

1. Zielsetzung, Chancen und Herausforderungen

Antwort auf Leitfrage 2:

„2. Welche zentralen Herausforderungen und Chancen sehen Sie für den Rechenzentrumsstandort Deutschland in den kommenden Jahren? vorangestellt: Aussagen zur Zielsetzung.“

Zielsetzung:

Die Komm.ONE begrüßt ausdrücklich die Initiative des BMDS!

Eine nationale Rechenzentrumsstrategie ist ein Schlüsselfaktor für die digitale Resilienz und Souveränität Deutschlands, der Bundesländer und der Kommunen. Sie ist zugleich eine wichtige Basis für die weitere Digitalisierung der öffentlichen Verwaltung. Die Strategie muss besonders die Rolle kommunaler Rechenzentren als elementarer Bestandteil der gesamtstaatlichen Vorsorge und ihren Beitrag zu einer nachhaltigen, sicheren und souveränen digitalen Infrastruktur berücksichtigen.

Wir bereiten aktuell gemeinsam mit dem Land BW den Bau eines energieeffizienten Rechenzentrums vor, um unsere Verantwortung für Nachhaltigkeit, Versorgungssicherheit und Innovation zu unterstreichen. Wir sind bereit, im Rahmen der Nationalen Rechenzentrumsstrategie ausgewählte Schwerpunktaufgaben zu übernehmen und diese in unsere Planung aufzunehmen.

Die öffentlich-rechtlichen Rechenzentren von Bund, Ländern und kommunalen IT-Dienstleistern sind gemeinschaftlich im Netzverbund für die digitale Souveränität auf allen Verwaltungsebenen verantwortlich und elementarer Bestandteil der gesamtstaatlichen Krisenvorsorge. Sie wirken im Verbund von Bund, Ländern und Kommunen eng zusammen. Sie dürfen vor diesem Hintergrund nicht in den gegenseitigen Wettbewerb untereinander gestellt werden.

Innerhalb Deutschlands muss eine Vernetzung der Rechenzentren von Bund, Ländern und kommunalen IT-Dienstleistern eine gegenseitige Absicherung bei physischen oder cyberbedingten Angriffen oder Ausfällen (z.B. bei Naturereignissen) garantieren. Staat und Verwaltung müssen zum Schutz der Demokratie jederzeit handlungsfähig sein und diese Rechenzentren verpflichtend nutzen. Das erfordert einen Nukleus an vollständig öffentlich-rechtlich getragenen und gesteuerten Rechenzentren, die zum Beispiel gerade im Falle einer Krise/einer Bedrohungslage orchestriert den Nationalen Sicherheitsrat unterstützen.

Die nationale Rechenzentrumsstrategie muss darüber hinaus in ein entsprechendes europäisches Format eingebettet werden. Deutschland kann seine nationale Souveränität nur gemeinsam mit anderen Ländern der Europäischen Union sicherstellen. Digitale Ökosysteme wie z.B. EuDI-Wallet, NOOTS/EU-OOTS erfordern eine Rechenzentrumstrategie, die EU-weit orchestriert wird.

Masterplan für eine abgestimmte Ausbauplanung: Für die Nationale Rechenzentrumsstrategie ist ein Masterplan erforderlich, bei dem frühzeitig Bedarfsanalysen vorgenommen und Roadmaps für einen gezielten Ausbau und eine ausgewogene Lastverteilung entwickelt werden. Dabei muss auch der steigende Kapazitäts- und Strombedarf durch KI-Technologien berücksichtigt werden. Hinzu kommt der Speicherbedarf für die digitale Langzeitarchivierung und damit verbundene weitere Schlüsseldienste.

Chancen:

Stärkung und Schutz der Demokratie: Die Kommunen sind bei 80% der Verwaltungsleistungen die ersten Anlaufstellen für die BürgerInnen. Ohne die Rechenzentren kommunaler IT-Dienstleister können diese nicht digital bereitgestellt werden. Die Komm.ONE ist als kommunale IT-Dienstleisterin und Betreiberin von Rechenzentren ein Schlüsselfaktor und Rückgrat für die digitale Souveränität, die Datensicherheit und die Modernisierung der öffentlichen Verwaltung in Baden-Württemberg.

Deutschlandarchitektur: Die nationale Rechenzentrumstrategie wird durch eine Deutschlandarchitektur mit gemeinsamen, interoperablen Standards, einer klaren Aufgabenverteilung und gegenseitiger Unterstützung in Krisen und Bedrohungslagen ein Garant für die Funktionsfähigkeit und Effizienz digitaler Leistungen von Bund, Ländern und Kommunen.

Dies schafft **Wirtschaftswachstum! Rechenzentren sind Wertschöpfungsmotoren.**

Funktionsfähige Kommunen stärken die Demokratie vor Ort, aber sie benötigen dafür leistungsstarke kommunale Rechenzentren! Die Bürgerinnen und Bürger wollen einen funktionierenden Staat und Demokratie „vor Ort“ erleben. Das sichert ihr Vertrauen in die Demokratie, in den Staat und in „ihre“ Verwaltung und fördert die Identifikation.

