Nationale Rechenzentrumsstrategie

Titel: Nationale Rechenzentrumsstrategie— Wegweiser für eine dezentrale, souveräne und resiliente Data-Center-Infrastruktur

Autor: Stephan Krausenegger KDI GmbH - Gesellschaft für Kommunikation, Datentechnik und Informationssysteme

Kontakt: stephan.krausenegger@kdit.de

München, 20.10.2025

Inhalt

Abstract

Dieses Dokument ist die Zusammenfassung einer Stellungnahme des Autors, die im Rahmen des Konsultationsprozesses für die Nationale Rechenzentrumsstrategie des Bundesministeriums für Digitales und Staatsmodernisierung erstellt wurde.

Im Rahmen der Stellungnahme wurden die einzelnen inhaltlichen Themenschwerpunkte des Artikels in Umfang und Tiefe ausführlich ausgearbeitet. Diese Zusammenfassung ist als Überblick über die zentralen, wichtigen und kritischen Rahmenbedingungen zu sehen und soll als Diskussionsgrundlage hinsichtlich Planung und Durchführung der erforderlichen Maßnahmen dienen. Jedes der aufgeführten inhaltlichen Themen erfordert darüber hinaus eine eigene dedizierte strategische und konzeptionelle Ausarbeitung.

Dieses Manuskript skizziert ein operationalisierbares Konzept für eine nationale Rechenzentrumsstrategie in Deutschland bis 2030 und darüber hinaus. Es formuliert ein Zielbild, legt zentrale Anforderungen an Standortwahl, Energieversorgung, Konnektivität, Sicherheit und Ausbildung dar und präsentiert einen priorisierten Maßnahmenplan (kurzfristig, mittelfristig, langfristig). Die vorgeschlagene Strategie verfolgt das Ziel, hoheitliche Aufgaben

resilient zu betreiben, digitale Souveränität zu stärken und die Grundlage für eine wettbewerbsfähige Digitalindustrie zu legen.

1. Einleitung

Rechenzentren (Data Center) sind heute integraler Bestandteil staatlicher Funktionsfähigkeit, industrieller Wertschöpfung und gesellschaftlicher Grundversorgung. Die zunehmende Digitalisierung macht sie zu kritischen Infrastrukturen. Ausfälle betreffen Verwaltung, Gesundheitswesen, Finanzsysteme und Verteidigung aber auch alle anderen wirtschaftlichen Sektoren. Vor diesem Hintergrund zielt die vorliegende Strategie auf die Schaffung eines flächendeckenden, dezentralen und resilienten Rechenzentrumsnetzes in Deutschland bis 2030 und darüber hinaus ab. Der Fokus liegt zunächst auf hoheitlichen Anforderungen. Die Herstellung einer Allgemeingültigkeit für privatwirtschaftliche Bereiche ist sinnvoll. Diese Bereiche, die im Einzelnen noch festzulegen sind, werden in die Strategie insofern integriert, als sie regulatorisch und infrastrukturell Relevanz für die Gesamtsicherheit besitzen.

2. Zielbild und Grundprinzipien

Ein zukunftsfähiger Data-Center-Standort Deutschland zeichnet sich durch folgende Merkmale aus:

- Dezentrale Flächenverteilung zur Vermeidung von Single-Point-Risiken.
- Modulare, erweiterbare Arealkonzepte zur technischen Ertüchtigung und ringtauschartigen Modernisierung.
- Mehrfache Redundanz in Energie- und Datenanbindung; planbare Verfügbarkeit über 24/7-Zeiträume.
- Verbindliche Sicherheits- und Datenschutzstandards (Zero-Trust, Resilienztests, unabhängige Audits).
- Stärkung einer souveränen Lieferkette für kritische Hardware und Software durch gezielte Fördermaßnahmen.
- Systematische Nutzung von Abwärme zur Erhöhung der Energieeffizienz und gesellschaftlichen Akzeptanz.

Diese Prinzipien bilden die Grundlage für die nachfolgenden Maßnahmen und Governance-Empfehlungen.

3. Standort- und Flächenpolitik

Konzentrierte Hot-Spots bergen erhöhte Bedrohungspotenziale. Eine dezentrale Strategie verfolgt daher zwei Kernziele:

(1) Reduktion geografischer Konzentration durch verteilte Cluster

(2) Schaffung großflächiger, modular nutzbarer Areale, die technischen Austausch und sukzessive Erneuerung erlauben.

Ein bundesweiter Flächennutzungsplan muss Top-Lagen, bevorzugte Gebiete und Ausschlusszonen unter Berücksichtigung von hydrologischen, klimatischen und sicherheitsrelevanten Kriterien ausweisen. Von übergeordneter Bedeutung ist dabei die Bereitstellung von Energie, in ausreichender Menge, zuverlässig und sicher und zu wettbewerbsfähigen Preisen.

Empfehlungen:

- Entwicklung einer kartographierten Standortstrategie als Grundlage für Genehmigungsentscheidungen.
- Flächenreserve für modulare Erweiterung und Ringtauschverfahren festlegen.

4. Energieversorgung und Abwärmenutzung

Energie ist das zentrale betriebliche Risiko für Data Center. Eine rationale Strategie berücksichtigt Verfügbarkeit, Preis, Redundanz und Nachhaltigkeit. Planungsvorgaben sollten übergeordnete und umfassende 15-Jahres-Lastszenarien integrieren, multiple Lieferquellen vorsehen und moderne Notstromkonzepte einbinden.

Abwärme ist als wirtschaftliche und ökologische Ressource zu behandeln. Die Einspeisung in urbane Wärmenetze oder industrielle Kreisläufe reduziert Gesamtkosten und erhöht gesellschaftliche Akzeptanz.

