dadurch können datengetriebene Geschäftsmodelle, neue Services und Effizienzgewinne möglich werden.

Schließlich eröffnet sich durch attraktive Rahmenbedingungen und gezielte Investitionen die Möglichkeit, internationale Investoren anzuziehen. Deutschlands zentrale geographische Lage in Europa, stabile Rechts- und Wirtschaftsstrukturen sowie wachsende Nachfrage nach nachhaltiger und souveräner Digitalinfrastruktur machen den Standort für globale Cloud- und Hyperscale-Betreiber interessant. Das kann nicht nur zu Kapitalzufluss führen, sondern auch zur Schaffung hochqualifizierter Arbeitsplätze und langfristiger Wertschöpfung im Land.

### **Zentrale Chancen für den Rechenzentrumsstandort Deutschland**

- **Investitionen in KI-Infrastrukturen und „AI Factories“:** Der Aufbau leistungsfähiger GPU- und HPC-Cluster („AI Factories“) stärkt Deutschlands Innovationskraft, reduziert Abhängigkeiten von ausländischen Clouds und ermöglicht die Entwicklung eigener KI-Ökosysteme.
- **Modernisierung der Energie- und Wärmeinfrastruktur:** Der steigende Energiebedarf von Rechenzentren kann als Treiber für Energieeffizienz, Abwärmenutzung, Integration erneuerbarer Energien und den Ausbau smarter Netze dienen — ein wesentlicher Hebel für nachhaltige Wertschöpfung.
- **KI-gestützte Cybersecurity und neue Sicherheitsarchitekturen:** Fortschritte in KI-basierten Security-Systemen ermöglichen frühzeitige Angriffserkennung, Zero-Trust-Konzepte und höhere Resilienz. Gleichzeitig entstehen neue Kompetenzfelder und Qualifikationsprofile im Bereich Sicherheitstechnologien.

- **Europäische Harmonisierung und digitale Souveränität:** Einheitliche Daten-, Cloud- und Interoperabilitätsstandards (z. B. GAIA-X-basierte Ansätze) erleichtern grenzüberschreitende Kooperation, stärken europäische Cloud-Ökosysteme und erhöhen die internationale Wettbewerbsfähigkeit.
- **Digitalisierung der öffentlichen Verwaltung und kritischer Infrastrukturen:** Moderne Cloud- und Rechenzentrumsarchitekturen ermöglichen effizientere Verwaltungsprozesse, sichere Datenverarbeitung und stabilere KRITIS-Strukturen — was wiederum Innovation, Standortattraktivität und Vertrauen stärkt.
- **Anziehung internationaler Investitionen und Fachkräfte:** Eine leistungsfähige, nachhaltige und regulativ verlässliche Rechenzentrumslandschaft macht Deutschland zu einem attraktiven Standort für globale Hyperscaler, Co-Location-Anbieter und digitale Wachstumsbranchen, was Arbeitsplätze und Know-how stärkt.

#### 4. Merkmale und Rahmenbedingungen eines zukunftsfähigen und leistungsstarken Rechenzentrumsstandort Deutschland

Ein leistungsstarker Rechenzentrumsstandort Deutschland muss in der Lage sein, die wachsenden Anforderungen daten- und KI-intensiver Anwendungen abzubilden. Dazu gehören Hochleistungsrechner für KI-Training, verteilte Edge-Infrastrukturen für Echtzeitanwendungen sowie skalierbare Cloud-Umgebungen<sup>10</sup>.

