VERBAND KOMMUNALER UNTERNEHMEN e.V.

STELLUNGNAHME

zum Cybersicherheitspaket der Europäischen Kommission

Berlin / Brüssel, 29.07.2026

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

DIE KOMMUNALEN UNTERNEHMEN

Bedeutung des Vorhabens für kommunale Unternehmen

Als Betreiber kritischer Infrastrukturen stellt Sicherheit für kommunale Unternehmen ein besonders hohes Gut dar. Seit der Einführung des **Cybersicherheitsrechtsakt, (*Cybersecurity Act*, CSA)** im Jahr 2019 hat sich das geopolitische und sicherheitspolitische Umfeld der EU dramatisch verändert. Vor diesem Hintergrund ist es aus VKU-Sicht durchaus angemessen, dass die Kommission nun in der **Überarbeitung des CSA (*Cybersecurity Act* 2, CSA2)** strengere Sicherheitsmaßnahmen vorsieht: darunter auch einen neuen Mechanismus zur Überprüfung „nicht-technischer" Risiken auf unterschiedlichen Ebenen bei Einrichtungen gemäß **Anhang I und II der NIS-2-Richtlinie**. Gleichzeitig belasten kommunale Unternehmen – insbesondere im KRITIS-Bereich – bereits erhebliche **Dokumentations-, Berichts- und Transparenzpflichten**. Dies ist eine besonders große Herausforderung angesichts fehlender personeller Ressourcen. Diese werden wiederum in anderen Arbeitsbereichen dringen benötigt, um die Sicherheit kritischer Infrastrukturen vor Ort zu gewährleisten. Vor diesem Hintergrund teilt der VKU das Ziel der Europäischen Kommission, Bürokratie abzubauen und den Cybersicherheitsrechtsrahmen zu vereinfachen: ohne dabei den Schutz kritischer Infrastrukturen in Frage zu stellen.

Positionen des VKU in Kürze

In diesem Sinne begrüßt der VKU grundsätzlich das Bestrebung der Kommission, die **NIS-2-Richtlinie** zu vereinfachen. Fragwürdig ist allerdings, warum diese Vereinfachungen zum einem im Digitalomnibus und zum anderen im Rahmen des CSA2 vorgeschlagen werden. Dies könnte zu Rechts- und Planungsunsicherheiten führen. Zudem ist die Ausweitung der **KMU-Definition auf *Small Mid-Caps* (SMC)** aus Sicht der Kommunalwirtschaft sehr problematisch. Kommunale Unternehmen sind von dieser Definition ausgeschlossen und werden somit faktisch benachteiligt. Auch der Vorschlag der Kommission, nur **Stromerzeuger mit einer Gesamtleistung von mehr als 1 MW** als „wesentliche" oder „wichtige" Einrichtungen im Sinne der NIS-2-Richtlinie zu betrachten ist sehr kritisch. Es besteht die Gefahr, dass Mehrspartenunternehmen, die mehr als 1 MW Energie erzeugen, in Deutschland erneut deutlich strengeren Vorschriften unterliegen werden: trotz einer Ausnahmeregelung im deutschen Umsetzungsgesetz für Mehrspartenunternehmen.

Hinsichtlich der Vorschläge zum **CSA2** ist die grundsätzliche Stoßrichtung der Kommission, Risiken sowohl aus **technischer als auch aus politischer Perspektive** ganzheitlich zu bewerten – angesichts der angespannten Sicherheitslage – richtig. Als Betreiber kritischer Infrastrukturen nehmen kommunale Unternehmen diese Bedrohungen unmittelbar vor Ort wahr. Gleichzeitig sollten die entsprechenden Maßnahmen ein ***ultima ratio*** sein, mit

einem Schwerpunkt auf technischen Risiken und einer praxisnahen Ausgestaltung: insbesondere mit Blick darauf, wie etwaige Verbote innerhalb ohnehin **anspruchsvoller europäischen Vergabe- und schwierigen Beschaffungsprozessen** umgesetzt werden sollen.

