

STELLUNGNAHME

zum Cloud and AI Development Act der Europäischen Kommission (CADA)

Berlin / Brüssel, 01.09.2026

EU Transparenz Register: 1420587986-32

Der Verband kommunaler Unternehmen e. V. (VKU) vertritt über 1.600 Stadtwerke und kommunalwirtschaftliche Unternehmen in den Bereichen Energie, Wasser/Abwasser, Abfallwirtschaft sowie Telekommunikation. Mit rund 319.000 Beschäftigten wurden 2023 Umsatzerlöse von über 213 Milliarden Euro erwirtschaftet und mehr als 19 Milliarden Euro investiert. Im Endkundensegment haben die VKU-Mitgliedsunternehmen signifikante Marktanteile in zentralen Ver- und Entsorgungsbereichen: Strom 66 Prozent, Gas 65 Prozent, Wärme 72 Prozent, Trinkwasser 88 Prozent, Abwasser 50 Prozent. Die kommunale Abfallwirtschaft hat seit 1990 rund 90 Prozent ihrer CO2-Emissionen eingespart – damit ist sie der Hidden Champion des Klimaschutzes. Immer mehr Mitgliedsunternehmen engagieren sich im Breitbandausbau und investieren pro Jahr über 1 Milliarde Euro. [Zahlen Daten Fakten 2025](#). Wir halten Deutschland am Laufen – denn Zukunft wird vor Ort gemacht: Unser Beitrag für heute und morgen: #Daseinsvorsorge.

Unsere Positionen: <https://www.vku.de/vku-positionen/>

Interessenvertretung:

Der VKU ist registrierter Interessenvertreter und wird im Lobbyregister des Bundes unter der Registernummer: R000098 geführt. Der VKU betreibt Interessenvertretung auf der Grundlage des „Verhaltenskodex für Interessenvertreterinnen und Interessenvertreter im Rahmen des Lobbyregistergesetzes“.

Verband kommunaler Unternehmen e.V. · Invalidenstraße 91 · 10115 Berlin

Fon +49 30 58580-0 · info@vku.de · www.vku.de

Der VKU ist mit einer Veröffentlichung seiner Stellungnahme (im Internet) einschließlich der personenbezogenen Daten einverstanden.

Bedeutung des Vorhabens für kommunale Unternehmen

Als dezentrale, lokale und resiliente Strukturen sind kommunale Unternehmen eine Voraussetzung sowie ein zentraler Bestandteil der europäischen technologischen Souveränität. Der Verband kommunaler Unternehmen (VKU) schließt sich der Einschätzung der Kommission an, dass die weitreichenden Abhängigkeiten von wenigen Anbietern aus Drittländern im Digitalbereich angesichts der heutigen sicherheits- und geopolitischen Lage sehr alarmierend sind. Insbesondere als **Betreiber kritischer Infrastrukturen (KRITIS)** steht Cybersicherheit für kommunale Unternehmen an oberster Stelle. In diesem Zusammenhang ist eine Vielzahl **sicherer und leistbarer Cloud-Dienste** von entscheidender Bedeutung. Wo bereits möglich, setzen kommunale Unternehmen auf europäische Lösungen – auch, um den hohen Sicherheitsstandards gerecht zu werden, die sie als KRITIS-Betreiber auf EU- und nationaler Ebene erfüllen müssen. Ausfälle und Abhängigkeiten haben unmittelbare Auswirkungen auf die Versorgungssicherheit und eine funktionierende Daseinsvorsorge vor Ort, die trotz stetig steigender Cybersicherheitsangriffe als selbstverständlich gilt.

Vor diesem Hintergrund betreiben **eine Vielzahl von kommunalen Unternehmen und IT-Dienstleister** eigene Rechenzentren, in denen **Daten aus KRITIS** gehostet werden. Rechenzentren kommunaler Unternehmen ermöglichen eine dezentrale Datenspeicherung und -verarbeitung vor Ort und genießen ein hohes Vertrauen der Bevölkerung.

Häufig ergänzen Rechenzentren andere Geschäftsfelder kommunaler Unternehmen im Telekommunikationsbereich, vor allem den Ausbau von Glasfasernetzen. **Mehr als 220 VKU-Mitgliedsunternehmen investieren pro Jahr über eine Milliarde Euro** in den Breitbandausbau. Glasfasernetze sind essenziell für den Betrieb moderner Rechenzentren. Nur sie gewährleisten einen stabilen und schnellen Transport sehr großer Datenmengen.

Mit **über 2.000 Rechenzentren** verfügt Deutschland derzeit über die höchste Anzahl in Europa. Aufgrund einer hohen Netzstabilität und weiterer Standortvorteile ist Deutschland in der Tat gut positioniert, diesen Erfolgskurs fortzusetzen. Auch in dieser Hinsicht sind kommunale Unternehmen eine Voraussetzung für einen zeitnahen und nachhaltigen Ausbau von Rechenzentren. Kommunale Unternehmen stellen die notwendige **Energie-, Wasser- und Netzinfrastruktur** für Rechenzentren bereit. Aufgrund ihrer starken lokalen Verankerung betrachten kommunale Unternehmen **Nachhaltigkeit** als einen zentralen Bestandteil ihres öffentlichen Auftrags gegenüber der Kommune vor Ort. Ressourceneffizienz steht dabei an erster Stelle. Die notwendige Infrastruktur für Rechenzentren sollte aus Sicht der Kommunalwirtschaft von Anfang an mitgedacht

werden – inklusive Stromnetzanbindung, Stromversorgung und Potenzialen zur Abwärmenutzung.

Positionen des VKU in Kürze

In diesem Sinne begrüßt der VKU ausdrücklich, dass die Kommission die Komplexität der technologischen Souveränität im vorgelegten Paket und im CADA adressiert. Kommunale Unternehmen sind ein wichtiger Baustein dieses Ziels. Demzufolge ist es wichtig, dass der CADA den Ausbau **kommunaler Rechenzentren** fördert. Vereinfachte Genehmigungsverfahren und eine frühzeitige, koordinierte Planung mit ausreichender Bereitstellung von Flächen- und Kapazitätskarten sind hierfür zentral. Vielmehr sollte die **notwendige Infrastruktur** von Anfang an mitgedacht werden. Kommunale Unternehmen bieten hier mit ihrer Vielzahl an Geschäftsfeldern – von Glasfaser über Netze bis hin zu Abwärme und Wasser – einen aktiven **Mehrwert**. Die Einschränkungen und Anforderungen dieser Ressourcen sollten im CADA in Bezug auf die Beschleunigungszonen für Rechenzentren und die strategischen Rechenzentrumsprojekte ausdrücklich anerkannt werden.