Ein zukunftsfähiger und leistungsstarker Rechenzentrumsstandort Deutschland basiert auf einem **ausgewogenen Mix aus großskaligen Hyperscale-Rechenzentren, Unternehmensrechenzentren, regionalen Co-Location-Angeboten und Edge-Infrastrukturen**. Diese Vielfalt ist essenziell, um eine robuste, KI-native Infrastruktur bereitzustellen, die hochperformante, skalierbare und sichere Lösungen für anspruchsvolle KI-Workloads ermöglicht. Moderne Rechenzentren, Hochgeschwindigkeitskonnektivität und leistungsfähige Netzwerke verhindern Engpässe und stellen sicher, dass datenintensive Anwendungen — von großem KI-Training bis zu latenzkritischen Echtzeitdiensten — zuverlässig betrieben werden können. Die IT-Anschlussleistung deutscher Rechenzentren hat 2025 bereits knapp 3 GW erreichen können, getrieben vor allem durch KI- und cloudbasierte Anwendungen.<sup>11</sup> Eine nationale Rechenzentrumsstrategie muss deshalb Rahmenbedingungen schaffen, die diese Vielfalt langfristig erhalten und nicht die einseitige Konsolidierung auf wenige Hyperscaler begünstigen.

Ein weiterer zentraler Baustein ist eine **effiziente, zuverlässige und wettbewerbsfähige Energieversorgung**. Rechenzentren sind energierelevante Infrastrukturen, und der durch KI, HPC und Cloud steigende Bedarf erfordert eine Diversifizierung der Energiequellen sowie digitale Lösungen für ein intelligentes Energiemanagement.

<sup>10</sup> Wirtschaft digital Baden-Württemberg, KI treibt Ausbau der Rechenzentren in Deutschland voran, 02.12.2025, <https://www.wirtschaft-digital-bw.de/aktuelles/news/detailseite/ki-treibt-ausbau-der-rechenzentren-in-deutschland-voran>.

<sup>11</sup> Borderstep Institut, Rechenzentren in Deutschland: Aktuelle Marktentwicklungen (Update 2025), <https://www.borderstep.de/2025/11/12/rechenzentren-in-deutschland-aktuelle-marktentwicklungen-update-2025>.

Energieeffiziente IT-Hardware, moderne Kühltechnologien und Abwärmenutzung gelten laut Fraunhofer ISE als entscheidende Hebel für eine nachhaltige Transformation des Sektors. Damit lässt sich nicht nur der ökologische Fußabdruck reduzieren, sondern zugleich die Versorgungssicherheit stärken. Ein koordiniertes Vorgehen ermöglicht es, Rechenzentren nicht als isolierte Energieverbraucher, sondern als aktive Bestandteile eines intelligenten Energiesystems zu verstehen – etwa durch netzdienliche Flexibilitätsoptionen oder die Einbindung in kommunale Wärmeplanung. Die erfolgreiche Integration von Rechenzentren in zukünftige Energiesysteme erfordert einen **integrativen, modularen und sektorübergreifenden Ansatz**. Eine enge Kooperation zwischen Rechenzentrumsbetreibern, Energieversorgern, Netzbetreibern, kommunalen Versorgern, Stadtverwaltungen sowie innovativen Startups im Energie- und Rechenzentrumsbereich ist essenziell. Bereits heute zeigen einzelne Modellprojekte, dass durch gemeinsame Planung von Netzanschlüssen, Wärmenutzungskonzepten und Lastmanagementsystemen sowohl Effizienzgewinne als auch Akzeptanzsteigerungen erzielt werden können.

Zukunftsfähigkeit bedeutet jedoch auch, **Cybersicherheit und Resilienz ganzheitlich zu denken**. Die wachsende Komplexität globaler Lieferketten, KI-spezifische Angriffsvektoren und die zunehmende Abhängigkeit kritischer Sektoren von digitalen Diensten verschärfen die Sicherheitsanforderungen. KI-gestützte Security-Lösungen können Bedrohungen in Echtzeit erkennen, antizipieren und abwehren und werden daher laut BSI zu einem strategischen Baustein moderner Sicherheitsarchitekturen (siehe BSI-Lagebericht 2024). Ergänzend müssen international anerkannte Standards wie ISO 27001, ENISA-Frameworks oder NIS2-konforme Prozesse entlang der gesamten Wertschöpfungskette implementiert werden, um Ausfälle, Manipulationen und Datenverluste wirksam zu verhindern. Ein leistungsfähiger Rechenzentrumsstandort bildet damit das technologische Rückgrat für digitale Souveränität und Innovation.

