VERBAND KOMMUNALER UNTERNEHMEN e.V.

EMPFEHLUNGEN DER KOMMUNALWIRTSCHAFT

für den EU-Digitalomnibus

Berlin / Brüssel, 08.10.2025

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 309.000 Beschäftigten wurden 2022 Umsatzerlöse von 194 Milliarden Euro erwirtschaftet und mehr als 17 Milliarden Euro investiert. Im Endkundensegment haben die VKU-Mitgliedsunternehmen signifikante Marktanteile in zentralen Ver- und Entsorgungsbereichen: Strom 66 Prozent, Gas 65 Prozent, Wärme 91 Prozent, Trinkwasser 88 Prozent, Abwasser 40 Prozent. Die kommunale Abfallwirtschaft entsorgt jeden Tag 31.500 Tonnen Abfall und hat seit 1990 rund 78 Prozent ihrer CO2-Emissionen eingespart – damit ist sie der Hidden Champion des Klimaschutzes. Immer mehr Mitgliedsunternehmen engagieren sich im Breitbandausbau: 220 Unternehmen investieren pro Jahr über 912 Millionen Euro. Künftig wollen 90 Prozent der kommunalen Unternehmen den Mobilfunkunternehmen Anschlüsse für Antennen an ihr Glasfasernetz anbieten.
Zahlen Daten Fakten 2024
Wir halten Deutschland am Laufen – denn nichts geschieht, wenn es nicht vor Ort passiert: Unser Beitrag für heute und morgen: #Daseinsvorsorge. Unsere Positionen: https://www.vku.de/vku-positionen/

Verband kommunaler Unternehmen e.V. · Invalidenstraße 91 · 10115 Berlin
Fon +49 30 58580-0 · info@vku.de · www.vku.de

DIE KOMMUNALEN UNTERNEHMEN

Das Vorhaben der Kommission, den administrativen Aufwand für Unternehmen schnell und massiv zu reduzieren, um Europas Wettbewerbsfähigkeit zu stärken, ist aus Sicht der Kommunalwirtschaft ausdrücklich begrüßenswert. Wichtig ist, dass auf Vereinfachungsvorschläge schnelle Verhandlungsabschlüsse folgen, um Planungs- und Rechtssicherheit zu gewährleisten. Wichtig ist aber auch, das bestehende Regelwerk spürbar zu vereinfachen, ohne dabei zu deregulieren.

An Ex-ante-Regulierung im Glasfaserausbau festhalten

Überlegungen der EU-Kommission, von der **Ex-ante-Regulierung im Glasfaserausbau abzurücken,** sind in Anbetracht der bestehenden Marktverhältnisse (mindestens) in Deutschland **deutlich verfrüht**. Unverändert verfügt hier der einstige Monopolist über beträchtliche Marktmacht, wie die Bundesnetzagentur als Regulierungsbehörde mehrfach festgestellt hat. Kommunale Unternehmen sind weiterhin vor allem mit der Drohung des Überbaus ihrer Glasfasernetze durch das Unternehmen mit beträchtlicher Marktmacht konfrontiert. Der Vorschlag der Kommission im Weißbuch zum Digital Networks Act, keine Märkte für eine Vorabregulierung zu empfehlen und stattdessen auf den nachgelagerten Drei-Kriterien-Test (Art. 67 Abs. 1 EKEK) zu setzen, ist deswegen mit Blick auf Deutschland völlig unzureichend. Nach dem Drei-Kriterien-Test wird für einen Markt eine Regulierungsbedürftigkeit angenommen, wenn (a) beträchtliche und anhaltende strukturelle, rechtliche oder regulatorische Marktzutrittsschranken bestehen, (b) der Markt hinter den Zutrittsschranken strukturell nicht zu einem wirksamen Wettbewerb tendiert und (c) das Wettbewerbsrecht allein nicht ausreicht, um dem Marktversagen angemessen entgegenzuwirken. Nur mit einer Ex-ante-Regulierung kann Marktmacht aufgebrochen und Wettbewerb gerade im Sinne der Verbraucher geschützt werden.

