WIRTSCHAFTSRAT Deutschland

Stellungnahme zur Entwicklung einer nationalen Rechenzentrumsstrategie

Wirtschaftsrat der CDU e.V.

Die Stimme der Sozialen Marktwirtschaft

September 2025

Einleitung

Deutschland steht vor der zentralen Aufgabe, seine Rechenzentrumsinfrastruktur zukunftsfähig, resilient und international wettbewerbsfähig aufzustellen. Als Wirtschaftsrat sehen wir leistungsstarke, sichere und energieeffiziente Rechenzentren als unverzichtbare Grundlage für Innovation, digitale Transformation und die langfristige Wettbewerbsfähigkeit der deutschen Wirtschaft.

Angesichts der rasant wachsenden Nutzung von KI-Anwendungen, steigender Anforderungen an Datensicherheit und der Notwendigkeit einer nachhaltigen Energieversorgung muss Deutschland Rechenzentren als strategische Schlüsselressource der Digitalisierung anerkennen. Entscheidend ist, dass der Standort nicht nur weiterentwickelt und an internationale Standards angepasst wird, sondern diese aktiv mitgestaltet. Gleichzeitig gilt es, Resilienz, Fachkräfteentwicklung und technologische Exzellenz gezielt zu fördern.

Wir begrüßen ausdrücklich die Möglichkeit, uns aktiv in die Entwicklung einer nationalen Rechenzentrumsstrategie des Bundesministeriums für Digitales und Staatsmodernisierung einzubringen. Im Folgenden stellen wir unsere Perspektiven und Empfehlungen vor, wie Deutschland bis 2030 zu einem führenden Standort für Rechenzentren werden kann – einer Infrastruktur, die technologische Leistungsfähigkeit, wirtschaftliche Effizienz und gesellschaftliche Verantwortung gleichermaßen vereint. Für einen weiterführenden fachlichen Dialog stehen wir selbstverständlich jederzeit gerne zur Verfügung.

1. Welche Merkmale und Rahmenbedingungen kennzeichnen aus Ihrer Sicht einen „zukunftsfähigen und leistungsstarken“ Rechenzentrumsstandort Deutschland im Jahr 2030?

Ein zukunftsfähiger und leistungsstarker Rechenzentrumsstandort Deutschland basiert auf einem ausgewogenen Mix aus großskaligen Hyperscalern, Unternehmens-, Edge- und regionalen Co-Location-Rechenzentren. Gemeinsam bilden sie eine robuste, KI-native Infrastruktur, die skalierbare und sichere Lösungen für anspruchsvolle KI-Workloads ermöglicht. Dazu gehören moderne Rechenzentren, Hochgeschwindigkeitskonnektivität und leistungsfähige Netzwerke, die den wachsenden Anforderungen gerecht werden, Engpässe vermeiden und so die Effizienz von KI-Training und Echtzeitanwendungen sichern.

Eine nationale Rechenzentrumsstrategie muss daher gezielt Rahmenbedingungen schaffen, um diese Vielfalt und Dynamik langfristig zu erhalten – und darf keine einseitige Konsolidierung hin zu wenigen Hyperscalern fördern.

Eine **effiziente, zuverlässige und wettbewerbsfähige Energieversorgung** ist für den Rechenzentrumsstandort Deutschland von zentraler Bedeutung. Dazu gehören digitale Lösungen für ein intelligentes Energiemanagement ebenso wie die Diversifizierung der Energiequellen. Der Einsatz energieeffizienter Rechenzentrums- und IT-Infrastruktur ist dabei ein entscheidender Hebel.

Zukunftsfähigkeit bedeutet auch, **Cybersicherheit und Resilienz ganzheitlich zu denken** – über die gesamte Wertschöpfungskette hinweg. Dazu zählen die Integration von KI in Sicherheitslösungen zur Erkennung, Vorhersage und Abwehr von Bedrohungen ebenso wie die konsequente Anwendung international anerkannter Sicherheitsstandards und Risikomanagement-Frameworks. Ein moderner Rechenzentrumsstandort schafft darüber hinaus **Zugang zu Spitzentechnologien** und bildet damit das Rückgrat für Innovation und digitale Souveränität.

