Energie. Wasser. Leben.

Berlin, 1. September 2026

BDEW Bundesverband
der Energie- und
Wasserwirtschaft e.V.
Reinhardtstraße 32
10117 Berlin
www.bdew.de

Stellungnahme

zum Vorschlag für einen Cloud and AI Development Act (CADA, COM(2026) 502 final)

Executive Summary

Der BDEW begrüßt das Ziel des CADA, digitale Souveränität und Resilienz zu stärken. Dies muss aber risikobasiert, technologieoffen und praxistauglich ausgestaltet werden.

Rechenzentren

- Rechenzentren müssen integriert mit Strom-, Wärme-, Wasser und Kommunikationsinfrastrukturen sowie dezentraler Stromerzeugung aus erneuerbaren oder CO_2-armen Quellen geplant werden.
- Beschleunigungszonen und strategische Projekte dürfen keinen automatischen Vorrang beim Netzanschluss erhalten und müssen zwingend die vorhandene Wasserverfügbarkeit berücksichtigen.
- Nachhaltigkeitsanforderungen müssen standortbezogen und verhältnismäßig sein. Zusätzliche Label, Berichts- und Zertifizierungspflichten sowie Doppelmeldungen sind zu vermeiden. Zudem führen spezifische Vorgaben für lediglich einzelne Stromabnehmer (Bsp. Rechenzentren) zu weiterer Fragmentierung bestehender Regelungen und sind daher zu vermeiden.
- Sensible Betriebs-, Netz- und KRITIS-Daten müssen nach dem Need-to-know-Prinzip geschützt und Veröffentlichungen ausreichend aggregiert werden.

Cloud-Dienste

- Union Assurance Levels dürfen nicht pauschal an Branchen oder public-order-relevante Tätigkeiten anknüpfen. Maßgeblich müssen Funktion, Kritikalität und konkreter Schutzbedarf sein.
- Anerkennungs-, Audit- und Transparenzverfahren müssen generell rechtssicher und bürokratiearm sein sowie mit NIS2 und dem Cybersecurity Act verzahnt werden. Ein paralleles Cybersicherheitsregime sowie doppelte Risikoanalysen, Prüfungen und Nachweise sind zu vermeiden. Migrationsprozesse müssen technisch realisierbar sein und die Service- und Versorgungskontinuität gewährleisten. Der BDEW lehnt starre Fristen und faktische Multi-Cloud-Verpflichtungen ab.
- Zusätzliche Beschaffungs-, Nachweis- und Prüfvorgaben dürfen vergabepflichtige Unternehmen nicht benachteiligen. Mehrkosten müssen kompensiert oder regulatorisch anerkannt und praxistaugliche Ausnahmen ermöglicht werden.
- Innovations- und KMU-Ziele dürfen nicht zu einer technisch oder wirtschaftlich unsachgerechten Aufteilung bestehender Cloud-Architekturen führen.

1 Einleitung

Am 03. Juni 2026 hat die EU-Kommission den Entwurf des Cloud and AI Development Acts (CADA) im Rahmen des European Tech Sovereignty Packages vorgestellt. Ziel des Legislativvorschlags ist die Entwicklung von nachhaltiger Rechenzentrumskapazitäten innerhalb der EU, um den erwarteten Mehrbedarf neuer digitaler Anwendungen decken zu können. Vorgesehen sind insbesondere Beschleunigungszonen (sog. „Acceleration Areas“), koordinierte Genehmigungs- und Anschlussverfahren, Nachhaltigkeitskennzahlen sowie ein europäisches Monitoring der Rechenkapazitäten. Zweitens soll das Paket die Verfügbarkeit souveräner Cloud-Dienste verbessern, um sich von strategischen Abhängigkeiten zu lösen und die Resilienz digitaler Infrastrukturen zu stärken.

Für die Energie- und Wasserwirtschaft ist die Ausgestaltung dieses Rahmens von erheblicher Bedeutung. Als Betreiber von Rechenzentren und Glasfasernetzen sowie als Strom-, Wärme- und Wasserversorger sind die BDEW-Mitglieder direkt oder indirekt auf allen Ebenen durch die neuen Vorgaben des CADA betroffen. Gleiches gilt für die geplanten Regelungen im Cloud-Bereich, da Unternehmen der Energie- und Wasserwirtschaft zum Teil public-order-relevante Aufgaben im Vergabekontext durchführen. Der Einsatz vieler Anwendungen, die derzeit durch außereuropäische Anbieter bereitgestellt werden, wird zukünftig aufgrund der geplanten Sicherheitsanforderungen nicht mehr möglich sein. Die Vorschläge würden in beiden Bereichen tief in bestehende IT-Architekturen, Geschäftsprozesse und Investitionsentscheidungen der Energie- und Wasserwirtschaft eingreifen.

Der BDEW unterstützt eine integrierte Planung von Rechenzentren mit Strom-, Wärme-, Wasser- und Kommunikationsinfrastrukturen sowie dezentraler Stromerzeugung aus erneuerbaren oder CO_2-armen Quellen (z.B. Photovoltaik, Windenergie, Gas-, Biomethan- oder Wasserstoff-Kraftwerke). Rechenzentren können bei entsprechend netz- und systemdienlichen Betrieb durch flexible Betriebsweisen, Speicher und Abwärmenutzung einen Beitrag zum Energiesystem leisten, sind jedoch nicht automatisch netz- oder systemdienlich. Anforderungen an Rechenzentren müssen aus Sicht der Energie- und Wasserwirtschaft daher standortbezogen, technologieoffen und verhältnismäßig ausgestaltet werden. Beschleunigungszonen oder strategische Projekte dürfen keinen automatischen Vorrang beim Netzanschluss begründen. Darüber hinaus muss vor der Bestimmung von Beschleunigungszonen die Wasserverfügbarkeit genau geprüft werden, um gesteigerten Nutzungskonflikten vorzubeugen. Insbesondere bestehende Industrie- und Kraftwerksstandorte sollten für den weiteren Kapazitätsausbau in den Blick genommen werden, da diese viele notwendige Voraussetzungen für die schnelle und ressourcenschonende Ansiedlung von Rechenzentren erfüllen. Unabhängig davon sind zusätzliche Meldepflichten zu vermeiden und sensible Betriebs- und KRITIS-Daten wirksam zu schützen.

Im Bereich der Cloud-Dienste begrüßt der BDEW die Zielrichtung des Vorschlags. Der angestrebte Souveränitätsgewinn darf jedoch nicht durch unverhältnismäßige Vorgaben, eingeschränkte Marktverfügbarkeit oder zusätzliche operative Risiken erkauft werden. Maßgeblich muss der konkrete Schutzbedarf der jeweiligen Tätigkeit sein. Sind alternative europäische Produkte für kritische Aufgaben nicht mit gleichen Sicherheitsstandards und vergleichbaren Preisen verfügbar, muss ein zuverlässiger Weiterbetrieb mit bisherigen Anbietern gewährleistet werden. Zudem sind Unternehmen, die an öffentlichen Vergabeverfahren teilnehmen, bereits jetzt durch umfangreiche Auflagen belastet. Weitere Vorgaben würden Unternehmen zusätzlich und unverhältnismäßig benachteiligen. Daher sollte der CADA stattdessen den Fokus auf Investitionen richten.