Die EU-Kommission betont im Digital Economy and Society Index (DESI), dass Deutschland in der Cloud-Nutzung und digitalen Infrastruktur im europäischen Vergleich bisher nur mittelmäßig abschneidet und insbesondere von harmonisierten europäischen Regeln profitieren könnte. Vor diesem Hintergrund ist es zentral, **regulatorische Fragmentierung abzubauen**. Nationale Sonderwege – wie aktuell beim E-Invoicing – erschweren grenzüberschreitende Datennutzung, erhöhen den Administrationsaufwand und bremsen Innovationen. Ein tatsächlich barrierefreier europäischer Datenraum erfordert daher die Harmonisierung sowie gezielte Entschlackung bestehender EU-Digitalregulierungen, insbesondere im Produktsicherheits- und Datenschutzbereich, wo Doppelregulierungen und Inkohärenzen zu erheblichen Belastungen führen. Nur ein einheitlicher, kohärenter Rechtsrahmen ermöglicht die effiziente Nutzung hochwertiger Datenströme, Trainingsdaten und KI-Lösungen – und stärkt die internationale Wettbewerbsfähigkeit.

Qualifizierte Fachkräfte sind ein zentraler Erfolgsfaktor für den Rechenzentrums- und KI-Standort Deutschland. Der Fachkräftemangel ist mit rund 109.000 offenen Stellen in der deutschen IT-Branche gravierend und betrifft insbesondere Schlüsselbereiche wie Künstliche Intelligenz, Cloud Engineering, Energie- und Gebäudetechnik sowie Cybersicherheit. Gleichzeitig ist ein leichter Rückgang des

Bedarfs zu beobachten, da durch Automatisierung im KI-Bereich bestimmte Tätigkeiten effizienter gestaltet und teilweise eingespart werden können.<sup>12</sup>

Breite Qualifizierungsinitiativen — wie die Allianz für Digitale Kompetenzen des Bayerischen Digitalministeriums — leisten einen wichtigen Beitrag zur digitalen Breitenbildung, greifen aber zu kurz, wenn es um die gezielte Förderung von High Potentials für hochspezialisierte Technologierollen geht. Ein sinnvoller Ansatz besteht daher in einer dualen Strategie: einerseits die **Breitenqualifizierung der Arbeitskräfte und andererseits die gezielte Förderung hochqualifizierter Spezialistinnen und Spezialisten**. Dieser Ansatz sollte idealerweise in enger Partnerschaft mit der Wirtschaft und den Unternehmen entwickelt werden. Besonders wichtig ist dabei ein verstärkter und systematischer Austausch zwischen Universitäten und Unternehmen, der in unterschiedlichen Bildungs- und Weiterbildungsphasen fest verankert ist. Hierbei können Praxis-Seminare und Projektmodule in der Digitalwirtschaft als feste Bestandteile des Studiums dazu beitragen, den Studierenden praxisnahe Erfahrungen zu vermitteln und die Kluft zwischen akademischer Ausbildung und den Anforderungen der Wirtschaft zu überbrücken. Solche praxisorientierten Elemente stärken nicht nur die Fachkompetenz der Absolventen, sondern fördern auch die Innovationskraft und Wettbewerbsfähigkeit der Unternehmen.