Ein hybrider Ansatz, der sowohl globale Public-Cloud-Kapazitäten als auch lokale Angebote einbezieht, ermöglicht es Unternehmen, Industrie und weiteren Nutzergruppen, ihre spezifischen Anforderungen bestmöglich zu erfüllen. Die Förderung internationaler Datenflüsse ist dabei essenziell, um den Zugang zu qualitativ hochwertigen Daten sicherzustellen.
Gleichzeitig ist es wichtig, auf EU- und nationaler Ebene konsequent an der Entwicklung und Harmonisierung internationaler Standards zu arbeiten. Entscheidend ist, regulatorische Barrieren innerhalb der EU abzubauen und eine einheitliche Gesetzgebung zu etablieren – anstatt, wie im Fall des E-Invoicing, auf nationale Sonderwege zu setzen. Nur ein tatsächlich barrierefreier europäischer Datenraum ermöglicht die effiziente Nutzung hochwertiger Datenströme, Trainingsdaten und KI-Lösungen – und stärkt damit die internationale Wettbewerbsfähigkeit.

Zudem müssen bestehende europäische Digitalrechtsregulierungen gezielt entschlackt werden – insbesondere mit Blick auf Doppelregulierungen und Inkohärenzen im Bereich des Produktsicherheitsrechts.

Qualifizierte Fachkräfte sind ein zentraler Erfolgsfaktor für den Rechenzentrums- und Digitalstandort Deutschland. Kontinuierliche Aus-, Weiter- und Umschulungsprogramme lassen sich besonders wirksam in Partnerschaft mit Unternehmen und der Wirtschaft umsetzen und fördern. Initiativen wie die *Allianz für Digitale Kompetenzen* – ein Zusammenschluss des Bayerischen Digitalministeriums mit Unternehmen, der auf digitale Breitenbildung abzielt – sollten gestärkt, stärker bekannt gemacht und als Modell für andere Regionen und Zielgruppen genutzt werden. Gleichzeitig fehlt bislang eine tragfähige Strategie, um dem akuten Fachkräftemangel im Hochtechnologiesektor – insbesondere bei hochqualifizierten Spezialistinnen und Spezialisten – kurzfristig zu begegnen. Während die genannte Allianz vor allem auf eine breite digitale Grundqualifizierung ausgerichtet ist, bleibt die gezielte Förderung von *High Potentials* in Schlüsselbereichen wie Künstlicher Intelligenz unzureichend. Zwar ist es wichtig, klar zwischen Maßnahmen zur digitalen Breitenbildung und den Anforderungen im Hochtechnologiebereich zu unterscheiden – doch dürfen diese Ansätze nicht gegeneinander ausgespielt werden. Aus Sicht des Wirtschaftsrats ist es in beiden Fällen sinnvoll, auf bewährte Initiativen aus der Wirtschaft zurückzugreifen und diese gezielt zu stärken.

Eine **digitalisierte öffentliche Verwaltung**, die Cloud-Migration, den Einsatz von Künstlicher Intelligenz und die Modernisierung ihrer IT-Infrastruktur in den Mittelpunkt stellt, kann als Vorbild dienen und ein innovationsfreundliches, KI-affines Ökosystem fördern. Dabei müssen auch sicherheitspolitische Anforderungen von Anfang an mitgedacht werden.

2. Welche zentralen Herausforderungen und Chancen sehen Sie für den Rechenzentrumsstandort Deutschland in den kommenden Jahren?

Eine der zentralen Herausforderungen für den digitalen Fortschritt in Deutschland sind bestehende **Infrastrukturlücken** – sie behindern die Einführung und Nutzung von Künstlicher Intelligenz erheblich. Der **wachsende Energiebedarf** KI-basierter Rechenzentren bringt die bestehende Energieinfrastruktur an ihre Grenzen. Zugleich erschweren **Konnektivitätsdefizite** und langwierige Genehmigungsverfahren beim Breitbandausbau den notwendigen Ausbau digitaler Netze.
Auch die zunehmende Komplexität der **Cybersicherheitsrisiken** – etwa durch KI-spezifische Schwachstellen oder Angriffe auf Lieferketten – erfordert neue, vorausschauende Schutzstrategien. Der anhaltende **Fachkräftemangel** in den Bereichen KI und Cybersicherheit verlangsamt zusätzlich die technologische Entwicklung.

Nicht zuletzt kann **regulatorische Komplexität** – etwa durch divergierende Vorschriften und nationale Sonderwege – Innovationen hemmen und den Zugang zu Spitzentechnologien unnötig erschweren.