2 Energiewirtschaftliche Rahmenbedingen beim Ausbau von Rechenzentren berücksichtigen

Im Mittelpunkt des CADA stehen energie- und wassereffiziente Rechenzentren und der Ausbau europäischer Rechenkapazitäten, insbesondere für Anwendungen der Künstlichen Intelligenz (KI). Aus Sicht der Energiewirtschaft ist zu begrüßen, dass Rechenzentren nicht mehr ausschließlich als Stromverbraucher, sondern als relevante Akteure des Energiesystems betrachtet werden. In Verbindung mit Speichern, flexibler Anschlussnutzung und einem netzdienlichen Betrieb können sie einen Beitrag zur Stabilität und Effizienz des Energiesystems leisten.

2.1 Förderung des Ausbaus energie- und wassereffizienter Rechenzentren

Grundsätzliches Verständnis von Rechenzentren im CADA

Der BDEW unterstützt die integrierte Betrachtung von Rechenzentren, verfügbaren Netzkapazitäten, erneuerbarer beziehungsweise CO_2-armer Stromerzeugung, Speichern, Wärmenetzen und flexiblen Betriebskonzepten, wie sie in Art. 4 CADA vorgeschlagen wird. Rechenzentren sind allerdings nicht automatisch flexible Lasten oder Speicher. Ihre tatsächliche Systemdienlichkeit muss im Einzelfall technisch nachweisbar, vertraglich abgesichert und mit den hohen Anforderungen an Betriebs-, Versorgungs- und IT-Sicherheit vereinbar sein.

Der Ausbau von Datenzentren sollte sich an den jeweiligen standortspezifischen Gegebenheiten orientieren. Bei der Abwärmenutzung sind insbesondere das Temperaturniveau der Abwärme, das Vorhandensein oder die verbindliche Planung eines Wärmenetzes, geeignete Abnehmer sowie die tatsächliche und saisonale Wärmenachfrage zu berücksichtigen. Entsprechendes gilt für die Wassernutzung: Neben der Effizienz einzelner Kühltechnologien müssen die regionale Wasserverfügbarkeit, konkurrierende Nutzungen und mögliche Wasserknappheiten berücksichtigt werden. An Standorten mit begrenzter Wasserverfügbarkeit sollten

wasserschonende Kühltechnologien, etwa luftkühlende Systeme, besonders berücksichtigt werden.

Bei der Ausgestaltung von Art. 4 CADA sollten Anforderungen an Flexibilität, Abwärmenutzung sowie Energie- und Wassereffizienz daher standortbezogen, technologieoffen und verhältnismäßig ausgestaltet werden. Pauschale Vorgaben könnten geeignete Standorte ausschließen und den Ausbau europäischer Rechenkapazitäten eher behindern als fördern. Die EU-Mitgliedstaaten sollten weiterhin Spielraum für Regelungen auf regionaler und lokaler Ebene behalten. Außerdem ist zu berücksichtigen, dass aktuelle Technologien nicht erlauben sowohl Energie- als auch Wassereffizienz zur gleichen Zeit zu verbessern. Dieser Zielkonflikt muss entsprechend aufgelöst werden.

Beschleunigungszonen

Art. 10 CADA sieht vor, die Mitgliedstaaten zur Ausweisung von Beschleunigungszonen für Rechenzentren zu verpflichten. Hierdurch sollen Planungssicherheit geschaffen und die Genehmigung neuer Projekte beschleunigt werden. Bei der Auswahl geeigneter Standorte sollen unter anderem verfügbare Netzkapazitäten, Abwärmepotenziale, Umweltauswirkungen und weitere Voraussetzungen an die jeweilige Infrastruktur berücksichtigt werden.

Die Ausweisung geeigneter Vorranggebiete für Rechenzentren könnte für alle Beteiligten (Netzbetreiber sowie Entwickler von Rechenzentren und sich eignender Anlagentypen wie beispielsweise EE-Parks, Batterien und Nah-/Fernwärmesysteme) die Planungssicherheit verbessern und die gemeinsame Fokussierung auf konkret benannte und präqualifizierte Flächen erhöhen. Für die Standortauswahl sind insbesondere vorhandene und zukünftig verfügbare Netzkapazitäten, die Nähe zu Erzeugungsanlagen und Wärmeabnehmern, die Verfügbarkeit von Wasser und leistungsfähiger Glasfaserinfrastruktur, Flächenpotenziale sowie regionale Umwelt- und Klimarisiken zu berücksichtigen.

Eine integrierte Betrachtung dieser Faktoren kann Verfahren beschleunigen und die Ansiedlung von Rechenzentren gezielt in Regionen lenken, in denen sie in das Netz integriert, bei der Netzplanung berücksichtigt und möglichst systemdienlich betrieben werden können. Hierfür müssen neben den zuständigen nationalen, regionalen und kommunalen Stellen auch Stromnetzbetreiber sowie in gleichem Maße auch -erzeuger, Wasserunternehmen, Wärmenetzbetreiber und Betreiber von Kommunikationsnetzen frühzeitig und kontinuierlich in die Ausweisung der Zonen eingebunden werden. In Bezug auf die Verfügbarkeit von Wasser muss dabei neben der Kapazität auch der mögliche Ausbaubedarf der Trinkwasser-, Rohwasser- und Abwasserinfrastrukturen sowie die damit verbundenen Investitionen beachtet werden.

Zu berücksichtigen ist allerdings, dass geeignete Beschleunigungszonen nicht kurzfristig ausgewiesen werden können. Häufig müssen die für Rechenzentren erforderlichen Energie-,

Wärme-, Wasser- und Kommunikationsinfrastrukturen erst geschaffen oder ausgebaut werden. Soweit hierfür ein vorausschauender Netzausbau erforderlich ist, müssen dessen Finanzierung, die regulatorische Anerkennung der entstehenden Kosten und der Umgang mit Auslastungsrisiken rechtssicher geregelt werden.

Die Ausweisung einer Beschleunigungszone darf weder einen automatischen Netzanschlussanspruch noch einen Vorrang gegenüber anderen Anschlussbegehren begründen. Entscheidungen über Netzanschlüsse und die Zuteilung knapper Anschlusskapazitäten müssen weiterhin nach den geltenden energiewirtschaftsrechtlichen Regelungen und auf Grundlage einer technischen Einzelfallprüfung erfolgen. Sektorale Sonderregelungen im CADA dürfen die bestehenden nationalen Netzanschlusssystematiken nicht überlagern, müssen technologieoffen und diskriminierungsfrei gegenüber anderen Anschlusspetenten ausgestaltet sein. Eine weitere Fragmentierung des Rechtsrahmens und zusätzliche Rechtsunsicherheiten sind zu vermeiden.