Überschneidungen im Rechtsrahmen für die Digitalpolitik klarstellen

Die Themenbereiche **Daten**, **Smart Meters** (als Connected Product) und **Cybersicherheit** werden auf EU-Ebene in mehreren Rechtsakten reguliert. Die Vorgaben sind dabei nicht immer kongruent: z. B. sind **Meldepflichten** jeweils unterschiedlich im **Cyber Resilience Act**, der **NIS-2-Richtlinie** und der **DSGVO** geregelt. Außerdem bestehen in vielen Unternehmen bereits **Compliance-Prozesse**, die auf verschiedenen eigenen Regularien basieren (z. B. Informationssicherheit, Datenschutz, technische Konzepte). Diese müssen wiederrum auf Überschneidungen mit der KI-Verordnung geprüft, abgestimmt und angepasst werden. Das Ergebnis ist ein erheblicher bürokratischer Aufwand für die Unternehmen. Der Omnibus sollte deswegen dringend Überschneidungen der Rechtsakte klären und das Zusammenspiel konkretisieren.

Datenregelwerk

Im Bereich der Datenregulierung ist insbesondere das Verhältnis zwischen dem **Data Act**, der **Open-Data-Richtlinie** und der **nationalen Regulierung** (dem deutschen Datennutzungsgesetz, welches die Open-Data-Richtlinie national umsetzt) unklar. Geklärt werden sollte auch, ob der **Data Act** nur dann für Datenverteiler gilt, wenn kein automatisierter Zugang durch den Hersteller besteht.

Erleichterungen auch für kommunale Unternehmen mit mittlerer Marktkapitalisierung („midcaps“) schaffen

Anknüpfend an die europäische KMU-Definition hat die EU-Kommission Vereinfachungen für Unternehmen mit weniger als 750 Beschäftigten und entweder bis zu 150 Mio. Euro Umsatz oder bis zu 129 Millionen Euro Gesamtvermögen vorgeschlagen. Wegen des Verweises auf die KMU-Definition, die Unternehmen, an denen die öffentliche Hand unmittelbar oder mittelbar mit mehr als 25 Prozent beteiligt ist, aus ihrem Anwendungsbereich ausschließt, profitieren kommunale Unternehmen aber nicht von Erleichterungen, die für Unternehmen dieser Größe vorgesehen sind. Das führt zu einer Benachteiligung, vor allem dort, wo sie mit privaten Unternehmen im Wettbewerb stehen. **Der Digitalomnibus muss deswegen auch für kommunale KMU und Midcaps spürbare Erleichterungen in der Datenregulierung schaffen und darf kommunale Unternehmen nicht einseitig weiter mit bürokratischen Hürden belasten**. Gerade im Datenbereich ist ein Level-Playing-Field zwischen öffentlichen und privaten Akteuren besonders wichtig.

Damit auch für kleine und mittlere kommunale Unternehmen sowie kommunale Midcaps effektiv regulatorische und bürokratische Hürden abgebaut werden, muss die Ungleichbehandlung öffentlicher Unternehmen grundsätzlich durch **Artikel 3 Absatz 4 der KMU-Definition** unter **Anhang I der AGVO** aufgehoben werden.

Datensicherheit wahren

Daten kritischer Infrastrukturen und sicherheitsrelevanter Bereiche erfordern einen besonders hohen Schutz und dürfen keinesfalls geteilt werden. Hier würde eine Vereinfachung der einschlägigen Regeln mehr schaden als nützen. Gemäß Artikel 13 Absatz 1 der aktuellen INSPIRE-Richtlinie hat Deutschland eine Ausnahme für die Datenlieferung von kritischen Infrastrukturen, wenn dieser Zugang nachteilige Auswirkungen auf die öffentliche Sicherheit hätte. Diese Ausnahme muss auf EU-Ebene weiter bestehen, besonders angesichts der derzeitigen geopolitischen Spannungen und der anhaltenden Bedrohungen für die Sicherheit Europas. Angesichts der veränderten und verschärften geopolitischen Lage erscheint eine kritische Überprüfung der Informationsrechte sinnvoll.

Beim EU-Datengesetz (Data Act) nicht zurückrudern

Als zugleich Datenempfänger und Dateninhaber ist das Teilen von Daten von entscheidender Bedeutung für kommunale Unternehmen. Zum einen ist es unerlässlich, dass Datenbereitstellungspflichten nicht einseitig öffentliche Unternehmen adressieren. Zum anderen sollten die Kosten und Risiken der Datengenerierung nicht allein beim Dateninhaber liegen. **Der Data Act bietet eine solide Grundlage für das Teilen von Daten.** Auch die Bestimmungen zum Cloud-Switching für Rechenzentren sollten nicht zurückgenommen werden. Die Kommunalwirtschaft braucht diese klaren rechtlichen Vorgaben und technisch einfachen Prozesse. Ein Rückschritt bei dieser Regulierung (etwa durch die Einführung eines rein freiwilligen Rahmens für Unternehmen) würde erhebliche Rechts- und Planungsunsicherheit verursachen. Stattdessen ist ein Level-Playing-Field mit klaren Regeln gefragt.

