

Deutscher Landkreistag, Postfach 11 02 52, 10832 Berlin

Ulrich-von-Hassell-Haus
Lennéstraße 11
10785 Berlin

Tel.: 030 590097-353
Fax: 030 590097-400

E-Mail: Andree.Pruin
@Landkreistag.de

AZ: II-25

Datum: 23.09.2025

**Bundesministerium für Digitales und
Staatsmodernisierung**
Referat DW II 5 - Recheninfrastruktur und
Anwendungen

Per Mail

Stellungnahme des Deutschen Landkreistages zur Konsultation über die Nationale Rechenzentrumsstrategie

Sehr geehrte Damen und Herren,

die digitale Transformation stellt Verwaltung, Wirtschaft und Gesellschaft gleichermaßen vor tiefgreifende Veränderungen. Für die kommunale Ebene gilt dies in besonderem Maße: Landkreise tragen Verantwortung für eine Vielzahl von Leistungen der Daseinsvorsorge, sie bündeln IT-Services für ihre kreisangehörigen Gemeinden, sichern kritische Infrastrukturen in Bereichen wie Katastrophenschutz oder Gesundheitsversorgung und gestalten die Digitalisierung im unmittelbaren Kontakt zu Bürgerinnen und Bürgern. Eine leistungsfähige, sichere und resilient ausgelegte Rechenzentrumsinfrastruktur ist dafür unverzichtbar. Vor diesem Hintergrund begrüßt der Deutsche Landkreistag ausdrücklich das Anliegen der Bundesregierung, mit der Nationalen Rechenzentrumsstrategie die Weichen für einen leistungsfähigen, sicheren und nachhaltigen Rechenzentrumsstandort Deutschland zu stellen. Wir teilen das Ziel des Koalitionsvertrages, Deutschland als Leuchtturm Europas für Rechenzentren zu etablieren und massive Investitionen in Cloud- und KI-Infrastruktur zu initiieren.

Föderale Strukturen sichern Resilienz und Bürgernähe

Eine solche Strategie muss jedoch die föderalen Strukturen unseres Landes respektieren und stärken. Sie darf nicht dazu führen, dass Kommunen in die Rolle bloßer Nutzerinnen gedrängt werden, sondern muss sicherstellen, dass kommunale und regionale Rechenzentren weiterhin eigenverantwortlich handeln und ihre Infrastruktur strategisch steuern können. Nur wenn die kommunale Ebene fest als tragende Säule einbezogen wird, können Resilienz, Bürgernähe, Cybersicherheit und digitale Souveränität gleichermaßen gewährleistet werden.

Eine Konzentration auf wenige Bundesrechenzentren mag oberflächlich betrachtet Effizienzgewinne versprechen, würde aber zugleich Monostrukturen schaffen, die im Falle von Ausfällen oder Angriffen die gesamte Verwaltung anfällig machen: ein gefährlicher Single Point of Failure. Monostrukturen bergen gerade im Bereich der Cyber- und Informationssicherheit erhebliche Risiken, während ein föderiertes Netzwerk von Rechenzentren Angriffe und Störungen besser isolieren und abfangen kann. Eine nationale Strategie kann dabei durchaus auch Rechenzentren des Bundes und der Länder vorsehen, die einzelne zentrale Fachverfahren oder Querschnittsanwendungen standardisiert betreiben; etwa dort, wo gemeinsame Schnittstellen, Registeranbindungen oder besondere Sicherheitsanforderungen

einen zentralisierten Betrieb sinnvoll machen. Entscheidend ist jedoch, dass solche Angebote die föderalen Strukturen ergänzen, den Kommunen freiwillig zur Verfügung stehen und die kommunale Eigenverantwortung unberührt bleibt. Ebenso entscheidend ist, dass überall in der Fläche regionale und kommunale Rechenzentren bestehen bleiben, die die digitale Daseinsvorsorge unmittelbar sichern. Gerade als Edge-Rechenzentren übernehmen sie eine unverzichtbare Rolle: Sie verarbeiten Daten nah am Ort ihrer Entstehung, gewährleisten geringe Latenzzeiten, sichern die Verfügbarkeit auch im Krisenfall und tragen dazu bei, kritische Infrastrukturen wie Energieversorgung, Verwaltungsleistungen, Katastrophenschutz oder Gesundheitsdienste stabil zu halten. Erst im Zusammenspiel von zentralen und dezentralen Rechenzentren entsteht eine resiliente Gesamtarchitektur, die Effizienz und Sicherheit verbindet.