Für die Zuteilung von Netzanschlusskapazitäten in Beschleunigungszonen hat der BDEW auf nationaler Ebene bereits konkrete Instrumente vorgeschlagen, die auch für die Umsetzung des CADA von Bedeutung sind. Dazu zählen insbesondere die Möglichkeit für Netzbetreiber, bei Anschlussbegehren großer Bezugskunden eine Vorschusszahlung zu verlangen, um die Realisierungswahrscheinlichkeit von Anfragen besser einschätzen zu können, sowie die Möglichkeit, ortsungebundene Anschlussbegehren im Falle fehlender Kapazitäten auf andere geeignete Standorte zu verweisen. Ergänzend sollte die Nachfrage gezielt in Regionen mit verfügbaren Netzkapazitäten gelenkt werden, etwa durch gezielte Standortanreize, damit Beschleunigungszonen tatsächlich dort entstehen, wo sie netzverträglich realisiert werden können. Anschlusspetenten, die sich netz- und systementlastend untereinander koordinieren, könnten bei der Zuteilung begrenzter Netzanschlusskapazitäten einen Vorzug erhalten[1].

Der BDEW begrüßt den expliziten Hinweis auf die Notwendigkeit, dass bei der Festlegung von Beschleunigungszonen die potenziellen Auswirkungen auf die Ziele der Wasserrahmenrichtlinie (2000/60/EG) berücksichtigt werden müssen. Denn die Auswirkungen eines hohen Wasserbedarfs auf die Wasserqualität vor Ort sind derzeit unklar und müssen im Vorfeld untersucht werden. Zudem greift eine reine Betrachtung der Qualität zu kurz: Während die

[1] Beispielhaft etwa, wenn Rechenzentrum und Großbatteriespeicher an einem Standort in der Nähe eines EE-Parks und in Zusammenarbeit mit einem (kommunalen, gewerblichen oder landwirtschaftlichen) Abwärmenutzer geplant werden. Diese Bündelung bewirkt einen geringeren Netzanschlussbedarf und im Falle einer flexiblen Betriebsweise auch eine geringere Netzbelastung.

Wasserrahmenrichtlinie einen Fokus auf die Wasserqualität legt, werden die Auswirkungen von Rechenzentrumsstandorten auf die Wasserverfügbarkeit im aktuellen Vorschlag nicht ausreichend berücksichtigt. Zwar liegt aktuell kein europäischer Rechtsrahmen zur Sicherung der Wasserquantität vor, dennoch muss diese zwingend bei der Festlegung von Beschleunigungszonen berücksichtigt werden. Die implizite Nennung im Rahmen von Umweltauswirkungen gemäß Artikel 10 1(h) CADA reicht nicht aus. Eine Vernachlässigung der aktuellen sowie ebenfalls projizierten Wasserverfügbarkeit würde Nutzungskonflikte steigern und könnte langfristig den kontinuierlichen Betrieb von Rechenzentren selbst gefährden, wenn Verfügbarkeiten (ggf. auch nur saisonal) erschöpft sind, da gemäß geltendem Recht die öffentliche Wasserversorgung einen verfassungsrechtlichen Vorrang hat. Eine ganzheitliche Betrachtung, die auch kommende Trends und die Auswirkungen des Klimawandels berücksichtigt, ist daher zwingend im Vorfeld der Festlegung der Beschleunigungszonen erforderlich. Zudem muss berücksichtigt werden, dass auch die für Rechenzentren notwendige Energieerzeugung je nach Erzeugungsform einen hohen Wasserbedarf hat. Darüber hinaus steigt der Wasserverbrauch besonders dann an, wenn allgemeine Spitzenabnahmen bei Trinkwasser (z.B. durch Hitzewellen) stattfinden und mehrere Rechenzentren kumulativ Wasser in einer Region angesiedelt werden. In diesen Fällen steigt das Risiko für Wasserengpässe zusätzlich an. Beim Bau neuer Rechenzentren sollte daher eine belastbare Prüfung und ein Nachweis erfolgen müssen, dass eine langfristige Wasserverfügbarkeit sichergestellt werden kann.

Aus Sicht der Energie- und Wasserwirtschaft sind bei der Identifikation geeigneter Beschleunigungszonen besonders bestehende bzw. ehemalige Industrie- und Kraftwerksstandorte zu berücksichtigen. An vielen dieser Standorte sind bereits leistungsfähige Netzanschlüsse, Flächenreserven, Energie- und teilweise Kühlwasserinfrastrukturen sowie Zufahrtswege vorhanden. Dadurch können zusätzliche Infrastrukturbedarfe reduziert, Genehmigungs- sowie Anschlussprozesse vereinfacht und weitere Rechenzentrumskapazitäten effizient sowie ressourcenschonenden gefördert werden.

Ausbaubeschleunigung fair, bürokratiearm und sicher ausgestalten

Die in Art. 11 CADA vorgesehene faire, angemessene und diskriminierungsfreie Zuteilung knapper Ressourcen innerhalb der Beschleunigungszonen wird vom BDEW grundsätzlich unterstützt. Für die Vergabe von Netzanschlusskapazitäten müssen jedoch die energiewirtschaftsrechtlichen Zuständigkeiten der Netzbetreiber und die bestehenden Anforderungen an einen diskriminierungsfreien Netzanschluss gewahrt bleiben.

Statt des im CADA vorgeschlagenen eigenständigen europäischen Zuteilungsregimes kann die im deutschen Energiewirtschaftsrecht etablierte und erprobte Systematik zur transparenten und sachlich begründeten Differenzierung zwischen Anschlussnehmergruppen (vgl. § 17 EnWG) als zentraler Referenzrahmen dienen. In Deutschland bewährte Kriterien wie die

Transparenz der angewandten Verfahren, die objektive Nachvollziehbarkeit der Ergebnisse und die Vermeidung eines Ausschlusses künftiger Anschlussbegehren sollten dabei auch auf europäischer Ebene anerkannt werden. Zusätzlich kann die koordinierte Anschlussplanung mehrerer Vorhaben, etwa die Kombination von Rechenzentren mit Batteriespeichern oder Erzeugungsanlagen an einem Standort, Netz- und Systembelastungen reduzieren. Entsprechende Koordinierungsansätze zwischen Projektträgern, Kommunen und Netzbetreibern sollten bei der praktischen Umsetzung der Beschleunigungszonen ausdrücklich unterstützt werden (s.o.).