Im Hinblick auf den vorgeschlagenen neuen Rahmen für Cloud-Souveränität ist es ebenso wichtig, die praktischen Gegebenheiten vor Ort und in diesem Marktsegment anzuerkennen. Noch fehlt es an **ausreichenden Angeboten leistbarer europäischer souveräner Cloud-Anbieter** mit hohen Cybersicherheitsstandards, Interoperabilität und zielgenauen Datenschutzauflagen. Eine bloße Kategorisierung des bestehenden Cloud-Angebots anhand von Sicherheitsstufen ist nach Einschätzung des VKU nicht ausreichend. **Langfristig starke Infrastrukturen auf EU-Ebene müssen geschaffen werden, um dies zu gewährleisten.** Nur so können die ambitionierten Anforderungen des CADA erfüllt und die Ziele der Digitalen Dekade erreicht werden. Positiv ist, dass die Kommission betont, auch künftig mit vertrauenswürdigen internationalen Partnern zusammenarbeiten zu wollen. Sinnvoll sind zudem die vorgesehenen Finanzierungsinstrumente sowie angebotsseitige Maßnahmen im CADA und in weiteren Initiativen.

Problematisch ist in diesem Zusammenhang jedoch die Gefahr einer **systematischen Doppel- und Parallelregulierung** im Bereich *tech sovereignty*. Besonders bedenklich ist jede Verankerung im europäischen **Vergaberecht**. Zweckmäßiger ist eine ausschließlich sektorspezifische Regulierung. Insbesondere für kommunale Unternehmen und ihre Geschäftsfelder können so Planungs- und Rechtssicherheit gesteigert werden. Im weiteren Verfahren des CADA sollte dies berücksichtigt und ein Schwerpunkt auf praxistaugliche, interoperable Lösungen gesetzt werden.

Kernforderungen des VKU

- › Förderung des **Ausbaus kommunaler Rechenzentren** in Beschleunigungszonen durch vereinfachte Genehmigungsverfahren mit einer maximalen Dauer von zwölf Monaten, die grundsätzliche Anerkennung der Errichtung und des Betriebs kommunaler Rechenzentren als zulässig sowie die frühzeitige Bereitstellung von Raumplanungsdaten;
- › Berücksichtigung der **lokalen Infrastruktur vor Ort** (Stromnetze, Glasfaser, Abwärmeinfrastruktur, Wasserwirtschaft) beim Rechenzentrumsausbau verankern und die Zusammenarbeit zwischen Rechenzentren, Kommunen und Wärmeversorgern erleichtern;
- › Genauere Ausgestaltung der **Cloud-Vorgaben auf die aktuellen Marktrealitäten in Europa anpassen** und ausreichende, leistbare und sichere europäische Angebote durch eine Stärkung der Anbietervielfalt und von Multi-Vendor-Strategien sicherstellen;
- › **Benachteiligungen kommunaler Unternehmen als öffentliche Auftraggeber vermeiden** durch Anknüpfung an die Tätigkeiten des öffentlichen Sektors gemäß der NIS-2-Richtlinie oder durch eine Ausnahme im CADA für öffentliche Auftraggeber, die im Wettbewerb mit privaten Unternehmen stehen;
- › Vermeidung von **Doppel- und Parallelregulierung** durch einen klaren Schwerpunkt auf praxistaugliche Vorgaben, Interoperabilität sowie Planungs- und Rechtssicherheit für kommunale Unternehmen.

Positionen im Detail

I. Rechenzentren

Der VKU begrüßt grundsätzlich den Vorschlag der Europäischen Kommission zur Benennung strategischer Rechenzentrumsprojekte (*data centre strategic projects*) sowie zur Einrichtung von Beschleunigungszonen für Rechenzentren (*data centre acceleration zones*): sowohl aus Sicht kommunaler Unternehmen als eigene **Betreiber kommunaler Rechenzentren** als auch als **KRITIS-Betreiber** (Energie- und Wasserversorgung sowie Abwärmeinfrastruktur).

Ausbau kommunaler Rechenzentren fördern

Art. 10-14

Als Betreiber von Rechenzentren sollte die konkrete Ausgestaltung der Beschleunigungszonen und strategischen Rechenzentrumsprojekte einen **Local-First-Ansatz** unterstützen. Wie in Art. 14 festgelegt, unterstützen und stärken kommunale Rechenzentren unmittelbar „wesentliche Funktionen des öffentlichen Sektors.“ Die Errichtung und der Betrieb von Rechenzentren durch Kommunen und kommunale Unternehmen sind **verlässlich**, stärken die **Digitalisierung vor Ort** und leisten einen wichtigen Beitrag zur **digitalen Souveränität** Europas. Jedoch stoßen Rechenzentren häufig aufgrund ihres hohen Flächen-, Energie- und Wasserbedarfs auf geringe Akzeptanz bei der lokalen Bevölkerung. Kommunale Unternehmen genießen wiederum ein sehr **hohes Maß an Vertrauen**. Kommunale Rechenzentren können diesen Vorbehalten somit entgegenwirken. Lokale Rechenzentren können zudem **neue Marktsegmente für Kommunen, kleine und mittlere Unternehmen sowie die öffentliche Verwaltung** erschließen. Dabei bleiben die Daten vor Ort. Demzufolge stärken solche Geschäftsmodelle Vertrauen, Sicherheit und Souveränität.

Als wichtige Voraussetzung für die Beschleunigung des Ausbaus kommunaler Rechenzentren begrüßt der VKU ausdrücklich das Vorhaben der Kommission, **Genehmigungsverfahren** zu beschleunigen und zu vereinfachen. Auch die in Art. 13(5) vorgesehene Festlegung einer maximalen Dauer von **zwölf Monaten** für Genehmigungsverfahren entspricht den Forderungen des VKU. Wichtig ist, dass auch in anderen Bereichen mit Genehmigungsverfahren dies angestrebt wird, um Bottlenecks zu vermeiden. Insbesondere bei anlagenspezifischen Genehmigungen muss nationales Recht weiterhin beachtet werden. Aus Sicht der Kommunalwirtschaft wäre ein *One-Stop-Shop* auf nationaler Ebene sowie eine solche **verbindliche** Genehmigungsfrist notwendig, um Investitionen im internationalen Wettbewerb besser abzusichern. Dieser sollte jedoch nicht zu zusätzlichem bürokratischem Mehraufwand für die betroffenen Kommunen und kommunalen Unternehmen führen. Für die **Erteilung der aggregierten Basisgenehmigung** gemäß Art. 13 sollte der Mitgliedsstaat die Zuständigkeiten in den Kommunen berücksichtigen und die lokalen Behörden rechtzeitig informieren.