Herausforderungen:

Ein leistungsstarker Rechenzentrumsverbund erfordert einen Masterplan und erhebliche Investitionen. Cyber-Resilienz, ausfallsichere und skalier-bare Stromversorgung und Rechenzentren, cloudfähige Softwarelösungen, zentrale Portale, die aufgebaut werden müssen, sind nur einige Themen, die im Fokus stehen. Für die Umsetzung müssen – bei aller Themenkonkurrenz – Mittel aus den Sondervermögen für Bund und Länder/Kommunen priorisiert bereitgestellt werden. EU-weit sind auch Co-Finanzierungen/Förderungen der Europäischen Union notwendig.

Die Abhängigkeit Deutschlands und der EU in Hard- und Softwareangelegenheiten von außereuropäischen Firmen muss reduziert werden. Das schließt KI-getriebene Lösungen mit ein.

Gleichzeitig müssen europäische Kompetenzen aufgebaut werden. Souveränität erfordert eigene Steuerungsmöglichkeiten durch staatliche Institutionen und/oder EU-Institutionen sowie in kritischen Situationen durchsetzbare gesetzliche Einwirkungsmöglichkeiten auf Hersteller und Dienstleister.

2. Rahmenbedingungen für leistungsstarke (öffentlich-rechtliche) Rechenzentren in Deutschland und der EU 2030 ff

- inkl. der Förderung von Investition und Innovation

Hier werden die Leitfragen 1 und 3 behandelt:

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

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

Verlässlicher Rahmen und Staat als Ankerkunde: Leistungsstarke Rechenzentren benötigen einen klaren gesetzlichen Rahmen in Deutschland und in der EU sowie einheitliche Vorgaben zur Zertifizierung und zum Reporting. Die öffentliche Verwaltung auf allen Ebenen muss ihre digitalen Dienste bevorzugt über inländische Rechenzentren in öffentlich-rechtlicher Trägerschaft betreiben.

Vereinfachte Genehmigungsverfahren: Beschleunigte und vereinfachte Genehmigungsverfahren für Bau, Netzanbindung und Energieversorgung kommunaler Rechenzentren sind zwingend.

Kofinanzierung und Förderung von Schutz, Know-how und Innovation: Kommunale Rechenzentren sind kritische Infrastruktur. Ihre Resilienz und Sicherheit müssen gezielt gefördert werden. Eine gesicherte, langfristige Förderung und Kofinanzierung müssen insbesondere für Maßnahmen der Cybersicherheit und Krisenresilienz (inkl. Zertifizierungen), der ausfallsicheren und ökologisch ausgerichteten Stromversorgung sowie zum physischen Schutz der Infrastruktur und Gebäude gewährleistet sein.

Hinzu kommen Mittelbedarfe für zukunftsfähige Rechenzentrumstechnologien sowie für nachhaltige und energieeffiziente Bauweisen.

Neben IT-Fachkräften sind insbesondere Kompetenzen in den Bereichen Kälte-, Klima- und Elektrotechnik unverzichtbar. Notwendig sind gezielte Förderprogramme, duale Studiengänge und Kompetenzzentren für Energieeffizienz. Die Komm.ONE treibt ihrerseits bereits seit längerem gezielt die Zusammenarbeit mit Hochschulen, Kompetenzzentren und Forschungsclustern voran.

Vorrangiger Infrastrukturzugang: Öffentlich-rechtliche Rechenzentren müssen vorrangig Zugang zu leistungsfähigen und ausfallsicheren Stromanschlüssen

erhalten.

Zudem muss der Bezug günstiger, erneuerbarer Energie sowie die Einbindung in Wärmenetze – flankiert durch entsprechende Förderprogramme – gewährleistet sein.

Kooperation in der EU: Kommunale Rechenzentren, föderale Strukturen und Redundanzen müssen systematisch in europäische Cloud-Initiativen und – Strategien eingebunden werden, um kritische Dienste auch im Krisenfall abzusichern. Hierfür werden Standards, Prozesse und Schnittstellen für grenzüberschreitende Verwaltungs- und Krisenkooperationen benötigt.

3. Anforderungen (an den Staat D zur Sicherstellung von Resilienz und Souveränität/Autarkie

hier folgt die Antwort auf Leitfrage 4:

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

Kritische Infrastruktur: Kommunale Rechenzentren müssen Teil der nationalen Sicherheitsstrategie sein.

Cyber-Resilienz: Für die Deutschlandarchitektur sind einheitliche, verbindliche, praxisnahe Standards für IT-Sicherheit nach BSI-Vorgaben notwendig.

Interoperabilität: Einheitliche Vorgaben für Schnittstellen und Standards sichern im Regelbetrieb wie im Krisenfall den medienbruchfreien Datenaustausch zwischen Bund, Ländern und Kommunen – auch für Verschlusssachen.

(Inter)nationale Bedrohungslagen: Der Aufbau föderaler Redundanzen ist notwendig, um die Datenhoheit und Versorgungssicherheit zu gewährleisten.