Verordnung über Künstliche Intelligenz (AI-Act)

Stop-the-clock umsetzen

Der VKU verfolgt die Diskussionen um eine Verschiebung des Inkrafttretens der Regelungen des AI-Acts. Eine z. B. **zweijährige Verschiebung** (v. a. im Hinblick auf Hoch-Risiko-KI-Systeme, deren Vorschriften ab August 2026 bereits in Kraft treten sollen) würde den bestehenden Planungen kommunaler Unternehmen nicht widersprechen. Für den Fall, dass inhaltliche Anpassungen zur Diskussion stehen, ist es definitiv sinnvoll, **Zeit für die Verhandlungen** zwischen den Institutionen über den Omnibus-Vorschlag zu schaffen. Andernfalls drohen Verwirrung sowie Rechts- und Planungsunsicherheit.

Trotzdem sind schnelle Verhandlungsschlüsse gefragt. Konkret wären eine Vereinfachung und Konkretisierung der Vorschriften für **kritische Infrastrukturen** wichtig. Auch die Leitlinien für die praktische Umsetzung der Vorschriften über wesentliche Änderungen sollten zeitnah veröffentlicht werden, um Unternehmen wiederum Zeit für die Umsetzung der Pflichten zu erlauben.

Zu Art. 3 Nr. 14 – Präzisierung der Definition von „Sicherheitsbauteil“

Es sollte klargestellt werden, unter welchen Bedingungen KI-Komponenten in kritischen Infrastrukturen (z. B. Drucksensoren in Wasserversorgungssystemen, autonome Kontrollroboter in Kraftwerken, intelligente Kameras mit Bilderkennung) als „Sicherheitsbauteil“ (Art. 3 Nr. 14 KI-VO) gelten. In diesem Zusammenhang ist ebenfalls zu spezifizieren, was in der Legaldefinition von „Sicherheitsbauteil“ unter der Erläuterung „Bestandteil eines Produkts oder KI-Systems“ zu verstehen ist.

Zu ErwGr 55 – Abgrenzung zwischen Cyber- und physischer Sicherheit

In Erwägungsgrund 55 KI-VO ist erläutert, dass Komponenten, die für die ausschließliche Verwendung zu Zwecken der Cybersicherheit vorgesehen sind, nicht als Sicherheitsbauteile gelten. Die Unterscheidung zwischen Cybersicherheit und physischer Sicherheit ist jedoch nicht in jedem Fall trennscharf möglich. Oftmals haben Cyberangriffe direkte physische (Sicherheits-)Auswirkungen. An dieser Stelle sollte genauer beschrieben werden was unter „die ausschließliche Verwendung zu Zwecken der Cybersicherheit“ fällt. Auch ist es notwendig, die Frage der Erheblichkeit einer Störung im Sinne von Erwägungsgrund 55 näher zu bestimmen.

Zu Art. 25 – Klarheit zu Anbieter- vs. Betreiber-Rolle und „wesentlichen Änderungen“

Unklar ist derzeit noch, in welchen Fällen man nach Art. 25 Abs. 1 KI-VO im Falle von GPAI-Systemen von der Betreiber- in die Anbieterrolle wechselt, da die Kritikalität von GPAI-Systemen vom jeweiligen Anwendungsfall abhängt und sich oftmals nicht von vornherein bestimmen lässt. Wichtig ist in diesem Zusammenhang auch eine Bewertung, wie der grundsätzliche Einsatz von GPAI im Bereich der Personalabteilung einzustufen ist. Wird ein Betreiber, der ein GPAI-System mit begrenztem Risiko konzernweit einsetzt durch Art. 25 Abs. 1 lit. c KI-VO zum Anbieter eines Hochrisiko-KI-Systems, wenn er das System (auch) den Mitarbeitenden der Personalabteilung zur Verfügung stellt? Und wenn ja, welche Maßnahmen würden diese Konsequenz vermeiden können? Auch ist grundsätzlich für Klärung zu sorgen, wann im Einzelfall eine „wesentliche Veränderung” des KI-Systems anzunehmen ist, durch die der bisherige Betreiber selbst zum Anbieter wird.