Empfehlungen:

- Einbettung regionaler Energieplanungen in nationale Lastszenarien.
- Standardisierte Verträge und technische Schnittstellen für Abwärmeübergabe definieren.
- Einbindung neuer Energiequellen (z. B. Small Modular Nuclear Reactors) in die strategische Planung offenhalten.

5. Konnektivität und Lieferkettensicherheit

Sichere, vielfach redundante Datenanbindungen sind Voraussetzung. Neben mehreren Glasfasertrassen müssen alternative Übertragungswege (Mobilfunk, Satellit) berücksichtigt werden. Darüber hinaus ist die Abhängigkeit von nicht-europäischen Herstellern als Risiko zu bewerten und schrittweise zu reduzieren.

Empfehlungen:

- Mindestanforderungen an Trassen-Diversität und Provider-Pluralität in Standortentscheidungen verankern.
- Förderprogramme zur Entwicklung vertrauenswürdiger europäischer Zulieferer aufsetzen.

6. Sicherheit, Datenschutz und bauliche Resilienz

Sicherheitsarchitekturen müssen auf Zero-Trust-Prinzipien basieren; Resilienz ist cyclisch / permanent durch Pen-Tests, Ausfall-Szenarien und unabhängige Audits zu prüfen. Bauliche Vorkehrungen und Maßnahmen sind erforderlich, um Risiken des Klimawandels und militärische Bedrohungsszenarien abzumildern.

Empfehlungen:

- Einführung verbindlicher Resilienz-Prüfzyklen und Auditstandards.
- Katalog zur Klassifizierung hoheitlicher und kritischer Data Center entwickeln, gekoppelt an regulatorische Pflichten.

7. Fachkräfte, Ausbildung und Innovationsökosystem

Langfristige Versorgungssicherheit hängt wesentlich von der Ausbildung und Bindung qualifizierten Personals ab. Frühförderung, curriculare Anpassungen und eine enge Verzahnung zwischen Forschung und Wirtschaft sind erforderlich. Staatliche Anreize und Förderungen für Startups und Serienfertiger relevanter Hardware- und Softwarekomponenten stärken die nationale Souveränität.

Empfehlungen:

- Nationale Ausbildungsoffensive mit Stipendien, Praktikums- und Traineeprogrammen.
- Förderung öffentlicher Forschungspartnerschaften und technischer Inkubatoren.

8. Governance und staatliche Rolle

Für Data Center, die hoheitliche Aufgaben erfüllen, sollten Bund und Länder die volle Verantwortung über den gesamten Lebenszyklus übernehmen. Zur operativen Steuerung ist eine zentrale, ministerial angesiedelte Steuerungsstelle einzurichten, flankiert von einem interministeriellen Lenkungskreis. Staatlich initiierte Betreibergesellschaften können operativ marktwirtschaftlich handeln, müssen jedoch Transparenz- und Leistungsanforderungen erfüllen.

Empfehlungen:

- Einrichtung einer zentralen Steuerungsstelle mit Mandat zur Flächen- und Infrastrukturkoordination.
- Entwicklung eines Priorisierungskatalogs für kritische Dienste und entsprechende Regulierungsmechanismen.

9. Priorisierter Maßnahmenplan

Kurzfristig (0–18 Monate)

- Einrichtung zentraler Steuerungsinstanzen und Fast-Lane-Genehmigungen für priorisierte hoheitliche Projekte.
- Einführung verbindlicher Mindeststandards (Redundanz, Zero-Trust, Resilienzprüfungen).

Mittelfristig (18–48 Monate)

- Erstellung einer bundesweiten Flächennutzungskarte; Ausbau regionaler Energie- und Glasfaserinfrastruktur nach 15-Jahres-Lastszenarien.
- Förderprogramme zur Nivellierung der Erschließungs- und Betriebskosten auf internationales Niveau; Aufbau vertrauenswürdiger Zuliefernetzwerke.

Langfristig (48+ Monate)

- Nationale Ausbildungsoffensive
- Integration von Abwärmenutzung in kommunale Wärmepläne.
- Kontinuierliche Harmonisierung mit EU-Partnern zur Stärkung der digitalen Souveränität.

10. Risiken und Gegenmaßnahmen

Hauptgefahren sind Verzögerungen im Netzausbau, volatile Energiepreise, geopolitische Lieferengpässe und personelle Engpässe. Gegenmaßnahmen umfassen priorisierte Infrastrukturfinanzierung, europäische Abstimmungen zur Energiepolitik, gezielte Aufbauprogramme für Zulieferketten und Reformen im Bildungsbereich.

Als zentrales Risiko ist der Einsatz von Hardware und Software von Herstellern aus nicht vertrauenswürdigen Drittstaaten zu sehen. Zum einen könnten diese Lieferanten auf staatliche Anordnung die Versorgung einstellen, zum anderen besteht das Risiko absichtlich eingebauter Schwachstellen, zum Zweck der Spionage und Sabotage.

11. Schlussfolgerung

Die Implementierung einer nationalen Rechenzentrumsstrategie ist Chefsache. Nur ein integriertes Vorgehen, das Standortplanung, Energie- und Dateninfrastruktur, Sicherheitsstandards und Ausbildung verzahnt, schafft die Grundlage für eine souveräne und resiliente Digital-Industrie bis 2030. Die vorgeschlagenen Maßnahmen sind operationalisierbar und erfordern jetzt koordinierte politische Entscheidungen und verbindliche Zeitpläne.

Literatur / Quellenhinweis

Zur Erstellung dieses Dokuments, bzw. der zu Grunde liegenden „Stellungnahme zur Nationalen Rechenzentrumsstrategie“ wurden im Rahmen der Recherche unterschiedliche KI Werkzeuge eingesetzt. Die von der KI verwendeten Quellen sind nicht bekannt.