Kernforderungen des VKU

- Ausweitung der Erleichterungen für KMU auf Small Mid-Caps (SMCs) nur unter **Beibehaltung der bestehenden ausdrücklichen Ausnahme** für öffentliche Unternehmen vergleichbarer Größe;
- **Keine Benachteiligung von Mehrspartenunternehmen** in Deutschland, die mehr als 1 MW Energie erzeugen;
- Verbote aufgrund „nichttechnischer" Risiken in Lieferketten sind grundsätzlich nachvollziehbar, sollten jedoch nur als *ultima ratio* vorgesehen und praxisnah ausgestaltet werden, u.a. durch **wirtschaftliche Unterstützung für kommunale Unternehmen und Hersteller**;
- Die Verzahnung mit dem **Digital Networks Act (DNA)** birgt die Gefahr von **Wettbewerbsverzerrungen, steigenden Preisen und Verzögerungen** beim Glasfaserausbau. Besonders im Telekommunikationsbereich sind eine Orientierung an realen Lebenszyklen, eine schrittweise Umsetzung sowie ein Fokus auf technisch begründete Risiken wichtig;
- **Keine Ersetzung nationaler Kompetenzen durch die ENISA**;
- Verankerung von ***Security by Design*** im EU-Cybersicherheitszertifizierungsrahmen;
- **Vermeidung von Doppelregulierung** durch die zahlreichen EU-Vorschläge in den Bereichen Digitalisierung, Cybersicherheit und Vergaberecht sowie durch noch strengere **nationale Regelungen**.

Anpassungen der NIS-2-Richtlinie

2026/0012 (COD)

Anwendungsbereich für kommunale Unternehmen klarstellen

Die Ausgestaltung der Anhebung der Schwellenwerte ist aus Sicht der Kommunalwirtschaft klärungsbedürftig. Gemäß Kommissionsvorschlag soll der Begriff der **„wesentlichen Einrichtung“** (*essential entities*) (Art. 3(1)(a) NIS-2-Richtlinie) geändert werden. Wie in vielen anderen Bereichen (u.a. im Digital- und KI-Omnibus) führt die Kommission in der NIS-2-Richtlinie eine neue Unternehmenskategorie der ***Small Mid-Caps*** **(SMC)** ein. Demnach sollen zukünftig Unternehmen mit weniger als 750 Beschäftigten und einem Jahresumsatz von höchstens 150 Mio. Euro oder einer Bilanzsumme von höchstens 129 Mio. Euro regelmäßig nur noch als „wichtige Einrichtungen“ eingestuft werden, wodurch sich ihre regulatorischen Verpflichtungen verringern.

Unternehmen, an denen die öffentliche Hand unmittelbar oder mittelbar mit mehr als 25 Prozent beteiligt ist, fallen allerdings nicht in den Anwendungsbereich der KMU- sowie SMC-Definition. In Bezug auf die KMU-Empfehlung wurde deshalb eine entsprechende Klarstellung vorgenommen (siehe Art. 2(1) UA. 2 NIS2-Richtlinie). In den Anpassungen der NIS-2-Richtlinie sollte daher klargestellt werden, dass die Klarstellung auch in Bezug auf die SMC-Kategorie gilt. Zudem sollte überdacht werden, für Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste (Art. 3 (1)(c) NIS-2-Richtlinie) einen Verweis auf die höheren Schwellenwerte in der SMC-Definition zu machen. Anderenfalls würden diese Anbieter im Vergleich zu den restlichen Sektoren übermäßig streng reguliert.

Mehrspartenunternehmen nicht benachteiligen

Laut Kommissionsvorschlag sollten Erzeuger von der Definition von **„wesentlichen“ oder „wichtigen“ Einrichtungen** ausgeschlossen werden, deren gesamte Erzeugungsmenge **kleiner oder gleich 1 MW** ist. Nach Ansicht der Kommission wird dadurch die Verhältnismäßigkeit der NIS-2-Richtlinie gewährleistet. Allerdings kann dies erhebliche Auswirkungen auf deutsche kommunale **Mehrspartenunternehmen** mit einer vernachlässigbaren Tätigkeit oder Nebentätigkeit im Bereich der Energiewirtschaft haben. Dies betrifft beispielsweise:

- Betreiber von Müllverbrennungsanlagen, die die Abwärme zur Erzeugung von Energie nutzen.
- Unternehmen der Abwasserwirtschaft. Auf Grund von Art. 11 Abs. 2 der Kommunalwasserrichtlinie (RL/EU 2024/3019) werden Betreiber von Abwasseranlagen zukünftig vermehrt selbst Energie aus erneuerbaren Quellen erzeugen, wie z.B. durch Abwasserwärme. Bereits jetzt wird häufig Klärschlamm

zur Eigenversorgung mit Energie verbrannt. Auch Probeläufe von Notstromaggregaten in Pumpwerken der Abwassertechnik, bei denen die erzeugte Energie in das Netz einspeist wird, wären hiervon betroffen.
- Unternehmen aus allen Sektoren, die auf den Dächern ihrer Betriebsgebäude Solaranlagen installieren.
- Unternehmen, die im Rahmen der kommunalen Wärmeplanung verpflichtet sind, die Bevölkerung mit Fernwärme und -kälte zu versorgen, da Blockheizkraftwerke und Kraft-Wärme-Kopplung-Anlagen als Nebenprodukt Strom erzeugen.