EU-Datenschutzgrundverordnung (DSGVO)

Die Datenschutzgrundverordnung gehört zu den Bestandteilen der Regulatorik im Bereich Digitalisierung, die auch für kommunale Unternehmen mit erheblichem bürokratischem Aufwand verbunden ist. Im Folgenden unterbreiten wir konkrete Vorschläge, an welchen Stellen die DSGVO aus Sicht der Kommunalwirtschaft angepasst werden sollte.

Fehlen eines Konzernprivilegs in der DSGVO

Vorschlag zur Änderung

Ergänzung:

„Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind, sind berechtigt, personenbezogene Daten innerhalb der Unternehmensgruppe insbesondere für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln, es sei denn überwiegende schutzwürdige Interessen der betroffenen Personen stehen dem entgegen. Voraussetzung hierfür ist,

dass innerhalb der Unternehmensgruppe ein dem Risiko für die Rechte und Freiheiten der betroffenen Personen angemessenes einheitliches Schutzniveau gewährleistet ist.“

Begründung
Der Datenaustausch zwischen Gesellschaften eines Konzerns (z. B. Tochtergesellschaften) unterliegt im Grunde denselben Anforderungen wie ein Austausch mit Dritten (z. B. externen Unternehmen). Dies führt zu einen erheblichen Prüf- und Dokumentationsaufwand, trotz zentralem Compliance- und Datenschutzmanagement.

Zu Art. 12 – Datenschutzhinweise/umfassende Informationspflichten

Vorschlag zur Änderung
Die Pflicht zur Erstellung von Datenschutzhinweisen auf das Wesentliche zu reduzieren, vor allem den inhaltlichen Umfang zu reduzieren und eine einheitliche Umsetzung in der Praxis fördern.

Begründung
Datenschutzhinweise sind aufgrund hoher inhaltlicher Anforderungen häufig sehr umfangreich. Inhaltliche Richtigkeit und Vollständigkeit steht oft gegen Transparenz und Verständlichkeit. In der Praxis werden Datenschutzhinweise nicht oft gelesen: aufgrund ihrer Komplexität und ihres abschreckenden Umfangs. Es wäre wünschenswert, die Pflichtangaben zu vereinfachen. Dies würde die Verständlichkeit und Transparenz für Nutzerinnen und Nutzer deutlich verbessern.

Zu Art. 15 Abs. 1 lit. c – Auskunftsersuchen

Vorschlag zur Änderung
Streichung:
„(1) …. c) die ~~Empfänger oder~~ Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen; …“

Ergänzung:
„Verarbeitet der Verantwortliche eine große Menge an personenbezogenen Daten über die betroffene Person, kann er von der betroffenen Person verlangen zu präzisieren, auf welche Informationen oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht, bevor er ihr Auskunft erteilt. Gleiches gilt für personenbezogene Daten, die zum Zwecke der Datensicherheit, wie z. B. IT-Logdaten, verarbeitet werden.“

„Die Absätze 1 bis x finden keine Anwendung, wenn und soweit
a) die betroffene Person mit dem Auskunftsrecht andere Zwecke verfolgt, als sich der Verarbeitung sie betreffender personenbezogener Daten bewusst zu sein und deren Rechtsmäßigkeit zu überprüfen.

b) der betroffenen Person durch die Information ein Betriebs- oder Geschäftsgeheimnis des Verantwortlichen oder eines Dritten offenbart würde und das Interesse an der Geheimhaltung das Interesse der betroffenen Person an der Information überwiegt."

Begründung
Die Erfüllung von Datenauskunftsersuchen stellt in langjährigen Geschäftsbeziehungen und Arbeitsverhältnissen einen hohen Aufwand dar. Grund dafür sind große Datenmengen, die aus unterschiedlichen Quellen zu extrahieren sind. Zum Umfang der Kopie personenbezogener Daten liegen unterschiedliche Rechtsmeinungen auf europäischer und nationaler Ebene vor. Nach aktueller Rechtsprechung des Bundesgerichtshofs sind von der Person verfasste Dokumente oder Schriftstücke in ihrer Gesamtheit personenbezogene Daten, auch wenn sie der Person bereits bekannt sind. Der Mehrwert ist hier nicht klar ersichtlich.