Im Rahmen weiterer Regulierungsvorhaben, einschließlich Maßnahmen zur Beschleunigung von Umweltprüfungen, sollte des Weiteren die **Errichtung und der Betrieb von Rechenzentren in ausgewiesenen Beschleunigungszonen durch Kommunen und kommunale Unternehmen grundsätzlich als zulässig** anerkannt werden, um Rechts- und Investitionssicherheit zu schaffen. Zudem kann der Vorschlag der Kommission gemäß Art. 10(3), wonach die Mitgliedstaaten sicherstellen sollen, dass alle relevanten **Raumplanungsdaten** den Rechenzentrumsbetreibern zur Verfügung stehen, zu mehr Planungssicherheit führen. Für kommunale Rechenzentren ist insbesondere eine frühzeitige Bereitstellung von **Flächen- und Kapazitätskarten** (Strom und Glasfaser) wichtig.

In dieser Hinsicht könnte auch eine **zentrale Liste von geeigneten Standorten** einen Mehrwert für Investoren sowie kommunale Unternehmen bieten. Als Basis für die darauffolgenden Kriterien können **entsprechende Normvorgaben** (u. a. BSI, TSI, EN 50600) für die Auswahl der am besten geeigneten Standorte definiert werden. Die in Art. 12 vorgeschlagenen zentralen Anlaufstellen (*single information points*) könnten auf diese Weise im weiteren Verfahren ergänzt werden. Es gilt zu untermauern, dass in der Netzwirtschaft bei umfassenden Leistungsbedarfen komplexe Netzberechnungen mit zahlreichen Varianten (unterschiedliche Netznutzer, Stützjahre etc.) erforderlich sind. Zudem ist dabei klarzustellen, dass zentrale Informationsstellen Verfahren koordinieren und Mehrfachabfragen vermeiden können, jedoch nicht die gesetzlichen und technischen Zuständigkeiten der Strom-, Wärme-, Wasser- und Kommunikationsnetzbetreiber ersetzen dürfen. Verbindliche Aussagen zu verfügbaren Netzkapazitäten, technischen Anschlussbedingungen sowie zur Realisierbarkeit eines Anschlusses sollten den jeweils zuständigen Infrastrukturbetreibern vorbehalten werden.

Rechenzentrumsausbau und lokale Infrastruktur gemeinsam denken

Art. 10-14

Um Infrastrukturengpässe zu adressieren, sollten Rechenzentren als integraler Bestandteil der Energie- und Wärmeinfrastruktur betrachtet werden. In Deutschland mangelt es an **geeigneten Flächen** für Rechenzentren, insbesondere aufgrund begrenzter Netzanschlusskapazitäten, die mit der fortschreitenden Elektrifizierung der Wirtschaft, dem Ausbau erneuerbarer Energien und der Elektromobilität sowie den Anschluss neuer Lasten und Speicher noch knapper werden.

Die für den Betrieb von Rechenzentren erforderliche **Infrastruktur** sollte **von Anfang an mitberücksichtigt** werden, einschließlich **Glasfaseranschluss, Netzanschluss (Verteilnetzbetreiber), Stromversorgung und Abwärmenutzungspotenziale**. Kommunale Unternehmen haben hier ganz überwiegend einen Wissensvorsprung im Überblick über multiple (städtische) Entwicklungen. Durch die Wärmeplanung haben kommunale Unternehmen beispielsweise einen **Überblick** über diese Infrastruktur sowie

die Planung der Energiegewinnung. Um Nachhaltigkeit und Ressourceneffizienz durch die Nutzung von Abwärme zu fördern, sind unterstützende Maßnahmen wie z. B. Risikoabsicherungen erforderlich, damit dieses Potenzial in Zukunft besser ausgeschöpft werden kann. Dies gilt ebenso für alternative regionale Lösungen, wie z. B. die Nutzung der Abwärme als Heizenergie für Quartiere oder als Prozesswärme in benachbarten Industrie- und Gewerbegebieten. Nur in Zusammenarbeit mit den Kommunen, Städten und Ländern können Erschließungsthemen vorbereitet und definiert werden.

Damit Beschleunigungszonen tatsächlich zu einer besseren Steuerung des Rechenzentrumsausbaus beitragen, müssen die **relevanten Infrastrukturakteure** frühzeitig und fortlaufend **eingebunden** werden. Neben den zuständigen nationalen, regionalen und kommunalen Stellen betrifft dies insbesondere Stromnetzbetreiber, Betreiber erneuerbarer Erzeugungsanlagen, Wasserunternehmen, Wärmenetzbetreiber und Betreiber von Kommunikationsnetzen. Nur so kann sichergestellt werden, dass neue Rechenzentren dort entstehen, wo sie in bestehende oder geplante Energie-, Wärme-, Wasser- und Kommunikationsinfrastrukturen integriert und möglichst systemdienlich betrieben werden können.

Ergänzend sollte der CADA berücksichtigen, dass die **Ausweisung geeigneter Beschleunigungszonen allein noch keine kurzfristige Realisierbarkeit sicherstellt**. Gerade bei größeren Rechenzentrumsprojekten müssen Strom-, Wärme-, Wasser- und Kommunikationsinfrastrukturen häufig erst geplant, verstärkt oder neu errichtet werden. Soweit hierfür vorausschauende Netz- und Infrastrukturinvestitionen erforderlich sind, braucht es rechtssichere Vorgaben zur Finanzierung, zur regulatorischen Anerkennung entstehender Netzausbaukosten sowie zum Umgang mit Auslastungsrisiken.

Die vorgeschlagenen Beschleunigungszonen haben aus Sicht der Kommunalwirtschaft insbesondere dort einen Mehrwert, wo die Nutzung von bspw. erneuerbaren Energien oder Abwärme **bereits vorgesehen bzw. geplant** ist. Das bringt die Erfahrungen aus der Praxis von kommunalen Unternehmen mit den ambitionierten Zielen der Kommission in Einklang.