In Deutschland wird die NIS-2-Richtlinie durch das NIS-2-Umsetzungsgesetz in nationales Recht umgesetzt. Hierbei handelt es sich um ein „Artikelgesetz“, das ähnlich wie die Omnibus-Gesetze auf europäischer Ebene eine Vielzahl von einzelnen Gesetzen enthalten. Im Rahmen des NIS-2-Umsetzungsgesetzes werden insbesondere die Betreiber von Energieerzeugungsanlagen in einem sektorspezifischen Gesetz (dem Energiewirtschaftsgesetz) deutlich strenger reguliert, als es die NIS-2-Richtlinie vorgibt. Um eine unverhältnismäßige (Doppel-)Regulierung insbesondere der o.g. Mehrspartenunternehmen unter dem besonders strengen Energiewirtschaftsgesetz zu verhindern, wurden im deutschen Recht flexible Sonderregelungen vorgesehen, die eine solche Regulierung nach dem Energiewirtschaftsgesetz verhindern aber gleichwohl dazu führen, dass diese Unternehmen nach den Vorgaben der NIS-2-Richtlinie reguliert werden. Falls im Rahmen der angepassten NIS-2-Richtlinie Sonderregelungen nur für Betreiber bis zu 1 MW eingeführt werden, besteht die Gefahr, dass Mehrspartenunternehmen erneut in den Anwendungsbereich des Energiewirtschaftsgesetzes fallen. **Dementsprechend sollte die angepasste NIS-2-Richtlinie eine nationale Öffnungsklausel für Mehrspartenunternehmen enthalten**. Anderenfalls könnten kommunale Unternehmen auf Grund der hohen regulatorischen Anforderungen von der sehr effizienten Kombination von Versorgungsleistungen Abstand nehmen.

Überarbeitung des EU-Rechtsakts zur Cybersicherheit

2026/0011 (COD)

Realistische und praktikable Verbote durchsetzen

Der Vorschlag der Kommission für einen neuen horizontalen Rahmen für „nichttechnische“ Risiken in Lieferketten in bestimmten Sektoren (gemäß Anhang I und II der NIS-2-Richtlinie) ist vor dem Hintergrund einer angespannten sicherheits- und geoökonomischen Lage grundsätzlich **nachvollziehbar und als *ultima ratio* gerechtfertigt**: aber zugleich sehr weitreichend und ambitioniert.

Die Vorschläge der Kommission betreffen **IKT der gesamten Wertschöpfungskette** der Kommunalwirtschaft: im Fall der Energiewirtschaft von der Erzeugung über die Steuerung bis hin zur Vermarktung. So benötigen beispielsweise bereits kleine Photovoltaikanlagen Telekommunikationstechnik zur Fernsteuerung und Zustandsüberwachung. Entsprechend wären Phase-Outs mit **viel Kapital** gebunden, welches an anderen Stellen dringend für die Energiewende benötigt wird.

Dementsprechend sollte das Ziel des CSA2 eine realistische **Risikominimierung** sein. Die konkrete Ausgestaltung jeglicher Verbote sollte **praxisnah** sein und unnötige Belastungen für kommunale Unternehmen vermeiden. Der CSA2 soll in dieser Hinsicht u.a. folgende Ansätze verankern, um sicherzustellen, dass die Kommunalwirtschaft Verbote auch umsetzen kann:

- Den Schwerpunkt auf **messbare und überprüfbare Risiken** legen;
- Verbote **möglichst frühzeitig** klarstellen, um **Planungssicherheit** für Investitionen zu gewährleisten;
- Verbote und Austauschpflichten auf **Wirtschafts- und Lebenszyklusanalysen** basieren und – wenn möglich – mit natürlichen **Erneuerungsphasen** synchronisieren, um die Kontinuität der Dienstleistungen zu gewährleisten;
- Realistische **Übergangszeiträume** einführen, vor allem, wenn noch keine oder nur sehr wenige europäische Alternativen auf dem Markt verfügbar sind;
- Kommunale Unternehmen durch **staatliche Förderungen** bei der Umsetzung technischer Sicherheitsmaßnahmen unterstützen;
- **Wirtschaftliche Unterstützung (etwa durch Förderprogramme für Hersteller)** zur Sicherstellung leistbarer Produkte und einer ausreichenden Anbietervielfalt in Europa vorsehen;
- **Finanzielle Entschädigungen oder Schadensersatzansprüche** vorsehen, falls ein Verbot für bereits verbaute Technik, die noch nicht ersetzt werden müsste, ergeht;

- **Abhilfemaßnahmen** näher ausführen (beispielsweise unter **Art. 103(4)(b) und (c)**);
- Eine **freiwillige Positivliste** von sicheren und empfehlenswerten Anbietern in weiteren Leitlinien der Kommission veröffentlichen.