Auch eine mögliche/vermeintliche Pflicht zur namentlichen Angabe aller tatsächlichen Empfänger inkl. eingesetzter Sub-Dienstleister führt zu erheblichem Dokumentationsaufwand. Im IT-Bereich ist es üblich, mehrere Dienstleister zu beauftragen und zu wechseln. Es ist sehr schwierig, den eingesetzten (Sub-)Dienstleister, Zeitraum und Zuordnung zu dokumentieren. Auch diesbezüglich ist der Mehrwert fraglich, insbesondere wenn es sich um Auftragsverarbeiter handelt, die auf Weisung des Auftraggebers als verantwortliche Stelle handeln. In diesen Fall besteht kein Auskunftsanspruch gegenüber dem Auftragsverarbeiter. Daher wird der Auftragsverarbeiter die betroffene Person wieder an den Auftraggeber als verantwortliche Stelle verweisen.

Außerdem ist zunehmend zu beobachten, dass Auskunftsersuchen zur Erreichung von datenschutzfremden Zielen genutzt werden. Beispiele hierfür sind Differenzen im Arbeitsverhältnis (Ausforschung), Einstellungsverfahren oder andere Differenzen (z. B. Forderungen nach Gutschriften oder Erlass von erhöhtem Beförderungsentgelt). Das Recht wird in solchen Fällen als Druckmittel genutzt.

Zu Art. 26 – Joint Control/gemeinsame Verantwortlichkeiten

Vorschlag zur Änderung
Streichung:
Art. 26 soll gänzlich abgeschafft werden.

Begründung
Die Erstellung und Aktualisierung solcher Vereinbarungen ist mit erheblichem Aufwand verbunden, insbesondere im Mehr-Parteienverhältnis. Auch der Anwendungsbereich ist unklar und in der Praxis schwer handhabbar. Die Auslegungen auf EU-Ebene und Aufsichtsbehörden sind sehr weit gefasst und konturlos. In der Praxis kann das

Anschließen an von Dritten festgelegten Mitteln und Zwecken zu einer gemeinsamen Verantwortlichkeit führen, auch bei extern beauftragten Dienstleistungen. Daher soll dieser Artikel bestenfalls gelöscht werden, insbesondere angesichts der ohnehin bestehenden Datenschutzpflichten jedes Beteiligten. Ein JCA bietet hier keinen Mehrwert.

Zu Art. 30 – Verarbeitungsverzeichnis/Umfassende Dokumentationspflichten

Vorschlag zur Änderung
Streichung:
Verarbeitungen mit sehr geringem Risiko von der Eintragungspflicht in einem Verarbeitungsverzeichnis ausnehmen.

Begründung
Die Dokumentation jeder Datenverarbeitung (auch bei sehr geringem Risiko) führt zu erheblichem Aufwand ohne erkennbaren Mehrwert. Bei einem sehr geringen Risiko sollen die Mindestinhalte deutlich reduziert oder idealerweise darauf verzichtet werden.

Zu Art. 33 – Meldepflicht von 72 Stunden bei Risiko / Datenschutzverletzungen

Vorschlag zur Änderung
Streichung:
Meldepflicht bestenfalls gänzlich abschaffen.
Ergänzung:
Mindestens eine Konkretisierung und Beschränkung der Meldepflicht auf gravierende Datenschutzverletzungen.
„(1) [1] Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, **es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führt**.

[2] Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr **eine Begründung für die Verzögerung beizufügen**. Bei der Berechnung der Frist sind **Feiertage, Sonntage und Samstage nicht zu berücksichtigen**."

Begründung
Die Frist der Meldepflicht ist zu kurz bemessen. In Worst-Case-Szenarien (z. B. Hackerangriffe) sind Ressourcen für die Analyse und Ergreifung von Abhilfemaßnahmen dringend benötigt. Gleichzeitig ist eine Prüfung der Meldepflicht und ggf. Erstellung der Meldung gefragt. Das ist ein komplexer Prozess, auch aufgrund immer komplexerer

(technischer) Zusammenhänge und uneinheitlicher Positionierung der Aufsichtsbehörden. Zum Schutz der betroffenen Personen sollten Ressourcen besser in die Analyse und Definition der Abhilfemaßnahmen investiert werden. Ein konkreter Mehrwert der Meldung ist nicht erkennbar – insbesondere, wenn Rückmeldungen der Aufsichtsbehörden sich in der Regel lediglich auf formale Aspekte beschränken.

Für Rückfragen stehen Ihnen zur Verfügung:

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