Eine **digitalisierte öffentliche Verwaltung** schließlich kann zum Schlüsselfaktor für ein innovationsfreundliches, KI-affines Ökosystem werden. Die öffentliche Hand sollte als **Erstkunde** (Lead Customer) bei Rechenzentrumsprojekten ausdrücklich in den Vordergrund gestellt werden. Eine frühzeitige und verlässliche Nachfragestellung durch öffentliche Einrichtungen bietet eine bedeutende Planungssicherheit und schafft so die notwendigen Voraussetzungen für die Finanzierung und Realisierung von Projekten. Insbesondere für Investoren stellt die Gewissheit einer stabilen und langfristigen Abnahme durch staatliche Stellen einen entscheidenden Hebel dar, um Projekte auch in frühen Entwicklungsphasen wirtschaftlich tragfähig zu machen. Die öffentliche Hand sollte als Vorbild und verlässlicher Partner auftreten, um die Digitalisierung und den Ausbau von Rechenzentren in Deutschland und Europa voranzutreiben und private Investitionen zu fördern. Durch konsequente Cloud-Migration, Modernisierung der IT-Infrastruktur, Nutzung von Künstlicher Intelligenz und Integration sicherheitspolitischer Anforderungen von Beginn an dient die Verwaltung als Hebel für Effizienz, Cyberresilienz und eine flächendeckende digitale Transformation. Dies stärkt nicht nur die Wettbewerbsfähigkeit, sondern auch das Vertrauen in digitale staatliche Dienstleistungen — ein wesentlicher Erfolgsfaktor für den gesamten Standort.

**Anreizsysteme für Kommunen zur Ansiedlung von dezentralen Edge-Rechenzentren:** Um Kommunen zu ermutigen, Edge-Rechenzentren anzusiedeln, sollte ein Anreizsystem eingeführt werden, das die Gewerbesteuer analog zu Windkraftanlagen umlegt. Da Edge-Rechenzentren in der Regel nur wenige Arbeitsplätze vor Ort schaffen, fehlt oft der unmittelbare wirtschaftliche Anreiz für Kommunen, solche Projekte zu unterstützen.

---

<sup>12</sup> Institut der Deutschen Wirtschaft, Deutlicher Stellenrückgang in IT-Berufen – besonders für hochqualifizierte Experten, 16.08.2025, <https://www.iwkoeln.de/studien/jurek-tiedemann-deutlicher-stellenrueckgang-in-it-berufen-besonders-fuer-hochqualifizierte-experten.html>.

Eine Steuerzerlegung, bei der ein Teil der Gewerbesteuer direkt an die jeweilige Gemeinde fließt, würde den Kommunen einen klaren finanziellen Vorteil verschaffen und gleichzeitig die lokale Akzeptanz und Unterstützung für den Bau von Edge-Rechenzentren stärken. Diese Maßnahme würde nicht nur die Attraktivität solcher Projekte erhöhen, sondern auch einen entscheidenden Beitrag zur Schaffung von Infrastruktur für die digitale Transformation leisten.

Rechenzentren entfalten ihren volkswirtschaftlichen und technologischen Wert erst dann vollständig, wenn auf ihnen Anwendungen betrieben werden, die für Wirtschaft, Verwaltung und Gesellschaft einen konkreten Nutzen stiften. **Software-as-a-Service (SaaS)** spielt hierbei eine zentrale Rolle. Insbesondere Mittelstand und öffentliche Verwaltung greifen zunehmend auf spezialisierte SaaS-Angebote zurück, statt eigene Compute-Cluster zu betreiben. Typische Anwendungsfelder reichen von KI-gestützter Kommunikation, Prozessautomatisierung und Datenanalyse bis hin zu branchenspezifischen Geschäftsanwendungen. Immer mehr Anbieter integrieren Künstliche Intelligenz direkt in ihre Anwendungen, um Prozesse effizienter, datenbasierter und skalierbar zu gestalten. Für staatliche Stellen, Kommunen und Behörden bietet dies erhebliche Chancen: Statt für vergleichbare Anforderungen mehrfach eigene Lösungen zu entwickeln, können sie auf bereits verfügbare, geprüfte SaaS-Dienste zurückgreifen. Gleichzeitig werden die volkswirtschaftlichen Potenziale moderner Rechenzentren erst dann vollständig realisiert, wenn Anwendungen auf ihnen betrieben werden, die unmittelbar Nutzen stiften. Damit Deutschland seine Rechenzentren als strategische Infrastruktur versteht, muss auch die Anwendungsebene adressiert werden. Ohne klar geregelten Zugang zu souveränen SaaS-Lösungen bleibt selbst die modernste Rechenzentrumslandschaft ein unvollständiger Baustein der digitalen Souveränität.