In diesem Sinne begrüßt der VKU, dass die Mitgliedstaaten gemäß Art. 10(1) des Vorschlags u. a. (b) die bestehende und künftige **Netzkapazität** sowie die Möglichkeiten und Voraussetzungen für Energiespeicherung und die Erzeugung sauberer Energie vor Ort; (d) das Potenzial einer Zone zur Unterstützung der **Abschaltung bestehender Kupfernetze**; sowie (e) die vorhandenen und künftigen Möglichkeiten zur Nutzung von **Abwärme** aus Rechenzentren bei der Festlegung einer Beschleunigungszone berücksichtigen sollen. Ebenso positiv ist, dass die Mitgliedstaaten gemäß Art. 10(2) die **Energiebedarfe** und die **Treibhausgasauswirkungen** von Rechenzentren analysieren

sollen, einschließlich der Ermittlung der erforderlichen **Kapazitäten der Energieinfrastruktur**.

Es sollte jedoch weiter präzisiert werden, dass nicht lediglich ein Wärmeversorger vorhanden sein soll, sondern ein Wärmeversorger, der die **Abwärme aus Rechenzentren nutzen kann und will**. Darüber hinaus fehlt eine ausdrückliche Berücksichtigung der **Wasserressourcen** bzw. die Vorgabe, dass **Grundwasserressourcen** nicht von den genannten Rechenzentren beeinträchtigt werden dürfen (über die Erwähnung der betroffenen Gewässer gemäß der Wasserrahmenrichtlinie in den Raumordnungs- und Bebauungsplänen in Art. 10(3) des CADA hinaus). Mit Blick auf den im CADA angekündigten künftigen Gesetzesvorschlag **Verordnung (EU) 2026/XXX [zur Beschleunigung von Umweltprüfungen]** sollte diese zudem einen Verweis auf die bestehenden Vorgaben der Energieeffizienzrichtlinie (*Energy Efficiency Directive*; EED) einschließlich der damit verbundenen delegierten Rechtsakte herstellen: insbesondere falls Nachhaltigkeits- und Effizienzvorgaben, etwa zu Energieeffizienz und Abwärmeauskopplung, vorgesehen sind. Es gilt, Doppelregulierungen zu vermeiden.

Problematisch bleibt vielmehr, dass die **Infrastruktur vor Ort oftmals fehlt**, um dem Ziel der Kommission, die Rechenzentrumskapazitäten Europas bis 2030 zu verdreifachen, zu verwirklichen. Schon heute verschärft sich mit der fortschreitenden Elektrifizierung der Wirtschaft, dem Ausbau erneuerbarer Energien, der zunehmenden E-Mobilität und dem Anschluss neuer Lasten und Speicher der Wettbewerb um Netzanschlusskapazitäten. Um dies zu erreichen, empfiehlt der VKU aus Sicht der **relevanten Infrastrukturen** die Vorgaben für Beschleunigungszonen bzw. strategische Projekte wie folgt zu ergänzen:

Netzwirtschaft

- **Verteilnetzbetreiber** sollten verpflichtend frühzeitig in jegliche Planung von Rechenzentren **eingebunden** werden. Darüber hinaus sollten **netzdienliche Elemente (Systemdienlichkeit)** in Rechenzentren verpflichtend integriert werden (Lastmanagement, Flexibilität, Speicher, Eigenversorgung, Abwärmenutzung). Im CADA fehlen diese konkreten **operativen Vorgaben** sowie **verbindliche technische Anforderungen** mit Blick auf die genaue Ausgestaltung der Beschleunigungszonen und strategischen Projekte.
- Rechenzentren sind flexible Großverbraucher von Energie. Schon heute führen einzelne Großprojekte zu sehr hohen Anschluss- und Ausbaukosten in Verteil- sowie Übertragungsnetzen. Es fehlt jedoch an **Mechanismen für eine verursachungsgerechte Finanzierung** des für die Ziele des CADA erforderlichen Netzausbaus. Zusätzliche **Belastungen für allgemeine Netzentgelte und andere Netznutzer** sollten vermieden werden.
- Die **Ausweisung einer Beschleunigungszone** oder die **Einstufung als strategisches Rechenzentrumsprojekt** darf **keinen automatischen**

Netzanschlussanspruch und keinen Vorrang gegenüber anderen Anschlussbegehren begründen. Entscheidungen über Netzanschlüsse und die Zuteilung knapper Anschlusskapazitäten sollten weiterhin bei den zuständigen Netzbetreibern verbleiben, die diese auf Grundlage der geltenden energiewirtschaftsrechtlichen Vorgaben und einer technischen Einzelfallprüfung treffen. Sektorale Sonderregelungen im CADA dürfen bestehende nationale Netzanschlusssystematiken nicht überlagern und keine zusätzlichen Rechtsunsicherheiten schaffen.

- Durch Lastverschiebungen und *demand response* können Rechenzentren aber gleichzeitig das Energiesystem stabilisieren. Dafür bedarf es einer durchgehenden Koordination zwischen Netzentwicklung und -planung, Flächenentwicklung, Investitionsplanung der Verteilnetzbetreiber und den potenziellen Nutzern neuer Rechenzentren: bereits in der Planungsphase. **Der Bau neuer Rechenzentren sollte nur bei Bedarf entlang bestehender Leitungen möglich sein.** Keinesfalls sollte eine Genehmigung vor einer entsprechenden Netzverfügbarkeit bzw. einer belastbaren Netzkapazitätsprüfung stattfinden können.
- Obwohl die Kommission darauf hinweist, dass die Mitgliedstaaten bei der Ausweisung von Beschleunigungszonen die Erzeugung sauberer Energie berücksichtigen sollten, sollten **Standortanreize für Rechenzentren in der Nähe erneuerbarer Erzeugungskapazitäten** stärker hervorgehoben und priorisiert werden.
- Neben der Berücksichtigung von Netzkapazitäten, Energiespeichern vor Ort und der Erzeugung sauberer Energie sollten die Mitgliedstaaten im Rahmen der Ausweisung von Beschleunigungszonen für Rechenzentren auch **Vorrangflächen in der Nähe von Umspannwerken und Wärmesenken** vorsehen. Auch dies sollte Teil einer **frühzeitigen, integrierten Standortplanung** sein. Solche Standorte bieten Vorteile für die Effizienz und die regionale Wertschöpfung von Rechenzentren.
- Die im Rahmen von Art. 13 vorgeschlagenen Maßnahmen zur Vereinfachung **administrativer und genehmigungsrechtlicher Verfahren** sind grundsätzlich begrüßenswert. Aus Sicht der Netzwirtschaft dürfen verkürzte Umweltverträglichkeitsprüfungen jedoch nicht zu erhöhter **Rechtsunsicherheit** führen. Diese könnten andernfalls bei gerichtlichen Auseinandersetzungen leichter angegriffen werden. Obgleich Genehmigungen vereinfacht werden sollen, möchte der VKU unterstreichen, dass eine **realistische Umsetzungsfrist** mit Blick auf den Netzanschluss zentral bleibt. Klare Kriterien und eine **frühzeitige Beteiligung der Netzbetreiber und Kommunen sind mit Blick auf beschleunigte Verfahren** unverzichtbar.