Dementsprechend sollte der Kommissionsvorschlag die Verfügbarkeit nicht-europäischer Anbieter kritischer Komponenten nicht unbegründet einschränken: **insbesondere dort, wo es keine europäischen Alternativen gibt**. Die Kommission berücksichtigt diesen Punkt zwar in **Art. 103(4)(c)**, jedoch sollte dieser Aspekt im weiteren Verfahren verstärkt werden. Aus Sicht der VKU ist eine konsequente **Multi-Vendor-Strategie** erforderlich, um höhere Preise, Lieferengpässe und Sicherheitsbedenken (ein *Single Point of Failure*) zu vermeiden. Für kommunale Unternehmen bleibt eine ausreichende Anbieter- und Preisvielfalt von sicheren IKT-Komponenten entscheidend. Grundsätzlich gilt, dass höhere Kosten infolge einer sehr begrenzten Zahl von sicheren Europäischen Anbieter aus Sicht der Kommunalwirtschaft durch **gezielte Förderprogramme für Hersteller** abgefedert werden könnten.

Hinsichtlich der Durchsetzung des Verbots im **öffentlichen Beschaffungswesens** gemäß **Art. 100(4)(e)** besteht die Gefahr, dass ohnehin schon komplexe Vergabeverfahren für öffentliche Unternehmen weiter erschwert werden und die Beschaffungskosten steigen, was im **Widerspruch zu anderen europäischen Zielen** steht – u.a. die Energiewende und Dekarbonisierung. Positiv hervorzuheben ist, dass das **Vergaberecht nur ein Anwendungszweig unter vielen** ist und die Regelungen des CSA2 über das Vergaberecht hinaus auch nicht-öffentliche Unternehmen erfassen. So können Wettbewerbsverzerrungen zwischen privaten und öffentlichen Unternehmen vermieden werden. Gleichermaßen sollten komplizierte und **unnötige Querverweise** zwischen dem CSA2 und vergaberechtlichen Vorschlägen vermieden werden. Beispielsweise stellt die Kommission im kürzlich vorgelegten ***Industrial Accelerator Act*** (IAA) fest, dass es notwendig sei, Hoch-Risiko-Lieferanten (gemäß CSA2) von der Lieferung kritischer Komponenten an u. a. Bieter in öffentlichen Vergabeverfahren auszuschließen. Dieser Verweis sollte idealerweise gestrichen werden. Die Vorschläge werden parallel verhandelt und es besteht die Gefahr, dass die finalen Gesetzestexte sich widersprechen könnten. Dies führt zu Rechts- und Planungsunsicherheiten und sollte grundsätzlich im Sinne des Bürokratieabbaus vermieden werden.

Öffentliche elektronische Kommunikationsnetze
Kommunale Unternehmen sind Pioniere des Glasfaserausbaus in Deutschland. **Mehr als 220 VKU-Mitgliedsunternehmen** investieren pro Jahr über eine Milliarde Euro in den Breitbandausbau. Als kritische Infrastruktur stellt die Sicherheit öffentlicher elektronischer Kommunikationsnetze ein besonders hohes Gut dar. Der Vorschlag der Kommission, im Digital Networks Act die umfassenden Vorgaben des CSA2 mit der

allgemeinen Genehmigungspflicht zu verknüpfen, sind allerdings sehr weitreichend und ambitioniert. Auch in dieser Hinsicht spricht sich der VKU dafür aus, dass bei der Überprüfung von IKT-Lieferketten in erster Linie technische Kriterien ausschlagend sein sollten. Angesichts der angespannten geopolitischen Lage ist es zwar sinnvoll, auch nicht-technische Risiken zu überprüfen. Etwaige Verbote müssen dennoch praxisnah ausgestaltet werden und umsetzbar bleiben.