Voraussetzung dafür ist eine **einheitliche Definition digitaler Souveränität im Cloud- und SaaS-Kontext**. Derzeit werden Anforderungen an Datenhaltung, Infrastruktur und Anbieter je nach Behörde oder Projekt unterschiedlich interpretiert – häufig ohne einheitliche Bewertung der Kritikalität der jeweiligen Anwendung. Gerade im öffentlichen Sektor zeigt sich, dass ein zentrales Hindernis für Innovation nicht der Mangel an Technologien ist, sondern das Fehlen klarer Kriterien, nach denen beurteilt wird, welche Cloud- und SaaS-Lösungen als souverän gelten. Unterschiedliche Interpretationen zwischen Behörden und Ressorts führen zu Unsicherheiten, zusätzlichem Verwaltungsaufwand und erheblichen Kosten – insbesondere für den Mittelstand, der sowohl als Nutzer als auch als Anbieter digitaler Lösungen überproportional betroffen ist. Diese Widersprüche reduzieren Geschwindigkeit, erhöhen Komplexität und führen zu Wettbewerbsnachteilen auf nationaler wie internationaler Ebene. Notwendig ist daher ein transparenter, risikobasierter und anwendungsbezogener Rahmen, der klar beschreibt, welche Infrastrukturen in welchen Nutzungskontexten als souverän gelten – von europäischen Cloud-Angeboten bis hin zu national betriebenen Lösungen. Eine solche Einordnung schafft Planungs- und Investitionssicherheit, statt neue Hürden aufzubauen. Öffentliche Auftraggeber könnten bestehende konforme SaaS-Lösungen effizient beschaffen, während Anbieter gezielt in wirtschaftlich tragfähige Dienste investieren können. Die zentrale Erkenntnis lautet: Die Frage, wie souveräne Rechenzentren betrieben werden, ist untrennbar verbunden mit der Frage, welche souveränen Dienste darauf genutzt werden dürfen.

Gleichzeitig muss die **Wettbewerbssituation** realistisch analysiert werden. Der globale Markt für Cloud- und Hyperscale-Infrastrukturen wird derzeit von wenigen großen Anbietern dominiert. Diese Marktstellung beruht auf erheblichen Skaleneffekten, vertikaler Integration von Hard- und Software, massiven Investitionsvolumina, globalen Datenökosystemen sowie einer frühzeitigen Internationalisierung. Europäische Anbieter stehen vor der Herausforderung, mit diesen Skalenvorteilen zu konkurrieren und gleichzeitig höhere regulatorische Anforderungen zu erfüllen.

Für Deutschland und Europa stellt sich daher die strategische Frage, wie technologische Souveränität gestärkt werden kann, ohne aber die Innovationsdynamik zu bremsen. Mögliche Ansatzpunkte sind die Förderung interoperabler Cloud-Ökosysteme, offene Standards, Multi-Cloud-Strategien, gezielte Skalierungsfinanzierung für europäische Anbieter sowie eine innovationsfreundliche Ausgestaltung regulatorischer Rahmenbedingungen.