Abwärmenutzung

- Als kostengünstige und skalierbare Quelle für die Dekarbonisierung städtischer Wärmenetzen (Wärmekopplung) müssen Rechenzentren auch **frühzeitig und aktiv in die Wärmeinfrastrukturplanung und -entwicklung integriert** werden. Die Bereitstellung einer Infrastruktur zur etwaigen Abwärmeeinspeisung bedarf z. B. auf Seiten der Wärmenetzbetreiber je nach Situation mehrjähriger Planungs- und Realisierungszeiträume. Es gilt nach Möglichkeit, den Ausbau von Rechenzentren eng mit den Netzausbauplänen sowie den **kommunalen Wärmeplänen** zu verzahnen, um wirtschaftliche Potenziale der Abwärmenutzung frühzeitig zu erschließen. Planungen zur Nutzung von Wärme – insbesondere auch von Abwärme aus Rechenzentren – werden vielerorts bereits umgesetzt.
- In der Planung eines Rechenzentrums sollten **Netzanschlusspunkte für Wärmepumpen** bereitgestellt und **ausreichend Platz auf der Fläche** vorgesehen werden. Wärmepumpen sind nötig, um die Abwärmetemperatur anzuheben, und erfordern ebenfalls hohe Strommengen.

Wasserwirtschaft

- Obgleich eine Beschleunigung von Umweltprüfungen grundsätzlich sinnvoll ist, sollte dies auch **keineswegs zu einer Vernachlässigung von wasserbezogenen Belangen** führen. In der Praxis setzen Rechenzentrumsprojekte Wasserressourcen zunehmend unter Druck (u. a. für die Kühlung von Rechenzentren). Auch die Frage, ob der zusätzliche Wasserverbrauch von Rechenzentren in der Kanalisierung und in Kläranlagen vor Ort aufgenommen werden kann, muss in der Planung bzw. Genehmigung von Rechenzentren mitgedacht werden.

Schutz kritischer Infrastrukturen

- Darüber hinaus müssen Standort-, Anschluss-, Last- und Betriebsdaten, die im Rahmen von Beschleunigungszonen, strategischen Projekten oder Monitoringprozessen erhoben werden, strikt nach dem **need-to-know-Prinzip** geschützt werden. Veröffentlichungen und Weitergaben dürfen nur so aggregiert erfolgen, dass keine Rückschlüsse auf einzelne kritische Anlagen, Netzkapazitäten, Betriebsweisen oder Verwundbarkeiten kommunaler KRITIS-Betreiber möglich sind. Für Erhebung, Speicherung und Weitergabe sind klare Vorgaben zu Zweckbindung, Zugriffsrechten, Verschlüsselung, Protokollierung und Löschung erforderlich.

II. Clouds

Sicherheitsstufen praxisnah ausgestalten

Die von der Kommission vorgeschlagenen vier Sicherheitsstufen (*Union assurance levels*) zur Einstufung von Cloud-Diensten sind nach Einschätzung des VKU grundsätzlich gut geeignet, den aktuellen Cloud-Markt zu klassifizieren und abzubilden.

Der Ansatz der Kommission, öffentliche Stellen die Wahl eines Anbieters entsprechend den erforderlichen Sicherheitsanforderungen zu ermöglichen, folgt prinzipiell einem **fundierte und risikobasierte** Ansatz. Es ist zudem sinnvoll, dass die **Beweis- und Nachweispflichten** des CADA bei den Cloud-Anbietern selbst liegen. Dies hilft kommunalen Unternehmen als Anwendern etwaiger Vorgaben. Ein weiteres positives Signal ist das Bestreben der Kommission, künftig weiterhin mit vertrauenswürdigen **internationalen Partnern** zusammenzuarbeiten und diese nicht unbegründet von höheren Sicherheitsstufen auszuschließen. Der aktuelle Markt ist nicht bereit, sich gegenüber nicht-europäischen Akteuren abzuschotten. Das sollte unbedingt vermieden werden.

Schwierigkeiten entstehen nämlich dann, wenn **keine oder nur sehr wenige Anbieter** mit hohen Sicherheitsanforderungen verfügbar sind. Nach Einschätzung des VKU erfüllen **nur sehr wenige Anbieter Sicherheitsstufe 3** – und sehr wahrscheinlich keine US-amerikanischen – während für **Sicherheitsstufe 4** nach derzeitiger Einschätzung des VKU **noch gar keine Anbieter** auf dem Markt verfügbar sind.

Zugleich sollte klargestellt werden, dass eine größere Anbieter- und Architekturvielfalt zwar grundsätzlich sinnvoll ist, **Multi-Cloud- oder Multi-Vendor-Strategien** jedoch **kein Selbstzweck** sein dürfen. Sie können zur Stärkung von Resilienz und Anbietervielfalt beitragen, sollten jedoch nicht faktisch für jeden Anwendungsfall verpflichtend werden. Je nach Schutzbedarf, technischer Systemarchitektur, Betriebsstabilität, Performanceanforderungen und Kosten kann auch ein *Single-Source*-Ansatz sachgerecht und angemessen sein. Die Wahl der geeigneten Beschaffungs- und Betriebsstrategie muss Entscheidung über Dual-, Multi- oder Single-Sourcing sollte daher risikobasiert und praxistauglich beim jeweiligen Betreiber verbleiben.