Gleichzeitig eröffnen sich erhebliche Chancen: Geplante Investitionen in KI-Infrastrukturen – etwa in „AI Factories“ und „Gigafactories“ – können dazu beitragen, den wachsenden Bedarf zu decken und den Innovationsstandort Deutschland nachhaltig zu stärken. Der steigende Energiebedarf kann als Impuls für die Modernisierung der Energieinfrastruktur genutzt werden und dabei helfen, Energieeffizienz systematisch in den Betrieb von Rechenzentren zu integrieren.
Auch im Bereich Cybersicherheit entstehen neue Potenziale: KI-gestützte Sicherheitslösungen ermöglichen eine proaktivere Bedrohungserkennung und -abwehr. Insbesondere generative KI kann die Benutzerfreundlichkeit von Sicherheitssystemen verbessern und zugleich neue Zielgruppen für die Fachkräfteentwicklung erschließen. **Eine intensivere internationale Zusammenarbeit und die Förderung einheitlicher Standards** stärken die Interoperabilität und steigern die globale Wettbewerbsfähigkeit europäischer Lösungen. Zugleich kann die digitale Transformation der öffentlichen Verwaltung nicht nur Effizienzgewinne bringen, sondern auch die Resilienz kritischer Infrastrukturen erhöhen. **Durch gezielte Förderung von Kompetenzen und Talenten – etwa im Rahmen öffentlich-privater Partnerschaften – lässt sich der Fachkräftemangel systematisch adressieren.** Dies ist eine wesentliche Voraussetzung für nachhaltiges Wirtschaftswachstum und die Stärkung der internationalen Wettbewerbsfähigkeit Deutschlands.

3. Welche Rahmenbedingungen sollten aus Ihrer Sicht wie verändert werden, um Rechenzentrumsinvestitionen zu fördern und Innovation zu ermöglichen?

Im Bereich **Förderung und Beschaffung** ist es entscheidend, dass Finanzierungsmechanismen und öffentliche Beschaffungsprozesse explizit **Qualitätskriterien wie Sicherheit, Resilienz und Energieeffizienz** berücksichtigen. Gleichzeitig sollte der Wettbewerb gestärkt werden, um den Zugang zu den besten verfügbaren Technologien zu gewährleisten. Flexible Finanzierungsinstrumente können dabei sowohl souveräne als auch öffentliche Cloud-Dienste gezielt fördern.

Die **Energiepolitik** sollte einen dualen Ansatz verfolgen, der einerseits die Energiebeschaffung beschleunigt und andererseits die **Energieeffizienz von KI-Technologieinfrastrukturen** verbessert. Dies erfordert strategische Investitionen in die Modernisierung des Stromnetzes sowie die Diversifizierung der Energiequellen. Begleitend dazu sind eine europaweite Harmonisierung der regulatorischen Anforderungen an Energieeffizienz und Nachhaltigkeit von Rechenzentren sowie fiskalische Anreize für den Einsatz energieeffizienter Hardware notwendig.

Im Bereich **Konnektivität** müssen gezielte Anreize für Breitbandinvestitionen geschaffen und deren zügige Umsetzung sichergestellt werden. Dazu gehört insbesondere eine Straffung regulatorischer Anforderungen und Verfahren bei Genehmigungsbehörden, um den Ausbau von Rechenzentren und Hochgeschwindigkeitsnetzen deutlich zu beschleunigen.

Cybersicherheit sollte integraler Bestandteil von Investitionsprojekten sein – etwa durch verpflichtende Risikomanagement-Richtlinien. Gleichzeitig ist die gezielte Förderung von KI-basierten Tools in der Cyberabwehr notwendig, um Bedrohungen frühzeitig und effizient zu erkennen.

Dabei gilt: KI-Systeme in Sicherheitsanwendungen dürfen im Rahmen des **EU AI Act** nicht pauschal als Hochrisiko-Technologien eingestuft werden, um Innovationen nicht zu behindern. Eine regulatorische Angleichung und gegenseitige Anerkennung von Zertifizierungsverfahren auf europäischer Ebene sind entscheidend, um Kompatibilität, Vertrauen und Investitionssicherheit zu gewährleisten.

Die **Datenpolitik** sollte internationale Datenflüsse stärken und Datengesetze so anpassen, dass sie die KI-Entwicklung nicht behindert. Auch der Schutz kuratierter KI-Datensätze, einschließlich möglicher IP-Schutzrechte, sollte geprüft werden.