Auch flexible Netzanschlussverträge nach § 17 Abs. 2b EnWG („Flexible Connection Agreements“, FCAs), mit denen Entnahmeleistung oder Nutzungszeiträume vertraglich begrenzt und flexibilisiert werden können, sind ein denkbares Instrument, um Anschlusspetenten unter vertraglich vereinbarten Konditionen bereits vor Abschluss des erforderlichen Netzausbaus einen Netzanschluss trotz knapper Netzkapazitäten schneller zu ermöglichen. FCAs sind dabei ausdrücklich als Übergangsinstrument bis zur Realisierung des erforderlichen Netzausbaus zu verstehen. Hierzu sollte der CADA bestehende Instrumente wie FCAs, die in den EU-Mitgliedstaaten bereits zur Anwendung kommen, bei der Weiterentwicklung des Regelungsrahmens ausdrücklich anerkennen und nicht durch abweichende Vorgaben erschweren. Ebenfalls sollte auf Kohärenz mit verwandter Regulierung, beispielsweise das derzeit im ordentlichen Gesetzgebungsverfahren befindliche EU Grids Package, geachtet werden.

Der BDEW unterstützt grundsätzlich das Ziel, die Nachhaltigkeit von Rechenzentren anhand geeigneter und harmonisierter Leistungskennzahlen zu bewerten. Der CADA will hierfür auf das derzeit im Aufbau befindliche gemeinsame EU-Bewertungssystem für die Nachhaltigkeit von Rechenzentren nach Delegierter Verordnung (EU) 2024/1364 zurückgreifen. Hieraus dürfen jedoch weder ein zusätzliches CADA-Label noch neue Zertifizierungs- oder Berichtspflichten entstehen. Eine Weiterentwicklung zu verbindlichen Bewertungsklassen oder Nachhaltigkeitslabeln sollte nur nach einer gesonderten Folgenabschätzung und unter Berücksichtigung standortbezogener Unterschiede erfolgen.

Bislang im Gesetzgebungsvorschlag nicht hinreichend berücksichtigt wird aus Sicht der Energie- und Wasserwirtschaft der Schutz der im Zusammenhang mit dem CADA erhobenen Daten. Standort-, Anschluss-, Last- und Betriebsdaten können Rückschlüsse auf kritische Infrastrukturen ermöglichen. Die Datenübermittlung ist daher auf das zwingend erforderliche Maß zu begrenzen. Für die Erhebung, Speicherung und Weitergabe müssen klare Vorgaben zur Zweckbindung, zu Zugriffsrechten nach dem Need-to-know-Prinzip, zur Verschlüsselung, Protokollierung und Löschung gelten. Die zuständigen Stellen müssen hierfür angemessene Sicherheits- und Berechtigungskonzepte nachweisen. Eine Veröffentlichung oder Weitergabe

sensibler Betriebs-, Geschäfts- oder KRITIS-Informationen an unberechtigte Dritte muss ausgeschlossen sein.

Zentrale Informationsstelle

Mit Art. 12 CADA soll eine zentrale Informationsstelle geschaffen werden, in der zukünftig Genehmigungs- und Anschlussprozesse koordiniert und gebündelt werden. Eine zügige Abstimmung zwischen Netz- und Rechenzentrumsbetreibern, Kommunen und Behörden sowie die Vereinfachung, Standardisierung und Digitalisierung von Verfahren sind zentrale Forderungen des BDEW.

Eine zentrale Informations- und Koordinierungsstelle kann als einheitliche Anlaufstelle Genehmigungsverfahren beschleunigen, Mehrfachabfragen vermeiden und die knappen personellen Ressourcen der beteiligten Behörden und Infrastrukturunternehmen schonen. Daten sollten möglichst nur einmal erhoben (Once-only-Prinzip) und über standardisierte digitale Schnittstellen weitergegeben werden.

Die zentrale Stelle darf jedoch nicht die gesetzlichen und technischen Zuständigkeiten der Strom-, Wärme-, Wasser- und Kommunikationsnetzbetreiber ersetzen. Entscheidungen über verfügbare Netzkapazitäten, technische Anschlussbedingungen und die Realisierbarkeit eines Anschlusses müssen bei den jeweils zuständigen Infrastrukturbetreibern verbleiben. Die Informationsstelle kann Verfahren koordinieren, aber weder Netzkapazitäten verbindlich zusagen noch technische Anschlussprüfungen vorwegnehmen.

Klärungsbedürftig bleibt, wie die Aufgaben der zentralen Stelle gegenüber den zuständigen Behörden und Infrastrukturbetreibern abgegrenzt werden, wer ihren Betrieb finanziert und wie die unterschiedlichen Verfahren zu Netzanschluss, Wasserentnahme, Abwasser, Umweltprüfung und Wärmeplanung praktisch koordiniert werden sollen. Auch für die zentrale Stelle müssen verbindliche Vorgaben zur Datensicherheit, Zweckbindung und Begrenzung von Zugriffsrechten gelten.

2.2 Strategisch relevante Rechenzentrumsprojekte

Art. 14 CADA sieht vor, bestimmte Rechenzentrumsprojekte als strategisch relevant einzustufen. Maßgeblich sollen unter anderem ihr Beitrag zur europäischen Rechenkapazität, zur Nachhaltigkeit und Innovation sowie zur Sicherheit und Stabilität des Stromsystems sein. Der BDEW unterstützt das Ziel, strategisch relevante Rechenkapazitäten auszubauen und damit die digitale Souveränität Europas zu stärken. Dies kann auch die Resilienz der Energie- und Wasserwirtschaft unterstützen, sofern Rechenzentren systemrelevante Dienstleistungen sicher und verlässlich bereitstellen.

Bei der energiewirtschaftlichen Bewertung genügt es jedoch nicht, dass an einem Standort eine EE-Anlage oder ein Speicher vorhanden ist. Entscheidend sind das tatsächliche Anschluss- und Betriebsverhalten sowie die nachweisbare Wirkung auf das Netz. Zusagen des Projektträgers zur Flexibilität oder Netzentlastung eines Rechenzentrums müssen vertraglich abgesichert und für den zuständigen Netzbetreiber technisch überprüfbar sein.

Auch darf die Einstufung als strategisches Projekt keinen automatischen Vorrang beim Netzanschluss und keine Verdrängung anderer systemrelevanter Anschlussbegehren bewirken. Eine Beschleunigung von Planungs- und Genehmigungsverfahren kann grundsätzlich sinnvoll sein. Entscheidungen über Flächen- und Netzanschlusskapazitäten müssen jedoch innerhalb der bestehenden planungs- und energiewirtschaftsrechtlichen Systematik getroffen werden. Außerdem ist wie oben unter 2.1 ausgeführt die Verfügbarkeit von Wasser zu prüfen. Andernfalls drohen Doppelregelungen und Rechtsunsicherheiten, die Verfahren unnötig verzögern oder gar in ihrer Umsetzung gefährden könnten.