Standardisierung durch Kooperation statt Überregulierung

Standardisierung ist für ein solches Zusammenspiel unverzichtbar, darf jedoch nicht in Überregulierung münden. Einheitliche Mindeststandards, etwa zu Schnittstellen, Containerisierung, Compliance oder Identitätsmanagement, sind notwendig, damit Bund, Länder und Kommunen reibungslos zusammenarbeiten können. In diesem Sinne sollten auch die Anforderungen aus der NIS-2-Richtlinie und dem Cyber Resilience Act als Maßstab für die Ausgestaltung sicherheitsrelevanter Infrastrukturen herangezogen werden; auch wenn sie formal noch nicht verpflichtend für Kommunen sind. Gleichzeitig gilt: Eine zu enge Vorgabe bis ins letzte technische Detail würde Innovation hemmen, regionale Flexibilität einschränken und die Fähigkeit zur eigenständigen Weiterentwicklung beschneiden. Standardisierung muss deshalb Mindestanforderungen verbindlich festlegen, zugleich aber Freiräume für eigenverantwortliche technische Ausgestaltung lassen. Auf diese Weise können Skaleneffekte und Kostenvorteile realisiert werden, ohne in riskante Monostrukturen zu verfallen und Innovation zu hemmen.

Ergänzend ist zu beachten, dass die wachsende Komplexität regulatorischer Anforderungen insbesondere kleinere Kommunen vor erhebliche Umsetzungsprobleme stellt. Umso wichtiger ist es, Vorgaben operationalisierbar zu gestalten und mit gezielten Förderprogrammen zu flankieren. Einheitliche Compliance-Vorgaben müssen so umgesetzt werden, dass Kommunen nicht zusätzlich eigene Aufwände für Datenschutz, Informationssicherheit oder Grundrechtsfolgenabschätzungen tragen, wenn sie zentrale RZ-Angebote nutzen. Dabei ist entscheidend, dass Standardisierung und Vorgaben im kooperativen Schulterschluss von Bund, Ländern, Kommunen, Rechenzentrumsbetreibern und Fachverfahrensherstellern entwickelt werden. Lösungen dürfen nicht von oben herab diktiert werden, sondern müssen gemeinsam tragfähig gestaltet sein.

Schon heute beweisen kommunale und föderale Ansätze, dass föderierte Strukturen leistungsfähig, effizient und zukunftstauglich sein können. Die Bündelung kommunaler IT-Services auf Landkreisebene hilft insbesondere kleineren Gemeinden, Sicherheits- und Serviceanforderungen zu erfüllen, die sie alleine nicht stemmen könnten. Gemeinsame Beschaffungsmodelle senken Kosten, steigern Qualität und schaffen Skaleneffekte. Ergänzend zeigen föderale Cloud-Initiativen – etwa die Deutsche VerwaltungscLOUD bzw. das Cloud-Service-Portal – dass Bund, Länder und Kommunen gemeinsam praxistaugliche und skalierbare Lösungen entwickeln können.

Planungs-, Energie- und Netzinfrasturktur müssen Investitionen ermöglichen

Damit solche Ansätze ihre volle Wirkung entfalten können, braucht es jedoch nicht nur technische Standards und Förderung, sondern auch die passende Infrastruktur vor Ort. Der Staat muss deshalb für verlässliche Rahmenbedingungen sorgen: klare regulatorische Mindeststandards, gezielte Unterstützung bei Betrieb und Sicherheit sowie rechtliche Anpassungen, die den Ausbau von Rechenzentren erleichtern; etwa durch verkürzte und harmonisierte Planungs- und Genehmigungsverfahren im Bau- und Energiebereich. Für die Standortwahl sind neben der kommunalen Planungshoheit auch Fragen des Strukturwandels,

der Flächenverfügbarkeit und der Energieanbindung entscheidend. Regionale und kommunale Rechenzentren sind flächendeckend unverzichtbar, um digitale Daseinsvorsorge, Resilienz und Bürgernähe zu sichern. Dort, wo zusätzlich ein Überangebot an erneuerbarer Energie vorhanden ist – etwa Windkraft im Norden, Photovoltaik im Süden oder Biomasse und Wasserkraft in anderen Regionen –, können Rechenzentren darüber hinaus einen besonderen Beitrag zur Netzentlastung und zur Nutzung regionaler Potenziale leisten. Ebenso entscheidend ist die Verfügbarkeit leistungsfähiger Strom- und Breitbandnetze. Gerade im ländlichen Raum scheitern Ansiedlungen von Rechenzentren bislang oft daran, dass notwendige Netzkapazitäten nicht rechtzeitig bereitgestellt werden können. Die Verfahren für den Netzausbau müssen daher vereinfacht und verbindlich beschleunigt werden, sodass ein leistungsfähiger Anschluss innerhalb klar definierter Fristen gewährleistet ist. Damit Investitionen nicht an jahrelangen Genehmigungsverfahren scheitern, braucht es darüber hinaus beschleunigte Planungs- und Bauverfahren, inklusive Vorzugsflächen in Landes- und Regionalplanungen unter verbindlicher Einbindung der Kommunen, sowie einer besseren Koordinierung mit Netz- und Wärmenetzbetreibern.