Benachteiligung kommunaler Unternehmen vermeiden

Art. 29-31

Art. 30 sieht vor, dass lediglich öffentliche Auftraggeber sowie Einrichtungen der Union zur Beschaffung bestimmter Cloud-Computing-Dienste verpflichtet werden sollen. Diese Vorgabe ist im Grundsatz **nicht zweckmäßig**. Ob ein entsprechender Cloud-Computing-Dienst zu beschaffen ist, sollte sich primär nach dem **Betätigungsfeld der betreffenden Stelle** richten. Soweit es um öffentliche Auftraggeber geht, die nicht hoheitlich oder

aufgrund einer öffentlich-rechtlichen Ermächtigungsgrundlage handeln, ist das Anknüpfen an den Begriff des öffentlichen Auftraggebers nicht nachvollziehbar.

Bleibt es bei dem Vorschlag, so würden öffentliche Unternehmen aus den Bereichen Versorgung, Entsorgung oder Verkehr verpflichtet, weil sie unter den Begriff des öffentlichen Auftraggebers fallen. **Entsprechende private Unternehmen mit vergleichbarem Betätigungsfeld würden dagegen nicht verpflichtet** (bzw. nur im Ausnahmefall in den Sektoren mit hoher Kritikalität der NIS-2-Richtlinie). Dabei stehen kommunale Unternehmen und privatwirtschaftliche Unternehmen häufig in einem **direkten Wettbewerbsverhältnis**, sodass die zusätzlichen Anforderungen für die kommunalen Unternehmen einen massiven Wettbewerbsnachteil bedeuten würden. Ein sachlicher Grund für diese Ungleichbehandlung zugunsten solcher Unternehmen, die nicht unter den Begriff des öffentlichen Auftraggebers fallen, ist aber nicht erkennbar.

Vor diesem Hintergrund spricht sich der VKU im weiteren Verfahren für folgende Möglichkeiten aus:

- die Verpflichtung gemäß Art. 30 an **Tätigkeiten des öffentlichen Sektors gemäß Anhang I oder II der NIS-2-Richtlinie** anknüpfen (ohne die Eigenschaft als öffentlicher Auftraggeber vorauszusetzen);
- eine **Ausnahme gemäß Art. 30(4) für öffentliche Auftraggeber**, die im Wettbewerb mit privaten Unternehmen tätig sind (bzw. eine Optimierung nach Art. 31).

Sollten beide vorgenannten Optionen im weiteren Verfahren nicht aufgegriffen werden, sollte jedenfalls als Minimalforderung die Ausnahme nach Art. 30(4) praxistauglicher ausgestaltet werden. Insbesondere sollte konkretisiert werden, ab wann Kosten als unverhältnismäßig gelten. Aus Sicht der Kommunalwirtschaft sollten bereits deutliche **Kostenunterschiede**, etwa **ab 5 bis 10 Prozent**, als relevantes Indiz für Unverhältnismäßigkeit anerkannt werden können.

Eine Verpflichtung ausschließlich der öffentlichen Auftraggeber würde zudem keinesfalls dem **tatsächlichen Risiko** im Hinblick auf die Abhängigkeiten von Cloud-Diensten entsprechen. So sind in Deutschland insbesondere in der Energiewirtschaft die größten Unternehmen privatwirtschaftlich organisiert: mit sehr hohen Umsätzen und einer großen Kundenbasis. Aus Sicht des VKU ist es aus Sicherheitsgründen nicht nachvollziehbar, diese Unternehmen nicht von den Cloud-Dienst-Anforderungen zu umfassen, während ein kleines Stadtwerk mit einem Bruchteil des Umsatzes und des Kundenstamms vollständig der Regulierung unterworfen werden soll.

Des Weiteren sollten **Definitionen oder jedenfalls Erläuterungen** zu „**public sector activities**“ (Aktivitäten im öffentlichen Sektor) sowie zu „**public order**“ (öffentliche

Ordnung; worauf sich Art. 29(1)(a) des Kommissionsvorschlags bezieht) ergänzt werden. In Bezug auf diesen Begriff ist unklar, ob dieser als Einschränkung in Bezug auf die Sektoren in Anhang I bzw. II der NIS-2-Richtlinie genutzt wird, oder ob alle Aktivitäten in den dort genannten Sektoren automatisch der Aufrechterhaltung der öffentlichen Ordnung dienen. Ferner bleibt unklar, ob sich die öffentliche Ordnung auch auf die im Folgenden aufgezählten Begriffe der nationalen Sicherheit, inneren Sicherheit, Verteidigung etc. bezieht und einschränkt oder nicht. Vielmehr muss vermieden werden, dass ein Unternehmen, das eine Tätigkeit mit *public order*-Relevanz ausführt, zwingend als Sicherheitsstufe 4 eingestuft wird.

Grundsätzlich muss dringend klargestellt werden, welche Unternehmen unter diese Regelungen fallen sollen. Insbesondere muss klargestellt werden, ob auch **kommunale Unternehmen in privater Rechtsform** unter diese Regelungen fallen, wenn sie in den Sektoren der NIS-2-Richtlinie tätig sind.

Anwendungsbereich an Größenschwellen der NIS-2-Richtlinie anpassen

Art. 29-30

Um Cloud-Souveränität verhältnismäßig zu regulieren, muss sichergestellt werden, dass nicht unabhängig von der Größe sämtliche Unternehmen, die in den Sektoren der NIS-2-Richtlinie tätig sind, mindestens Level 2 des Sicherheitsniveaus erreichen müssen (siehe Art. 29(1)(b) und Art. 30(3) des Kommissionsvorschlags). Die NIS-2-Richtlinie hat aus guten Gründen selbst Größenschwellen für die Anwendbarkeit definiert. Als Minimalforderung muss mindestens auf diese Größenschwellen Bezug genommen werden und alle **Unternehmen unterhalb der Größenschwellen der NIS-2-Richtlinie auch nicht den Anforderungen des CADA unterworfen** werden.