2.3 Monitoring bürokratiearm umsetzen

Nach Art. 15 CADA soll ein Monitoring der verfügbaren Rechenkapazitäten, der Nachfrage sowie bestehender Kapazitätslücken und unterversorgter Gebiete aufgebaut werden. Daraus können sich auch Hinweise ergeben, in welchen Regionen neue Rechenzentrumscluster entstehen und wo Strom-, Wärme-, Wasser- und Kommunikationsinfrastrukturen künftig stärker beansprucht werden.

Der BDEW unterstützt grundsätzlich eine verbesserte Datengrundlage für die vorausschauende Infrastrukturplanung. Die Erkenntnisse zum zukünftigen Strombedarf von Rechenzentren sollten in die Szenariorahmen, Regionalszenarien und Netzausbaupläne einfließen. Gleichzeitig muss das Monitoring mit den dort bereits verwendeten Annahmen, Daten und Planungsprozessen abgestimmt werden.

Das Monitoring sollte, soweit möglich, bestehende Datenquellen, wie das Rechenzentrumsregister, nutzen. Da für die Bewertung der künftigen Entwicklung jedoch auch ergänzende Angaben zu geplanten Projekten und deren Reifegrade notwendig sind, sollte der bürokratische Mehraufwand für die Datenmeldungen für beteiligte Unternehmen möglichst geringgehalten werden.

Soweit sensible Standort-, Anschluss-, Last- oder Betriebsdaten verarbeitet werden, müssen die dargestellten Anforderungen an Datenminimierung, Zweckbindung und Zugriffsschutz gelten. Öffentlich zugängliche Ergebnisse sind ausreichend zu aggregieren, damit keine Rückschlüsse auf einzelne kritische Anlagen, Netzkapazitäten oder Verwundbarkeiten möglich sind.

3 Gefährdung der Versorgungssicherheit durch neue Cloud-Vorgaben ausschließen

Der Art. 16 CADA sowie Annex II sehen einen einheitlichen Cloud-Computing-Souveränitätsrahmen mit vier EU-weiten Bewertungsstufen („Union Assurance Level“, s. auch Abschnitt 3.2 dieser Stellungnahme) vor, durch die Unternehmen mit Aufgaben im Bereich der öffentlichen Versorgung unabhängiger von Cloud-Anbietern aus Drittstaaten werden sollen. Als KRITIS-Betreiber unterstützt der BDEW die Prüfung von Cloud-Diensten aufgrund vorgegebener öffentlicher Kriterien. In Fällen, in denen cloudbasierte Prozesse für kritische Aufgaben in der Energie- und Wasserbranche eingesetzt werden, kann hierdurch der souveräne Betrieb digitaler Systeme unterstützt werden.

Die Abhängigkeit von außereuropäischen Technologieanbietern ist in der Energie- und Wasserwirtschaft je nach Marktrolle und Anwendungsbereich unterschiedlich ausgeprägt. In Vertrieb und Handel ist sie tendenziell stärker als im Netzbetrieb. Auch europäische Softwareanbieter betreiben ihre Dienste vielfach auf US-amerikanischer Cloud-Infrastruktur. Angebote mit vollständig europäischer Infrastruktur stehen teilweise nur zu höheren Preisen zur Verfügung oder decken benötigte Standardfunktionen noch nicht vollständig ab. Auch bei Sicherheitsdiensten wie Monitoring sowie Identitäts- und Berechtigungsmanagement greifen europäische Cloud-Anbieter teilweise ebenfalls auf Leistungen nicht-europäischer Anbieter zurück.

Daher kommt es bei der Umsetzung auf die Praxistauglichkeit und Technologieoffenheit der Vorgaben an, um den dauerhaften Betrieb sicherstellen zu können. Ein Ausweichen auf technisch schlechtere Lösungen sowie unverhältnismäßige Preise müssen ausgeschlossen werden, um die Versorgungssicherheit und Kosteneffizienz der Energie- und Wasserversorgung nicht zu stark zu beeinflussen.

3.1 Sicherheitsprüfung und Transparenz von Cloud-Diensten kundenfreundlich ausgestalten

Engpässe durch Anerkennung und Audits vermeiden

Positiv zu bewerten ist, dass Art. 17 bis Art. 20 CADA einen Anerkennungs- und Auditmechanismus für souveräne Cloud-Dienste vorsehen. Anbieter müssen bei der nationalen Behörde eine Anerkennung beantragen und ein Konformitätsbewertungsverfahren durchlaufen, das eine Selbstbewertung bis zu einer unabhängigen Drittprüfung beinhalten kann. Es ist zu begrüßen, dass die Vergleichbarkeit von Cloud-Diensten durch die Einstufung in die verschiedenen Assurance-Level deutlich verbessert und die Beschaffung simplifiziert wird. Wichtig ist allerdings, dass die gewählten Souveränitätskriterien praxistauglich ausgestaltet werden, damit ein Umstieg auf andere Cloud-Dienste vor dem Hintergrund realistischer Übergangsfristen realisiert werden kann.

Der bisherige CADA-Vorschlag lässt derzeit noch offen, welche Behörden auf nationaler Ebene die Auditierung und Anerkennung durchführen sollen. Zur Förderung einer besseren Planungssicherheit sollten im weiteren Verfahren weitere Kriterien zur Auswahl der Institution festgelegt werden.

Ergänzend muss klar geregelt werden, welche Pflichten für Nutzer von Cloud-Diensten entstehen, wenn sich die Zertifizierung eines Cloud-Dienstes, dessen Anerkennung oder die zugrunde liegende Risikobewertung ändert. Die fortlaufende Überwachung der Gültigkeit von Sicherheitsstufen und Zertifizierungen darf nicht allein den Nutzern auferlegt werden. Vielmehr sollten Cloud-Dienstleister, Prüfstellen und zuständige nationale Behörden verpflichtet werden, relevante Änderungen aktiv, transparent und zeitnah an betroffene Kunden zu kommunizieren.

Erforderlich ist ein verbindlicher Informationsprozess, der eindeutig festlegt, ab welchem Zeitpunkt mögliche Folgeverpflichtungen, insbesondere Migrations- oder Anpassungspflichten, wirksam werden. Andernfalls entstehen zusätzlicher administrativer Aufwand, Rechtsunsicherheiten und erhebliche operative Risiken für betroffene Organisationen. Dies gilt insbesondere, wenn nach einer geänderten Einstufung kurze Migrationsfristen ausgelöst werden.

Transparenz schaffen, Benachrichtigungspflichten ergänzen und Betreiberverantwortung erhalten

Das nach Art. 21 und 22 CADA vorgesehene zentrale Verzeichnis der kategorisierten Cloud-Dienste kann einen wichtigen Beitrag zu mehr Transparenz im Cloud-Markt leisten. Besonders kleinere und mittlere Unternehmen sind darauf angewiesen, geeignete Cloud-Dienste für ihre jeweiligen kritischen Aufgaben einfach erkennen zu können, um die rechtskonforme Umsetzung zu erleichtern.