Im Bereich **Standardisierung** ist es wichtig, die europäische Standardisierungsarbeit mit bestehenden internationalen Standards abzustimmen und industriegeführte, marktorientierte Standards zu unterstützen.

Schließlich sollten bei der **öffentlichen Beschaffung** die Prozesse modernisiert werden, um ein umfassendes Verständnis für neue technologische Lösungen zu ermöglichen. Dabei gilt es Innovationen zu stärken und einen Mix aus internationalen und europäischen Angeboten zu stärken. Von diesem offenen Wettbewerb profitiert die Wirtschaft.

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

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

Der Staat sollte eine zentrale Rolle bei der Entwicklung und Förderung einer souveränen und resilienten Recheninfrastruktur einnehmen – sowohl als **strategischer Investor als auch als**

Regulierungsgeber: 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 **Regulierungsgeber und Standardisiere** 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.

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.

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.

Zuletzt muss der Staat als **Vorreiter bei der Digitalisierung des öffentlichen Sektors** fungieren, indem er die Cloud-Migration und Modernisierung veralteter Infrastrukturen vorantreibt und eine effektive Datenstrategie entwickelt, die fragmentierte Datensätze aufbricht und Interoperabilität fördert. Und schließlich sollte der Staat ein **Investor in Humankapital** sein, indem er Aus-, Weiter- und Umschulungsprogramme, insbesondere in Partnerschaft mit dem Privatsektor fördert und die Auswirkungen von KI auf die Arbeitskräfte in Schlüsselbranchen erforscht.

5. Gibt es konkrete Maßnahmen oder Best Practices aus Ihrer Praxis/Erfahrung, die in die Strategie aufgenommen werden sollten?

- **Förderung von Investitionen in robuste, skalierbare digitale Infrastrukturen**: Rechenzentren müssen KI-Workloads unterstützen, die Hochdurchsatz- und Niedriglatenz-Netzwerke erfordern. Investitionen in skalierbare Netzwerke (connectivity network) sind ebenfalls entscheidend für die Zukunft des Edge Computing, welches für latenzkritische KI-Anwendungen wichtig ist. Rechenzentren sind entscheidend für Inferenz/Training, doch der Trend geht hin zu einer stärker

verteilten Datenverarbeitung. Insofern sollte sowohl der Bedarf an zentralisierten Rechenzentren als auch an Edge Computing in der Strategie berücksichtigt werden.

- Anforderungen an **Unternehmensrechenzentren** berücksichtigen: Nicht nur Hyperscale-Rechenzentren sind wichtig, um Innovationen und die Einführung von KI zu fördern, sondern Unternehmen müssen auch ihre bestehenden Rechenzentren modernisieren, um die steigenden Anforderungen an die Datenverarbeitung durch KI bewältigen zu können. Investitionen in solche technischen Erneuerungen sollten gefördert und erleichtert werden. Außerdem unterliegen Rechenzentren in gemischt genutzten Einrichtungen (z. B. Gewerbeparks) oft Beschränkungen hinsichtlich der verfügbaren Strommenge, was wiederum die Rechenkapazität begrenzt.

- **Co-Location-Rechenzentren** sind insbesondere für die Digitalisierung mittelständischer Unternehmen von großer Bedeutung: Dennoch wird diese Form der Rechenzentren, insbesondere im Rahmen des Erneuerbare-Energien-Gesetzes (EEG), bislang vom Gesetzgeber nicht ausreichend berücksichtigt. Dies gilt insbesondere bei der Vorgabe von Effizienzkennzahlen wie dem Power Usage Effectiveness (PuE). Da CoLo-Betreiber keinen direkten Einfluss auf die Auslastung der Kundensysteme haben, sollte dies in der regulatorischen Bewertung 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.

- Die Einführung klarer **Energieeffizienzstandards und Nachhaltigkeitsbewertungssysteme** wird kontinuierliche Verbesserungen bei der Energieeffizienz von Rechenzentren fördern und dazu beitragen, die Umweltbelastung zu verringern.

- Bereitstellung finanzieller Anreize für die Einführung von **Energiemanagementsystemen und energieeffizienten IKT-Technologien** in Rechenzentren, um Energieverschwendung zu reduzieren, Betriebskosten zu senken und den CO_2-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 und/oder die Verwendung der Mittel für Cybersicherheit ermöglichen.

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

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.