Cloud-Sicherheitsstufen auf Anlagensteuerung beschränken

Art. 29

Da die Risikobewertung, welche Cloud-Anwendungen welche Stufe erfüllen müssen, den Mitgliedstaaten überlassen bleibt, muss bei der Umsetzung etwaiger Vorgaben sichergestellt werden, dass die **Anforderungen an kommunale Unternehmen im Verhältnis zur jeweiligen Cloud-Nutzung sinnvoll und realistisch** sind. Derzeit ist es unklar, ob sich die Pflicht zur Einhaltung der Sicherheitsstufen auf alle von den Unternehmen genutzten Cloud-Diensten beziehen (**eine unternehmensbezogene Betrachtung**) oder nur auf solche Cloud-Dienste, die für die Erbringung der Dienstleistung nach den Sektoren der NIS-2-Richtlinie unmittelbar relevant sind (**eine anlagenbezogene Betrachtung**). Fragwürdig ist, ob bspw. ein Unternehmen der Energiewirtschaft das Sicherheitslevel für alle Cloud-Dienste erfüllen (u. a. auch reine Office-IT oder interne Online-Kommunikation bspw. M365, Teams, SharePoint) oder nur für solche Cloud-Dienste, die unmittelbar der Anlagensteuerung dienen (z. B. OT-Systeme zur Steuerung von Energieanlagen). Des Weiteren lässt die Definition von Cloud-Diensten offen, ob

Public-Cloud-Angebote oder auch intern betriebene Private-Cloud-Umgebungen von den Vorgaben des CADA erfasst wären. Unklar ist zudem, wie unterstützende IT-Basisdienste zu bewerten sind. Idealerweise sollten diese differenziert bewertet werden, um Parallelstrukturen zu vermeiden. Der VKU fordert, dass sich die Pflichten des CADA **nur auf die unmittelbar für die Anlagensteuerung erheblichen Cloud-Dienste beziehen**.

Pauschale Regulierung von Mehrspartenunternehmen vermeiden

Des Weiteren muss ein sinnvoller Umgang mit **Unternehmen, die in mehreren Sektoren tätig sind (Mehrsparatenunternehmen)** gefunden werden. In der Mitgliedschaft des VKU ist dies eher der Standard als die Ausnahme. Nach der jetzigen Konzeption des Kommissionsvorschlags könnte ein Unternehmen komplett den Anforderungen des CADA unterworfen werden, auch wenn **nur ein minimaler Anteil der Tätigkeit in einem Sektor der NIS-2-Richtlinie** vorgenommen wird. Hierzu könnte eine **realistische Schwelle** eingeführt werden.

Ausreichend Zeit für Umsetzung schaffen

Art. 29(6)

Die vorgeschlagene Migrationsphase von höchstens zwölf Monaten ist nach Einschätzung des VKU unrealistisch. Allein durch die häufig notwendige **öffentliche Vergabe** wird diese Frist nicht gehalten werden können. Zudem ist die Migration von einem Cloud-System zu einem anderen Cloud-System technisch äußerst aufwendig: von der Neuimplementierung bestehender Integrationen, Betriebsprozesse und Automatisierungen bis hin zu neuen Sicherheits- und Berechtigungskonzepten, Zertifizierungen, Audits und Compliance-Nachweise. Statt einer starren Frist braucht es daher angemessene und risikoorientierte Migrationspläne, insbesondere für komplexe, hochintegrierte oder betriebskritische Systeme. Die **Übergangsfrist sollte auf Basis einer individuellen Bewertung des jeweiligen Systems festgelegt** werden können, **jedoch mindestens zwei Jahre betragen**, um Betriebsrisiken zu minimieren und die Kontinuität kritischer Geschäfts- und Versorgungsprozesse sicherzustellen.

Auch für den Fall, dass sich Anerkennung, Zertifizierung oder Sicherheitsstufe eines Cloud-Dienstes **nachträglich ändern**, braucht es klare und praxistaugliche Vorgaben. Daraus folgende Anpassungs- oder Migrationspflichten sollten erst nach einer verbindlichen Information der betroffenen Kunden, einer risikobasierten Bewertung der konkreten Nutzung sowie angemessenen Übergangsfristen greifen. Andernfalls drohen vermeidbare Betriebsrisiken und unverhältnismäßige Kosten.

Mehrkosten im Blick behalten

Umso wichtiger ist es, dass etwaige Einschränkungen bei der Auswahl von Cloud-Anbietern **risikobasiert, verhältnismäßig und sicherheitsbegründet** erfolgen. Eine sehr eingeschränkte Anbieterauswahl und jeder regulatorisch bedingte Wechsel sind mit

erheblichen Mehrkosten und hohen Migrationskosten verbunden. Dieses Kapital wird an anderen Stellen dringend benötigt – auch für die Energiewende. Jegliche hohen Kosten für sichere und europäische Cloud-Anbieter würden sich bei öffentlichen Unternehmen an anderer Stelle verlegen. Bei Energieversorgungsunternehmen bzw. Netzbetreibern würde sich dies in steigenden Netzentgelten widerspiegeln (höhere Stromkosten): mit gravierenden Auswirkungen auf Europas Wettbewerbsfähigkeit und die Bürgerinnen und Bürger vor Ort.

Europäische Cloud-Anbieter fördern

Aus Sicht der Kommunalwirtschaft kann eine bloße Klassifizierung des Cloud-Marktes seitens der Kommission das Angebot von sicheren Clouds nicht ausreichend ankurbeln. Derzeit sind europäische Anbieter keine gleichwertige Alternative für lokale Hyperscaler-Plattformen, KI-Dienste und hochintegrierte Plattformökosysteme aus Drittstaaten.

Dementsprechend sollten jegliche Einschränkungen der Anbieterauswahl mit einer **langfristigen (Digital-)Industriepolitik** in Europa einhergehen, um eine ausreichende **Anbietervielfalt sicherer europäischer Cloud-Anbieter** sicherzustellen und **überhöhte Preise** und einen **single point of failure** zu vermeiden. Aus Sicht der Kommunalwirtschaft leisten hierzu **Förderprogramme für Cloud-Anbieter** einen wesentlichen Beitrag. Die in der **Open-Source-Strategie** hervorgehobenen horizontalen Rahmenbedingungen, weitere Forschungs- und Innovationsprogramme sowie europäische Beteiligungsfonds sind in dieser Hinsicht ein **positives Signal**. Nun müssen auf Worte **rasch konkrete Maßnahmen** folgen, um ein bezahlbares und vielfältiges Angebot sicherzustellen.

Wichtig ist auch, dass *EU-Added-Value*- und KMU-Kriterien die Anforderungen an technische Qualität, Sicherheit, Verfügbarkeit, Wirtschaftlichkeit und Leistungsfähigkeit der Gesamtarchitektur nicht überlagern. Insbesondere darf das Ziel einer stärkeren Beteiligung innovativer KMU (Art. 33(4)) nicht dazu führen, dass technisch zusammenhängende Cloud-Leistungen künstlich aufgespalten oder *Multi-Provider*-Architekturen allein zur Erfüllung von Zielwerten erzwungen werden. Maßgeblich bleiben muss eine wirtschaftlich und technisch sinnvolle Gesamtarchitektur.