Daher ist es für die BDEW-Mitgliedsunternehmen entscheidend, dass die Informationen verständlich, aktuell, maschinenlesbar und praxisnah aufbereitet werden. Erkennbar sein muss insbesondere, welche Kriterien geprüft wurden, welches Union Assurance Level ein Dienst erfüllt, wie lange die Anerkennung gilt und unter welchen Voraussetzungen sie geändert oder entzogen werden kann. Nur dann kann das Verzeichnis Beschaffung, Marktorientierung und interne Due-Diligence-Prozesse tatsächlich erleichtern.

Das zentrale Verzeichnis auf der EU-Ebene darf zugleich nicht als Ersatz für Betreiberverantwortung und Vertragsprüfung verstanden werden. Auch bei anerkannten Cloud-Diensten bleiben Service Level Agreements (SLA), Exit-Regelungen, Incident-Handling, Backup, Audit-Rechte, Datenportabilität, Subunternehmertransparenz und konkrete Sicherheitsvereinbarungen erforderlich.

Ergänzend sollten die Transparenzpflichten nach Art. 23 CADA um einen verbindlichen Benachrichtigungsmechanismus gegenüber betroffenen Kunden erweitert werden. Änderungen, Aussetzungen oder Widerrufe einer Anerkennung, Zertifizierung oder Sicherheitsstufe dürfen nicht nur im Register nachvollziehbar sein. Betroffene Nutzer müssen aktiv, transparent und rechtzeitig informiert werden, damit sie mögliche Anpassungs-, Prüf- oder Migrationspflichten rechtssicher bewerten und fristgerecht umsetzen können.

3.2 Union Assurance Levels praxistauglich konkretisieren

Im Annex II des CADA werden die vier Union Assurance Level eingeführt, die abhängig von der Kritikalität der Tätigkeiten durch Unternehmen berücksichtigt werden müssen, wenn diese Cloud-Dienste neu implementieren und an öffentlichen Ausschreibungen teilnehmen. Aufgrund der NIS2-Einstufung und der Einordnung eines Teils der Unternehmen als KRITIS-Betreiber werden bestimmte Aufgaben der Energie- und Wasserwirtschaft voraussichtlich unter die Level 2 bis 3[2] fallen.

Die geplanten Anforderungen an Drittstaatenkontrolle, EU-Bürgerschaft, Sicherheitsfreigaben, Supportstrukturen sowie Design, Entwicklung, Wartung und Weiterentwicklung von Plattformen greifen tief in bestehende Cloud-Märkte und Betriebsmodelle ein. Es bedarf weiterer Konkretisierung bei Standort-, Kontroll- und Plattformanforderungen. Bei globalen Cloud-Anbietern befinden sich Management- und Steuerungskomponenten häufig außerhalb der EU. Zudem ist unklar, inwieweit Entwicklung, Betrieb und Bereitstellung zugrunde liegender Plattformtechnologien vollständig innerhalb der Union erfolgen müssen. Ohne rechtssichere Klärung drohen unterschiedliche Auslegungen, Planungsunsicherheit und Verzögerungen.

Die Anforderungen der Level 3 und 4 können faktisch dazu führen, dass bestimmte bislang genutzte internationale Cloud-Angebote, insbesondere von Anbietern unter Drittstaatenkontrolle, für sensible Anwendungen innerhalb der EU nicht mehr oder nur eingeschränkt nutzbar sind. In der Praxis sind diese Art von Anforderungen nur dort gerechtfertigt, wo der konkrete Schutzbedarf dies trägt.

Ein pauschaler Ausschluss etablierter Anbieter ist jedoch weder wirtschaftlich noch sicherheitstechnisch sachgerecht, wenn bestehende Lösungen hohe Sicherheitsstandards erfüllen und ein kurzfristiger Wechsel neue Betriebs- oder Sicherheitsrisiken auslösen würde. Bestehende Legacyprozesse, gewachsene Plattformarchitekturen und langfristige

[2] Level 4 kommt voraussichtlich nur in den Fällen zur Anwendung, wenn Energie- und Wasserversorgung Relevanz für die militärische Verwendungsfähigkeit besitzt.

Vertragsbeziehungen können eine kurzfristige Umstellung auf alternative europäische Cloud-Systeme erheblich erschweren.

Bestehende Lock-in-Effekte lassen sich nicht allein durch neue Souveränitätsanforderungen und Präferenzen für europäische Lösungen abbauen. Erforderlich sind realistische Übergangszeiten, Portabilitätsanforderungen, Interoperabilität und marktverfügbare Alternativen. Entscheidend sollte sein, ob ein Cloud-Dienst die einschlägigen Sicherheitsanforderungen nachweislich erfüllen. Die reine Anbieterherkunft sollte nicht das einzige Kriterium sein, soweit Risiken durch technische, organisatorische und vertragliche Maßnahmen wirksam beherrscht werden können.

3.3 Grundlage für differenzierte Risikobewertung und zuverlässige Umsetzung legen

Risikobewertung nicht branchen- sondern sektorspezifisch durchführen

Mit Art. 29 CADA wird parallel zu den Sicherheitskriterien für Cloud-Anbieter abgeglichen, welche Assurance Level für bestimmte public-order-relevanten Tätigkeiten notwendig sind. Dieser risikobasierte Ansatz ist grundsätzlich sachgerecht, weil Cloud-Dienste in der Energie- und Wasserwirtschaft sehr unterschiedliche Funktionen erfüllen können. Deshalb muss auch sichergestellt werden, dass nicht alle public-order-relevanten Tätigkeiten automatisch zu einer Level 4 Bewertung führen, sondern eine gerechtfertigte Abstufung anhand der konkreten Tätigkeit und des jeweiligen Risikos stattfindet.

Die Einstufung muss sowohl zwischen den einzelnen Tätigkeiten als auch nach deren Bedeutung für die Erbringung kritischer Dienstleistungen differenzieren. Unmittelbar kritische Tätigkeiten sind dabei von unterstützenden IT-Diensten zu unterscheiden. Systeme zur Steuerung kritischer Infrastruktur sind anders zu bewerten als Systeme zur Analyse oder Auswertung von Betriebsdaten. Ebenso muss präzisiert werden, wie zentrale IT-Basisdienste einzuordnen sind, die für den Betrieb moderner IT-Landschaften erforderlich sind, etwa Arbeitsplatzsysteme, Kommunikationsdienste, Identitäts- und Zugriffsmanagement oder Sicherheitsanalysesysteme. Eine pauschale Einstufung solcher Dienste könnte umfangreiche Parallelstrukturen und redundante Systemlandschaften erforderlich machen. Dies würde erhebliche zusätzliche Kosten verursachen, Komplexität erhöhen und die Wettbewerbsfähigkeit der betroffenen Organisationen beeinträchtigen.