Kooperation: Eine enge Einbindung in Melde- und Reaktionsketten mit BSI, CERT-Bund und Landes-CERTs wie auch über das BMDS in den nationalen Sicherheitsrat ist zwingend. Kommunale IT-Dienstleister müssen inhärenter Teil einer nationalen wie EU-weiten Sicherheitsarchitektur werden.

Abhängigkeiten vermeiden: Die Verringerung einseitiger Abhängigkeiten von Anbietern außerhalb der EU muss politisch flankiert werden.

Zentrale Rolle: Ohne kommunale Rechenzentren sind weder die deutsche noch die europäische Digital- und Datenstrategie autark umsetzbar.

Datensouveränität: Die Daten von Bürgern und Verwaltung müssen jederzeit sicher verarbeitet und gespeichert werden können und der Zugriff muss auch in Krisenzeiten gesichert sein. Die Portierbarkeit von Anwendungen und Daten muss durch geeignete Techniken (Container-Technologie, Verschlüsselung mit „Master-Key“) jederzeit möglich sein und rechtlich wie auch vertraglich abgesichert werden.

Europäische Integration: Nationale Rechenzentren müssen in eine EU-weite Rechenzentrumsstrategie eingebunden werden.

Datenethik: Es sind einfache, klare Leitlinien für faire, sichere und transparente Datennutzung im öffentlichen Sektor erforderlich (siehe Data Act, AI Act).

4. Ausblick: Einbettung der nationalen Rechenzentrumsstrategie in eine EU-Gesamtstrategie

(NOOTS/EU-OOTS, EU-DI, KI-Cluster, Innovation, Resilienz, Souveränität/Autarkie)

hier folgt die Antwort auf Frage 5:

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

Die nationale Rechenzentrumsstrategie und die diversen Cloudinitiativen müssen in europäische Cloudinitiativen und -strategien und KI-Cluster systematisch eingebunden werden. Zur Sicherstellung reibungsloser Standards, Prozesse und Schnittstellen für grenzüberschreitende Verwaltungs- und Krisenkooperation ist eine EU-weite Kooperation zwingend.

Krisenresilienz: Föderale Strukturen und Redundanzen müssen in europäische Strategien integriert werden, um kritische Dienste auch im Krisenfall EU-weit abzusichern.

Wettbewerbsfähigkeit: Der Aufbau eigener europäischer KI-Infrastrukturen ist zur Reduzierung von Abhängigkeiten von außereuropäischen Hyperscalern zwingend erforderlich.

5. Fazit (wesentliche Punkte auf einer Seite)

Souveränität: Die Nationale Rechenzentrumsstrategie ist ein notwendiger Garant für die Sicherstellung der digitalen Souveränität, Nachhaltigkeit und Resilienz von Bund, Ländern und Kommunen. Kommunale Rechenzentren sind dabei Schlüsselakteure. Sie sichern die Handlungsfähigkeit und das digitale Angebot ihrer überwiegend kommunalen Kunden, treiben die Modernisierung der Verwaltung voran und stabilisieren regionale Ökosysteme.

Förderung und Ko-Finanzierung: Öffentlich-rechtliche Rechenzentren erfordern eine langfristige, nachhaltige Förderung und Ko-Finanzierung von Bund, Ländern und EU für den sicheren Betrieb, die Schaffung von Know-how und Innovation.

Innovation und Wirtschaftswachstum: Öffentlich-rechtliche Rechenzentren sind Wertschäftungsmotoren und unterstützen auch insbesondere regionale Ökosysteme.

Deutschland- und EU-Architektur: Europaweite, digitale Ökosysteme wie zum Beispiel EuDI-Wallet oder NOOTS/EU-OOTS) erfordern eine Rechenzentrumstrategie, die auch EU-weit orchestriert wird. Die nationale Rechenzentrumsstrategie muss deshalb in ein entsprechendes europäisches Format eingebettet werden, denn Deutschland kann – wie alle anderen EU-Staaten auch – seine nationale Souveränität nur gemeinsam mit den Partnern der Europäischen Union sicherstellen.

Gemeinsame, interoperable Standards und die gegenseitige Unterstützung in einem nationalen wie auch EU-weiten Verbund der öffentlich-rechtlichen und ausgewählter privater Rechenzentren sichern in Krisenzeiten und Bedrohungslagen die Funktionsfähigkeit von Bund, Ländern und Kommunen wie auch der EU und ihrer Mitglieder.

Schutz und Stärkung der Demokratie: Die Bürgerinnen und Bürger und auch die Wirtschaft wollen einen funktionierenden Staat und Demokratie „vor Ort“ erleben. Die Nationale Rechenzentrumsstrategie ist das Rückgrat für die Modernisierung der öffentlichen Verwaltung insbesondere vor Ort in den Kommunen, die zu 80 % die erste Anlaufstelle für Verwaltungsleistungen der Bürgerinnen und Bürger sind. Leistungsstarke kommunale Rechenzentren

stärken die Demokratie vor Ort! Das sichert das Vertrauen der BürgerInnen in die Demokratie, in Staat und Verwaltung.