## 5. Maßnahmen und Best Practices

- **Förderung von Investitionen in robuste, skalierbare digitale Infrastrukturen:** Rechenzentren müssen in der Lage sein, KI-Workloads zu unterstützen, die Hochdurchsatz- und Niedriglatenz-Netzwerke erfordern. Investitionen in leistungsfähige und skalierbare Netzinfrastrukturen sind daher ebenso entscheidend – insbesondere mit Blick auf die Weiterentwicklung des Edge Computing, das für latenzkritische KI-Anwendungen zunehmend an Bedeutung gewinnt. Zwar bleiben Rechenzentren zentral für Training und Inferenz von KI-Modellen, doch der Trend geht hin zu einer stärker verteilten Datenverarbeitung. Entsprechend sollte eine zukunftsorientierte Strategie sowohl den Bedarf an leistungsfähigen, zentralisierten Rechenzentren als auch an dezentralen Edge-Computing-Strukturen berücksichtigen.
- **Netzentgeltreduzierung:** Rechenzentren haben einen hohen und kontinuierlichen Strombedarf, der mit dem klassischer energieintensiver Industrien vergleichbar ist. Energie ist damit ein zentraler Kostenfaktor und beeinflusst maßgeblich die Wirtschaftlichkeit sowie die Standortentscheidung der Betreiber. Zugleich übernehmen Rechenzentren eine systemrelevante Funktion für Wirtschaft, Verwaltung und kritische Infrastrukturen in Deutschland. Trotz umfangreicher Effizienzsteigerungen steigt der absolute Energiebedarf infolge wachsender digitaler Anwendungen und KI weiter an und ist nur begrenzt flexibel steuerbar. Vor diesem Hintergrund sollte die Netzentgeltreduzierung nicht abgeschafft, sondern vielmehr ausgeweitet werden – insbesondere unter Einbeziehung von Co-Location-Betreibern.
- Anforderungen an **Unternehmensrechenzentren** berücksichtigen: Nicht nur Hyperscale-Rechenzentren sind entscheidend für Innovation und die breite Einführung von KI. Auch Unternehmen müssen ihre bestehenden Rechenzentren modernisieren, um den steigenden Anforderungen an Datenverarbeitung und Rechenleistung gerecht zu werden. Entsprechende Investitionen in technische Erneuerungen sollten daher gezielt gefördert und regulatorisch erleichtert werden. Zudem unterliegen Rechenzentren in gemischt genutzten Einrichtungen (z. B. Gewerbeparks) häufig Beschränkungen hinsichtlich der verfügbaren Stromkapazitäten, was die Ausbau- und Leistungsfähigkeit der Rechenkapazität zusätzlich begrenzt.