Die Überprüfung der Risikobewertung in einem Abstand von zwei Jahren ist aufgrund des sich schnell wandelnden technologischen wie geopolitischen Umfeld nachvollziehbar. Entscheidend ist jedoch, dass bei veränderten Anforderungen durch Neukategorisierung von Tätigkeiten Unternehmen frühzeitig eingebunden und informiert werden. Mögliche Anpassungs- oder Migrationspflichten dürfen erst nach einem klar definierten Informations- und Bewertungsprozess sowie unter Berücksichtigung angemessener Übergangsfristen wirksam werden.

Sicheren Betrieb durch angemessene Migrationszeiten ermöglichen

Art. 29 Abs. 6 i.V.m. Art. 48 CADA regelt den Wechsel von Cloud-Anbietern in den Fällen, in denen die Risikoanalyse Sicherheitsbedenken identifiziert hat. Hierfür werden angemessene Übergangsfristen von bis zu 12 Monaten angesetzt. Dieses Vorgehen ist grundsätzlich für KRITIS-Betreiber nachvollziehbar, um die Ziele des CADA zu erreichen und Resilienz von kritischen Funktionen zu erhöhen. Die Umsetzung darf jedoch nicht über starre Fristen erfolgen, die der technischen und betrieblichen Realität komplexer Cloud-Landschaften nicht gerecht werden.

Für die Energie- und Wasserwirtschaft sind realistische und risikoorientierte Migrationspfade unverzichtbar. Migrationen betreffen nicht nur die Auswahl eines neuen Cloud-Dienstes, sondern Planung, Beschaffung, Architekturprüfungen, Vertragsbeziehungen, Schnittstellen, Testsysteme, Betriebsfreigaben und Inbetriebnahme. Gerade komplexe, hochintegrierte oder betriebskritische Systeme können nicht kurzfristig und ohne Risiko verlagert werden. Maßgeblich müssen daher technische Machbarkeit, Servicekontinuität, Datenportabilität, IT-Sicherheit und die Kontinuität kritischer Geschäfts- und Versorgungsprozesse sein.

Eine pauschale Maximalfrist von 12 Monaten wird der Komplexität kritischer oder hochintegrierter Migrationsvorhaben nicht gerecht. Statt der starren Zeitvorgaben sollte die erforderliche Übergangsfrist auf Basis einer individuellen Bewertung des jeweiligen Systems festgelegt werden können. Für komplexe Vorhaben sollten angemessene und risikoorientierte Migrationspläne zugelassen werden, die Planung, Umsetzung, Tests und Inbetriebnahme realistisch abbilden.

Zudem sind Unternehmen, bei denen Cloud-Dienste auch in kritischen Funktionen genutzt werden, auf zusätzliche Unterstützung bei der Servicekontinuität und Datenportabilität durch Cloud-Betreiber angewiesen. Neue Governance-, Audit- und Migrationsanforderungen müssen sich an den tatsächlich verfügbaren personellen Ressourcen orientieren. Zusätzliche regulatorische Komplexität darf bestehende Fachkräfteengpässe nicht zusätzlich verschärfen. Daher sollten auch Regelungen dazu gefunden werden, wie Cloud-Anbieter die sichere Migration, beispielsweise durch die Übertragung von Daten und Geschäftsprozessen unterstützen müssen. Diese Aufgabe können Nutzer von Cloud-Diensten nicht einseitig stemmen.

Multi-Cloud risikobasiert ermöglichen, aber nicht erzwingen

Der in Art. 29 Abs. 9 CADA angelegte Ansatz, Multi-Cloud-Strategien für besonders kritische Bereiche einzuführen ist generell nachvollziehbar. Multi-Cloud- oder Multi-Source-Ansätze können dazu beitragen, Lock-in-Effekte zu reduzieren, Resilienz zu stärken und Abhängigkeiten von einzelnen Anbietern zu verringern.

Multi-Cloud ist jedoch kein Selbstzweck und darf nicht faktisch für jeden Use Case verpflichtend werden. Ob ein Dual-, Multi-Source- oder Multi-Cloud-Ansatz erforderlich und

angemessen ist, muss risikobasiert im Ermessen des Betreibers geprüft werden. Je nach Strategie, Art und Umfang des Geschäfts sowie Schutzbedarf der jeweiligen Anwendung kann auch ein Single-Source-Ansatz ausreichend und sicher sein.

Entscheidend ist, dass neben Resilienz- und Souveränitätszielen auch Kosten, technische und organisatorische Komplexität, Leistungs- und Performanceanforderungen, Security Operations, Fachkräftebedarf sowie Exit- und Interoperabilitätsanforderungen berücksichtigt werden. Der parallele Einsatz mehrerer Cloud-Dienste kann erhebliche Lizenz-, Integrations-, Betriebs- und Transaktionskosten auslösen und die Steuerung moderner IT-Landschaften deutlich erschweren.

Die Anforderungen der Assurance Levels nach Annex II sollten daher so ausgestaltet werden, dass wesentliche Basis- und Plattformdienste möglichst konsistent von einem Anbieter bezogen werden können. Anbieterwechsel, Datenportabilität und Betriebsfortführung müssen praktisch abgesichert werden, ohne durch übermäßige Vorgaben neue Lock-in-Effekte oder faktische Multi-Provider-Zwänge zu schaffen.

3.4 Beschaffung von europäischen Cloud-Diensten begrenzen

Öffentliche Investitionen und Förderung statt Ausschreibungsverfahren, die zu Benachteiligungen führen

Der Art. 30 CADA sieht vor, dass Anbieter, die in öffentlichen Aufgaben eingebunden sind und Unternehmen, die sich auf öffentliche Vergabeverfahren bewerben angemessene Souveränitätskriterien erfüllen müssen. Werden die Sicherheitskriterien nicht eingehalten, können Unternehmen von sensiblen öffentlichen Aufgaben ausgeschlossen werden.

Sicherheits- und souveränitätsbezogene Anforderungen an Cloud-Beschaffungen sind bei kritischen Infrastrukturen im Wesentlichen gerechtfertigt. Dies darf allerdings nicht zu zusätzlichen, unverhältnismäßigen Beschaffungspflichten für die Energie- und Wasserwirtschaft führen. Die Anforderungen müssen strikt risikobasiert, verhältnismäßig, technologieoffen und praxistauglich ausgestaltet werden.

Vergabepflichtige Energie- und Wasserunternehmen, darunter klassische öffentliche Auftragnehmer und Sektorauftraggeber, unterliegen bereits umfangreichen vergaberechtlichen Anforderungen. Zusätzliche Nachweis-, Eigentümer-, Kontroll- und Lieferkettenprüfungen können Beschaffungsverfahren erheblich verlangsamen, die Anbieterbasis und Wettbewerbsintensität verringern sowie Kosten und Realisierungszeiten erhöhen.