Nachhaltigkeit technologieoffen und standortgerecht gestalten

Darüber hinaus muss die Strategie auf Nachhaltigkeit ausgerichtet sein. Rechenzentren sollten CO₂-Emissionen möglichst vermeiden, Energieeffizienz steigern und dort, wo möglich, Abwärme nutzen. Nachhaltigkeitsvorgaben sollten zudem mit energie- und wärmepolitischen Zielsetzungen verzahnt werden. Rechenzentren müssen in die kommunale Wärmeplanung eingebunden werden können, etwa durch verbindliche Abwärmekonzepte im Sinne des § 12 EnEfG. Auch anerkannte Standards wie die DIN EN 50600 sollten für Planung und Betrieb zugrunde gelegt werden. Zugleich muss anerkannt werden, dass kleinere Einrichtungen in ländlichen Räumen teilweise nur begrenzte Potenziale hierfür bieten. Nachhaltigkeitsvorgaben sind daher technologieoffen und standortgerecht zu formulieren und sollten durch gezielte Förderprogramme flankiert werden, die auch kleineren Rechenzentren helfen, ihre Energieeffizienz zu steigern; etwa durch modernisierte Kühlung, Photovoltaik oder lokale Abwärmenutzung. So werden Klimaschutz und Resilienz zusammengeführt, anstatt sie gegeneinander auszuspielen.

Digitale Souveränität braucht europäische Alternativen

Ein weiterer zentraler Punkt ist die Sicherung digitaler Souveränität. Die in den vergangenen Jahren gewachsene Abhängigkeit von Hyperscalern und außereuropäischen Technologien schwächt die Handlungsfähigkeit der Verwaltung. Rechenzentren, die in Kernbereichen auf proprietäre Plattformen angewiesen sind, können nicht souverän agieren. Eine nationale Strategie muss daher klare Leitplanken setzen, um Abhängigkeiten zu reduzieren: durch den verstärkten Einsatz europäischer Lösungen, die gezielte Förderung von Open-Source-Technologien, Multi-Vendor- und Multi-Cloud-Strategien sowie verbindliche Exit-Szenarien, die den sicheren Wechsel von Plattformen ermöglichen. Es reicht dabei nicht, bestehende Hyperscaler-Abhängigkeiten nur zu verringern; es braucht zugleich europäische Alternativen, die technologisch mit den großen Plattformanbietern mithalten können. Nur wenn solche souveränen Cloud- und Plattformangebote auf Augenhöhe verfügbar sind, können Bund, Länder und Kommunen ihre Fachverfahren sicher und zukunftsfähig betreiben. Ebenso wichtig sind vergaberechtlich tragfähige Modelle, die eine kommunale Nutzung von Bundesinfrastrukturen ohne Mehrkosten gegenüber Public-Cloud-Angeboten ermöglichen. Zur Stärkung digitaler Souveränität sollten zudem anerkannte Sicherheitsnachweise wie eine C5-Attestierung des BSI einbezogen werden. Resilienz umfasst dabei nicht nur Unabhängigkeit von Hyperscalern, sondern auch Energieversorgungssicherheit: Notfalllösungen, etwa durch den Einsatz alternativer Energieträger wie Wasserstoff, können die Verfügbarkeit von Rechenzentren auch bei Stromausfällen absichern. Solche Maßnahmen sind in eine nationale Wasserstoff-Infrastruktur einzubetten und müssen regional mitgedacht werden.

Künstliche Intelligenz macht dezentrale Edge-Rechenzentren unverzichtbar

Gerade mit Blick auf Künstliche Intelligenz ist dies besonders wichtig: KI-gestützte Anwendungen erhöhen die Anforderungen an Rechenleistung, Speicher, Verarbeitungsgeschwindigkeit und Sicherheit erheblich. Wenn Daten in Echtzeit oder nahezu Echtzeit verarbeitet werden sollen – etwa bei KI-gestützten Anwendungen in Verkehrssteuerung, Gesundheitswesen oder öffentlicher Sicherheit – sind Edge-Rechenzentren unverzichtbar, da sie Latenzen minimieren und die Einhaltung rechtlicher Vorgaben gewährleisten.

Fazit: Eine föderale Strategie für Resilienz, Nachhaltigkeit und Bürgernähe

Zusammenfassend fordert der Deutsche Landkreistag eine Nationale Rechenzentrumsstrategie, die föderale Strukturen stärkt, verbindliche Mindeststandards etabliert, ohne in Überregulierung zu verfallen, bewährte kommunale Ansätze aufgreift, digitale Souveränität durch Multi-Cloud- und Exit-Strategien sowie die Reduzierung von Hyperscaler-Abhängigkeiten sichert, die steigenden Anforderungen durch Künstliche Intelligenz berücksichtigt und zugleich auf Resilienz, Nachhaltigkeit, wirtschaftliche Impulse und Bürgernähe setzt. Nur so entsteht eine leistungsfähige, sichere und resiliente Infrastruktur, die den Anforderungen des Jahres 2030 gerecht wird und die Landkreise als tragende Säule der digitalen Daseinsvorsorge in Deutschland einbindet.

Mit freundlichen Grüßen
Im Auftrag

Pruin