- **Co-Location-Rechenzentren** stärken: Co-Location-Rechenzentren sind insbesondere für die Digitalisierung mittelständischer Unternehmen von zentraler Bedeutung. Dennoch wird diese Form des Rechenzentrumsbetriebs vom Gesetzgeber – insbesondere im Rahmen des Erneuerbare-Energien-Gesetzes (EEG) – bislang nicht ausreichend berücksichtigt. Dies zeigt sich vor allem bei der Anwendung von Effizienzkennzahlen wie dem Power Usage Effectiveness (PUE). Da Co-Location-Betreiber keinen direkten Einfluss auf die Auslastung und Energieeffizienz der von ihren Kunden betriebenen IT-Systeme haben, sollte dieser strukturelle Unterschied in der regulatorischen Bewertung angemessen berücksichtigt werden.
- Rechenzentren sollten **KI-gestützte Observability und Cybersicherheit** einsetzen, um Echtzeit-Transparenz und proaktive Bedrohungserkennung zu ermöglichen und so die betriebliche Resilienz und Vertrauenswürdigkeit zu erhöhen.
- **Energieeffizienz und Nachhaltigkeit gezielt fördern:** Die Einführung klarer Energieeffizienzstandards und transparenter Nachhaltigkeitsbewertungssysteme kann kontinuierliche Effizienzsteigerungen in Rechenzentren vorantreiben und zur Reduzierung der Umweltbelastung beitragen. Dabei sollte der Fokus nicht allein auf verbindlichen Mindestanforderungen liegen, sondern ebenso auf wirksamen Anreizen für einen klimafreundlichen Betrieb. Gleichzeitig gilt es, bürokratische Hürden zu minimieren, um Unternehmen die Implementierung nachhaltiger Technologien und Prozesse zu erleichtern. Ein effizientes Anreizsystem, das sowohl kurzfristige Förderinstrumente als auch langfristige Vorteile – etwa steuerliche Erleichterungen oder gezielte Subventionen – umfasst, kann den Übergang zu umweltfreundlicheren Rechenzentren beschleunigen und die Wettbewerbsfähigkeit der europäischen Branche im globalen Wettbewerb nachhaltig stärken.
- Bereitstellung finanzieller Anreize für die Einführung von **Energiemanagementsystemen und energieeffizienten IKT-Technologien** in Rechenzentren, um Energieverschwendung zu reduzieren, Betriebskosten zu senken und den CO<sub>2</sub>-Fußabdruck zu minimieren.
- Förderung der **Nutzung von Prinzipien des zirkulären Designs in Rechenzentren**, um die Lebensdauer von Produkten zu verlängern (z. B. modulare Server).
- **Förderung von Hardware-/Software-Lifecycle-Management-Richtlinien**, die eine zeitnahe Entfernung und den Ersatz veralteter Geräte sicherstellen, um Sicherheitsrisiken zu verringern und die Skalierbarkeit der Infrastruktur zu erhalten. Dies trägt entscheidend dazu bei, die allgemeine Sicherheit und Zuverlässigkeit von Rechenzentren zu verbessern.
- **Zuverlässige und erschwingliche Energie ist entscheidend:** Der beste Weg, kurzfristig die verfügbare Energie zu maximieren, ist die Modernisierung des Stromnetzes und der verstärkte Einsatz energieeffizienter Technologien.
- Investitionen oder finanzielle Unterstützung für Rechenzentrumsinfrastruktur und -komponenten sollten an die **Implementierung von Secure-by-Design-Technologien** geknüpft sein.

- **Digitale Zwillinge** sind ein zentraler Anwendungsfall für Künstliche Intelligenz, gerade auch im industriellen Kontext. Diese sollten daher bei der Rechenzentrumsstrategie entsprechend berücksichtigt werden.

## 6. Welche Rolle sollte der Staat bei der Entwicklung einer souveränen und resilienten Recheninfrastruktur einnehmen?

**Der Staat sollte eine koordinierende Rolle bei der Entwicklung und gezielten Förderung einer souveränen und resilienten Recheninfrastruktur übernehmen.**

Der Staat sollte bei der Entwicklung einer souveränen und resilienten Recheninfrastruktur eine aktive und koordinierende Rolle übernehmen, insbesondere als strategischer Investor, Regulierer und Förderer von Cybersicherheit, Datenzugang und Humankapital. Er sollte klare Rechts- und Sicherheitsstandards setzen, Förderprogramme gestalten und die Digitalisierung öffentlicher Einrichtungen vorantreiben. Gleichzeitig sollte sich der Staat bewusst zurückhalten, wenn es um den operativen Betrieb von Rechenzentren, die konkrete Technologieauswahl, die Entwicklung von KI-Anwendungen oder das Preis- und Ressourcenmanagement geht. Diese Bereiche sollten dem Markt, privaten Investoren und Forschungseinrichtungen überlassen bleiben, um Wettbewerb, Innovation und Effizienz zu fördern. So entsteht ein ausgewogenes Verhältnis zwischen staatlicher Steuerung und unternehmerischer Freiheit, das langfristig eine leistungsfähige, souveräne und international wettbewerbsfähige Recheninfrastruktur sichert.

Der Staat sollte als **strategischer Investor** auftreten: Durch ambitionierte Programme wie „AI Factories“ und „Gigafactories“ kann er gezielt Impulse setzen und technologische Entwicklungen vorantreiben. Dabei ist es entscheidend, dass Förder- und Finanzierungsmechanismen zentrale Qualitätskriterien wie Sicherheit, Resilienz und Energieeffizienz systematisch einbeziehen. Flexible Finanzierungsmodelle sollten zudem sowohl souveräne als auch Public-Cloud-Dienste adressieren, um technologischen Wettbewerb und Auswahlfreiheit sicherzustellen.