Art. 30 CADA darf daher weder zu einer Ausweitung vergaberechtlicher Pflichten auf bislang nicht vergabepflichtige Unternehmen führen noch vergabepflichtige Energie- und Wasserunternehmen gegenüber nicht vergabepflichtigen Marktakteuren strukturell benachteiligen.

Zudem plant die EU-Kommission bereits im Herbst 2026 die Reform des öffentlichen Vergaberechts, sodass Doppelregulierung für vergabepflichtige Energie- und Wasserunternehmen im Zuge des CADA unbedingt zu vermeiden ist.

Digitalpolitische Zielstellungen sollten vorrangig durch Förderinstrumente, Investitionsanreize und die direkte Stärkung europäischer Anbieter verfolgt werden. Soweit zusätzliche Beschaffungsanforderungen dennoch vorgesehen werden, sind sie auf sicherheits- oder systemkritische Dienste und Komponenten mit einem konkreten Mehrwert für die Resilienz kritischer Branchen zu begrenzen sowie risikobasiert, verhältnismäßig und technologieoffen auszugestalten. Sie müssen mit wirksamen Ausnahmen, angemessenen Übergangsfristen und Flexibilitätsmechanismen verbunden sein. Unvermeidbare Mehraufwände und Mehrkosten müssen sachgerecht berücksichtigt, kompensiert und bei regulierten Netzbetreibern regulatorisch anerkannt werden können.

Die Ausnahmen nach Art. 30 Abs. 4 CADA müssen praxistauglich, rechtssicher und mit geringem Dokumentationsaufwand anwendbar sein. Öffentliche Auftraggeber sollten keine aufwendigen Prüf- und Dokumentationsverfahren durchlaufen müssen, wenn keine geeigneten anerkannten Dienste verfügbar sind, kein hinreichender Wettbewerb zu erwarten ist oder die Anwendung der Anforderungen unverhältnismäßige Kosten verursachen würde. Die vorherige Durchführung oder Wiederholung eines erfolglosen Vergabeverfahrens darf nicht vorausgesetzt werden. Bestehende Zertifikate und Nachweise sollten anerkannt und Doppelprüfungen vermieden werden.

Für die Kostenprüfung sollte eine widerlegbare Vermutung gelten, dass Mehrkosten von mehr als fünf Prozent gegenüber einer ansonsten geeigneten marktverfügbaren Alternative unverhältnismäßig sind. Dabei sind neben dem Beschaffungspreis auch Implementierungs-, Umstellungs-, Nachweis-, Verzögerungs- und Lebenszykluskosten zu berücksichtigen. Auch unterhalb dieser Schwelle muss eine Ausnahme möglich bleiben, wenn die kumulativen Belastungen oder Auswirkungen auf den Zeitplan unverhältnismäßig sind. Andernfalls drohen zusätzlicher Verwaltungsaufwand, Verzögerungen beim Ausbau und bei der Digitalisierung kritischer Energie- und Wasserinfrastrukturen.

Doppelte Prüfpflichten für private und KRITIS-nahe Unternehmen vermeiden

Unternehmen, die nicht durch die vergaberechtlichen Auflagen von Art. 30 betroffen sind, können nach Art. 31 CADA eigene Assessments durchführen. Neben diesen freiwilligen Optionen kann die EU-Kommission über delegierte Rechtsakte verpflichtende Folgenabschätzungen (Impact Assessments) und Risikominderungsmaßnahmen für bestimmte private Einrichtungen in hochkritischen Sektoren festlegen. Aus Sicht des BDEW darf dies jedoch nicht zu zusätzlichen, formalisierten und doppelten CADA-Impact-Assessments führen, soweit bereits

bestehende Risikoanalysen, Sicherheitsnachweise und regulatorische Anforderungen aus NIS2, KRITIS, Datenschutzrecht oder sektorspezifischen Vorgaben greifen.

Der CADA darf zudem kein paralleles Cybersicherheitsregime neben NIS2 und dem Cybersecurity Act schaffen. Technische Cybersicherheitsanforderungen und das entsprechende Risikomanagement sollten weiterhin über die bestehenden Rechtsakte adressiert werden; zusätzliche CADA-Vorgaben für Unternehmen nach Art. 31 sollten auf spezifische Souveränitäts- und Abhängigkeitsrisiken begrenzt bleiben. Bestehende Risikoanalysen, Audits, Zertifizierungen und sonstige Sicherheitsnachweise müssen anerkannt und nach dem Once-only-Prinzip weiterverwendet werden können.

Neue Assessments und Risikominderungsmaßnahmen dürfen nur dort verpflichtend werden, wo sie gegenüber den bestehenden NIS2- und sektorspezifischen Anforderungen einen klar abgegrenzten zusätzlichen Regelungsbedarf adressieren. Doppelprüfungen, redundante Nachweispflichten und unklare Verantwortlichkeiten sind zu vermeiden. Hinzukommt, dass öffentlich verfügbare Assessments Orientierung und Entlastung bieten können. Sie dürfen unternehmens- und systembezogene Risikoanalysen jedoch nicht vollständig ersetzen, wenn konkrete OT-, Leitstellen- oder KRITIS-Prozesse betroffen sind. Für solche Anwendungen bleibt eine einzelfallbezogene Bewertung durch die jeweiligen Betreiber erforderlich.

3.5 Innovation fördern, Mehrkosten sachgerecht berücksichtigen

Mit Art. 32 CADA werden die Vorgaben zur Beschaffung von Cloud-Diensten durch nicht-preisliche Zusatzkriterien ergänzt, die den Beitrag zur Entwicklung europäischer Cloud-Ökosysteme bewerten sollen. Die Förderung von Innovation ist aus Sicht des BDEW zu begrüßen. Hierbei gilt allerdings erneut, dass etwaige Mehrkosten, die bei Unternehmen durch den Einsatz neuer Cloud-Dienste entstehen, sachgerecht kompensiert werden müssen. Bei regulierten Netzbetreibern sollten die Mehrkosten regulatorisch anerkannt werden können. Durch die nicht-preislichen Zusatzkriterien dürfen keine Benachteiligungen für vergabepflichtige Unternehmen entstehen.

Auch die in Art. 33 Abs. 4 CADA vorgesehene Zielsetzung, einen Anteil der Beschaffung von Cloud-Computing-Diensten und KI-Systemen an innovative KMU zu vergeben, muss mit tragfähigen IT-Architekturen vereinbar bleiben. Sie darf nicht zu einer erzwungenen Aufteilung von Cloud-Leistungen auf mehrere Anbieter führen. Für viele Unternehmen der Energie- und Wasserwirtschaft bieten standardisierte Plattformen aus einer Hand Vorteile hinsichtlich Sicherheit, Integration, Betrieb und Wirtschaftlichkeit. KMU- und Innovationsziele dürfen daher nicht zu Lasten einer wirtschaftlich und technisch sinnvollen Gesamtarchitektur erreicht werden.