Auch mit Blick auf die **Liste der wichtigen IKT-Ressourcen unter anderem für feste elektronische Kommunikationsnetze in Anhang II** ist der Kommissionsvorschlag ambitioniert. Wettbewerbsverzerrungen, steigende Preise und letztlich Verzögerungen beim Ausbau von Glasfasernetzen als der zukunftsfähigen Festnetzinfrastruktur drohen. In diesem Zusammenhang ist im Rahmen der gemäß Art. 110 (4) vorgesehenen Durchführungsrechtsakte eine Orientierung an den **realen Lebenszyklen** der Infrastruktur besonders entscheidend, verbunden mit einer **schrittweisen Umsetzung** etwaiger Verbote.

Nationale Kompetenzen nicht ersetzen

Die vorgeschlagene Erweiterung und Aufstockung der ENISA ist angesichts der wachsenden Cybersicherheitsbedrohungslage durchaus sinnvoll. Im CSA2 muss allerdings sichergestellt werden, dass Sicherheitsanalysen von ENISA schnellstmöglich an **Einrichtungen gemäß Anhang I und II der NIS-2-Richtlinie weitergeleitet** werden und die Kompetenzen von nationalen Behörden nicht ersetzt werden. Nationale Behörden bzw. einheitliche Meldestellen sollten aus Sicht der Kommunalwirtschaft weiterhin der zentrale Ansprechpartner für kritische Infrastrukturen bleiben. Ansonsten droht ein *Single Point of Failure* auf EU-Ebene. In diesem Sinne sollte zudem vermieden werden, dass Parallelstrukturen auf nationaler und europäischer Ebene aufgebaut werden. Ziel jeglicher Meldungen sollte es sein, einen operativen Mehrwert für kritische Infrastrukturen schaffen.

Security-by-Design verankern

Kommunale Unternehmen sind auf sichere IKT-Produkte angewiesen. Daher sollte aus Sicht der Kommunalwirtschaft *Security-by-Design* als Grundelement im **EU-Rahmen für Cybersicherheitszertifizierung (ECCF)** fundiert werden. Der ECCF sollte bestenfalls dazu führen, dass Hersteller von Hard- und Software bereits bei der Entwicklung ihrer Produkte steigende Sicherheitsanforderungen so weit wie möglich berücksichtigen. Diesbezüglich sollte der CSA2 mögliche Preissteigerungen durch **hohe Zertifizierungskosten** berücksichtigen (beispielsweise bei der höchsten Sicherungsstufe „high," die mit erheblichen Gebühren für externe Prüfstellen verbunden ist). Zudem dürfen **hohe Sicherheitsanforderungen** nicht so ausgestalten werden, dass nur sehr wenige Anbieter weltweit in der Lage sind, diese zu erfüllen. Dies würde bereits **schwierige**

Beschaffungsprozesse weiter erschweren. Die Sicherheitsstandards sollten daher praktikabel und für europäische Hersteller realistisch umsetzbar sein.

Doppelregulierung vermeiden und Bürokratie abbauen

Als kritische Infrastrukturen unterliegen kommunale Unternehmen bereits einer Vielzahl an Regularien auf nationaler und europäischer Ebene. In Brüssel kommen mit dem *Industrial Accelerator Act* (IAA), dem *Net Zero Industry Act* (NZIA), sowie dem *Cloud and AI Development Act* (CADA) zahlreiche Anforderungen auf kommunale Unternehmen zu – mit vergleichbaren und teils überschneidenden Zielen wie der CSA2. Im Sinne des Omnibusverfahrens wäre eine bessere Abstimmung mit der NIS-2-Richtlinie und sowie dem *Cyber Resilience Act* (CRA) wünschenswert. Beide Gesetze sind bestmöglich geeignet, eine angespannte Sicherheitslage zu adressieren – insbesondere auf Herstellerseite – und ermöglichen es kommunalen Unternehmen, verlässlich sichere Produkte zu beschaffen. Auf nationaler Ebene sollte wiederum insbesondere eine Doppelung gemäß dem Energiewirtschaftsgesetz in Verbindung mit dem BSI-Gesetz vermieden werden, welches ebenfalls kritische Komponente reguliert.

Bei Rückfragen oder Anmerkungen stehen Ihnen zur Verfügung:

Anna Sophie Kirchmayr
Senior-Referentin mit Schwerpunkt Digitalisierung und Nachhaltigkeitsberichterstattung, Büro Brüssel
Telefon: +32 2 74016-55
E-Mail: kirchmayr@vku.de

Wolf Buchholz
Senior-Fachgebietsleiter Kritische Infrastruktur und Cybersicherheit
Telefon: +49 30 58580-317
E-Mail: buchholz@vku.de

Sören Pinnekamp
Senior-Fachgebietsleiter Telekommunikation
Telefon: +49 30 58580-158
E-Mail: pinnekamp@vku.de