Gleichzeitig ist es Aufgabe des Staates als **Rahmengeber und Standardisierer** zu fungieren und einen klaren, innovationsfreundlichen Rechtsrahmen zu schaffen – insbesondere im Hinblick auf die Cybersicherheitsanforderungen an Betreiber kritischer Infrastrukturen. Einheitliche Standards und praxistaugliche Vorgaben sorgen für Planungssicherheit, fördern Vertrauen in neue Technologien und stärken langfristig die digitale Souveränität.

Darüber hinaus übernimmt der Staat eine wichtige Rolle als **Förderer von Cybersicherheit und Resilienz**. Er unterstützt die Integration robuster Cybersicherheitsstrategien in Investitionsprojekte, fördert den gezielten Einsatz von KI-gestützten Sicherheitstools und stärkt die Zusammenarbeit mit der Privatwirtschaft bei der Entwicklung von Leitlinien für den sicheren und verantwortungsvollen Einsatz von KI-Systemen.

Außerdem sollte er als **Wegbereiter für Datenflüsse und Innovation** agieren, indem er die Politik für internationale Datenflüsse stärkt, die DSGVO so anpasst, dass sie die KI-Entwicklung nicht unnötig behindert, und Optionen zum Schutz kuratierter KI-Datensätze prüft.

Er muss Genehmigungsverfahren straffen und verbindliche Maßnahmen zur Identifizierung und zum Ersatz veralteter Anlagen einführen. Zudem sollte er die **Entwicklung und Übernahme internationaler KI-Standards** aktiv fördern und die europäische Standardisierungsarbeit daran ausrichten.

Zuletzt muss der Staat als **Vorreiter bei der Digitalisierung des öffentlichen Sektors** agieren, indem er die Cloud-Migration vorantreibt, veraltete Infrastrukturen modernisiert und eine effektive Datenstrategie entwickelt, die fragmentierte Datensätze aufricht und Interoperabilität sicherstellt. Gleichzeitig sollte der Staat gezielt in Humankapital investieren, indem er Aus-, Weiter- und Umschulungsprogramme in Partnerschaft mit der Privatwirtschaft fördert und die Auswirkungen von KI auf Arbeitskräfte in Schlüsselbranchen systematisch untersucht. So werden technologische Modernisierung, effiziente Verwaltungsprozesse und Fachkräfteentwicklung zu einem integrierten Ansatz, der die digitale Resilienz und Innovationsfähigkeit Deutschlands nachhaltig stärkt.

## Fazit

Aus Sicht des Wirtschaftsrates ist ein zukunftsfähiger Rechenzentrumsstandort in Deutschland nur durch ein Zusammenspiel aus **technologischer Leistungsfähigkeit, verlässlicher Energieversorgung, robuster Cybersicherheit, qualifizierten Fachkräften und einem innovationsfreundlichen regulatorischen Umfeld** möglich. Der Staat sollte dabei als aktiver Förderer und strategischer Partner agieren, um Investitionen zu erleichtern, Standards zu setzen und Rahmenbedingungen für eine nachhaltige und souveräne digitale Infrastruktur zu schaffen. Die konsequente Umsetzung dieser Maßnahmen wird nicht nur die Wettbewerbsfähigkeit Deutschlands auf globaler Ebene stärken, sondern auch die Innovationskraft der Wirtschaft fördern, Arbeitsplätze sichern und eine vertrauenswürdige Grundlage für die Nutzung von KI und weiteren digitalen Technologien schaffen. Für den Wirtschaftsrat ist klar: Eine strategisch geplante, resiliente und international vernetzte Rechenzentrumsinfrastruktur ist zentral für die digitale Souveränität Deutschlands und ein entscheidender Standortfaktor für Wirtschaft und Gesellschaft.