III. Bürokratieabbau

Doppelregulierung sowie Rechts- und Planungsunsicherheiten vermeiden

Das Konzept der technologischen Souveränität ist in vielen der jüngsten Vorschläge der Europäischen Kommission fest verankert und zieht sich wie ein roter Faden durch die Gesetzgebung. Dies ist grundsätzlich zu begrüßen. Insbesondere angesichts der angespannten geopolitischen und sicherheitspolitischen Lage ist es sinnvoll, dass die Kommission die bestehenden Abhängigkeiten von wenigen Anbietern aus Drittländern verringern möchte. Ein souveränes Europa ist ein sicheres Europa. Kommunale Unternehmen – als lokal verankerte und dezentrale KRITIS-Betreiber – sind hierfür ein Schlüsselfaktor.

Schwierig ist es allerdings, dass gerade kommunale Unternehmen von einer Vielzahl paralleler Gesetze – die oftmals den **gleichen Themenbereich** regeln – auf EU- und nationaler Ebene überfordert werden. Der Vorschlag der Kommission zur Überarbeitung des *Cybersecurity Acts* regelt nicht-technische Risiken in IKT-Lieferketten; der *Cyber Resilience Act* wiederum IT-Produkte; der *AI Act* KI im KRITIS-Bereich. Die NIS-2-Richtlinie wird gezielt angepasst und zugleich als Teil des umfassenden Digitalomnibus überarbeitet. Rechenzentren werden im CADA sowie in verschiedenen delegierten Rechtsakten als Teil des strategischen Fahrplans für Digitalisierung und KI im Energiesektor reguliert. Auch das Zusammenspiel mit den Anforderungen des CADA und die laufenden Arbeiten an dem EU-Zertifizierungssystem für Cloud-Dienste (*EU Cloud Certification Scheme*, EUCS) ist unklar. Aus Sicht des VKU darf der CADA **kein paralleles Cybersicherheitsregime** neben den Vorgaben der NIS-2-Richtlinie, dem *Cybersecurity Act* sowie sektorspezifischen Regelungen etablieren. Bestehende Risikoanalysen, Audits, Zertifizierungen und sonstige Sicherheitsnachweise sollten nach dem *once-only*-Prinzip anerkannt und weiterverwendet werden können. Zusätzliche CADA-Assessments oder Risikominderungsmaßnahmen dürfen nur dort verpflichtend werden, wo sie einen klar abgegrenzten zusätzlichen Regelungsbedarf zu Souveränitäts- und Abhängigkeitsrisiken adressieren; Doppelprüfungen, redundante Nachweispflichten und unklare Verantwortlichkeiten sind zu vermeiden.

Auch auf **nationaler Ebene** wurde in Deutschland jüngst ein Kabinettsentwurf des Netzanschlusspaketes vorgelegt. Darin wird vorgesehen, dass auch Verteilnetzbetreiber Netzanschlussbegehren priorisieren dürfen. Im weiteren Verfahren spricht sich der VKU dafür aus, dass für die Verteilnetzebene auch eine „lokale Nutzen-Komponente“ nach dem *local first*-Prinzip Berücksichtigung findet. Mit Blick auf den CADA ist es nun wichtig, dass sich nationale und europäische Regulierungen hier **nicht widersprechen**, bspw. durch einen bevorzugten Netzzugang für Rechenzentren. Nach Erfahrungen des VKU kann diese Entscheidung letztendlich **nur von Verteilnetzbetreibern vor Ort** bewertet werden.

Für kommunale Unternehmen herrscht daher grundsätzlich **keine ausreichende Planungs- und Rechtssicherheit** in diesem Bereich. Viele kommunale Unternehmen stellen sich die Frage, ob die IT-Komponenten oder IT-Lösungen, die sie demnächst oder zuletzt eingekauft haben, als sicher eingestuft werden oder bald zu hohen Kosten ausgetauscht oder ersetzt werden müssen. Unklar bleibt auch die **Prüfbarkeit der Sicherheitsstufen** der Cloud-Dienste. Trotz eines umfassenden Pakets zur technologischen Souveränität fehlt ein Gesamtkonzept: zumindest im KRITIS-Bereich. Umso problematischer ist dies für kommunale Unternehmen, die auch das **Vergaberecht** anwenden müssen und somit von den Pflichten des kommenden *Industrial Accelerator Act* sowie der Überarbeitung des europäischen Vergaberechts betroffen sind.

In kommunalen Unternehmen bindet die Bürokratielast im Sicherheitsbereich personelle Ressourcen: insbesondere dort, wo diese an anderer Stelle dringend benötigt werden. Mit Blick auf den CADA sollten jegliche neuen Vorgaben zwingend **praxistauglich ausgestaltet werden**, mit einem **Schwerpunkt auf interoperablen Lösungen**. In dieser Hinsicht ist ein guter erster Schritt das **zentrale Verzeichnis für Cloud-Dienste**, welches in Art. 22 vorgeschlagen wurde. Idealerweise erhalten kommunale Unternehmen dadurch **frühzeitig Klarheit** über ihre Verpflichtungen und können entsprechend planen sowie dadurch für ihre jeweiligen Anwendungen gut geeignete und sicherheitsgerechte Cloud-Dienste auswählen und beschaffen. Derzeit fehlt allerdings ein **ausreichendes und leistbares Angebot** der genannten Cloud-Dienste. Zudem müssen Nutzer bzw. kommunale Unternehmen trotzdem Verträge, Service Level Agreements, Exit-Regelungen, Incident Handling, Backup-Konzepte, Audit-Rechte, Sicherheitsvereinbarungen und konkrete Betriebsanforderungen – selbst von Cloud-Diensten des zentralen Verzeichnisses – prüfen. Mit Blick auf Nutzerfreundlichkeit und Bürokratieabbau sollte **ein verbindlicher Benachrichtigungsmechanismus** der Anbieter, Prüfstellen oder Behörden hierzu eingeführt werden. So wären Kunden zeitnah informiert, falls sich bspw. eine Sicherheitsstufe eines Cloud-Dienstes ändert.