VERBAND KOMMUNALER UNTERNEHMEN e.V.

STELLUNGNAHME

zum Referentenentwurf des Bundesministeriums des Innern: Gesetz zur Anpassung von Transparenz-, Veröffentlichungs- und Informationspflichten zum angemessenen Schutz kritischer Infrastrukturen

Berlin, 17.11.2026

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.

DIE KOMMUNALEN UNTERNEHMEN

Der VKU bedankt sich für die Möglichkeit, zum „Gesetz zur Anpassung von Transparenz-, Veröffentlichungs- und Informationspflichten zum angemessenen Schutz kritischer Infrastrukturen“ (Transparenzanpassungsgesetzes) des Bundesministeriums des Innern Stellung zu nehmen.

Bedeutung des Vorhabens für kommunale Unternehmen

Der Verband kommunaler Unternehmen (VKU) vertritt rund 1.600 kommunalwirtschaftliche Unternehmen in den Bereichen Energie, Wasser/Abwasser, Abfallwirtschaft sowie Telekommunikation. Bei einer Vielzahl dieser Unternehmen handelt es sich um Betreiber von kritischen Anlagen, die insbesondere auf Grund des Kritis-Dachgesetzes dazu verpflichtet sind, ein angemessenes Sicherheitsniveau zu erreichen.

Positionen des VKU in Kürze

- Die Überarbeitung der Transparenz-, Veröffentlichungs- und Informationspflichten ist zu begrüßen. Die Abwägung zwischen Offenheit und Sicherheit muss auf Grund der neuen Bedrohungslage neu bewertet werden.
- Es ist dringend eine zentrale Steuerung des Schutzes kritischer Infrastrukturen auf Bundesebene notwendig. Insbesondere dürfen die hier vorgeschlagenen Anpassungen von Transparenz-, Veröffentlichungs- und Informationspflichten nicht Stückwerk bleiben, sondern müssen konsequent und zentral gesteuert über eine Vielzahl von Gesetzen einheitlich umgesetzt werden.
- Kritische Infrastrukturen müssen als besonderes Schutzgut anerkannt werden. Hierfür muss festgelegt werden, dass der Schutz von kritischen Infrastrukturen im überragenden öffentlichen Interesse liegt.
- Die Änderungen im Informationsfreiheitsgesetz werden begrüßt, bedürfen aber noch Anpassungen im Detail. Insbesondere müssen die Infrastrukturen unterhalb der Kritis-Schwellenwerte konsequent und für die Praxis handhabbar identifiziert und geschützt werden.
- Auch bereits auf Datenplattformen veröffentlichte Infrastrukturen müssen einer erneuten Überprüfung unterzogen werden. Falls die Schutzinteressen der Betreiber überwiegen, braucht es einen Anspruch auf Entfernung der auf den Datenplattformen hinterlegten Informationen.

Stellungnahme

I. Überarbeitung der Transparenz-, Veröffentlichungs- und Informationspflichten ist zu begrüßen

Die Überarbeitung der Transparenz-, Veröffentlichungs- und Informationspflichten entspricht einer langjährigen Forderung des VKU. **Die Erarbeitung des Transparenzanpassungsgesetzes wird deshalb ausdrücklich begrüßt und geht inhaltlich auch in die richtige Richtung.**

Vollkommen richtig wird auf die veränderte geopolitische Bedrohungslage, sowie die besseren technische Möglichkeiten der Informationsgewinnung und -auswertung (insbesondere durch den Einsatz von künstlicher Intelligenz) hingewiesen. Unter Einsatz von künstlicher Intelligenz ist es im Moment mit geringstem Aufwand möglich, anhand von öffentlichen verfügbaren Informationen die neuralgischen Punkte von kritischen Infrastrukturen zu identifizieren und für eine Anschlagsplanung zu nutzen.

Vor diesem Hintergrund muss die Abwägung zwischen Offenheit und Sicherheit neu bewertet werden. Es geht selbstverständlich nicht darum Transparenz-, Veröffentlichungs- und Informationspflichten generell abzuschaffen. Den berechtigen Anliegen der Zivilgesellschaft oder auch Unternehmen (z.B. Abfragen von Tiefbauunternehmen zu Leitungsinfrastrukturen, damit bei Bauarbeiten keine Leitungen beschädigt werden) soll und muss auch weiterhin Rechnung getragen werden. Es muss sich allerdings kritisch die Frage gestellt werden, wer genau welche Informationen wirklich benötigt.

Die Einschränkung der Transparenzpflichten wird nicht dazu führen, dass eine Anschlagsplanung zukünftig unmöglich ist, denn dafür sind viele Infrastrukturen deutlich zu einfach von öffentlichem Grund aus einsehbar. Allerdings handelt es sich um einen wichtigen Baustein, um die Gesamtresilienz Deutschlands zu steigern.

Auch feindliche Kräfte haben nur begrenzte Ressourcen zur Verfügung (z.B. in Form von Low-Level-Agenten / Wegwerf-Agenten) und die Einschränkung der Transparenzpflichten führt dazu, dass diese Kräfte mehr Ressourcen investieren müssen, um Anschläge zu planen. Deshalb führt der regelmäßige Hinweis darauf, dass die Informationen schon verfügbar seien (weil bereits im Internet veröffentlicht oder weil die Infrastrukturen von öffentlichem Grund aus einsehbar sind) ins Leere. Es macht einen deutlichen Unterschied, ob eine Person durch Deutschland fahren muss, um Infrastrukturen zur Anschlagsplanung auszuspionieren oder ob er dies automatisiert durch weiterhin im Internet auffindbare Informationen tut. Zudem kann so verhindert werden, das zukünftige Informationen über kritische Infrastrukturen überhaupt jemals im Internet landen.

Die Idee hinter der Einschränkung der Transparenzpflichten ist vergleichbar mit dem Abschließen eines Hauses: Mit genug Aufwand kann weiterhin in das Haus eingebrochen

werden. Dies führt trotzdem nicht dazu, dass wir unsere Häuser nicht abschließen oder dem Einbrecher den Schlüssel freiwillig aushändigen.

II. Zentrale Steuerung des Kritis-Schutzes notwendig

Das Transparenzanpassungsgesetz umfasst sehr wichtige gesetzliche Anpassungen im Hinblick auf die Transparenz-, Veröffentlichungs- und Informationspflichten. Allerdings existiert noch eine sehr hohe Zahl von weiteren gesetzlichen Regelungen, die ebenfalls solche Pflichten festlegen und entsprechend geprüft werden müssen. Dies macht der Gesetzesentwurf auch transparent. Denn es wird darauf hingewiesen, dass alle Ressorts fortlaufend weiteren rechtlichen Anpassungsbedarf und Möglichkeiten prüfen, veröffentlichte Daten zu löschen sowie europarechtliche Anpassungen vorzunehmen. Diese weiteren gesetzlichen Regelungen sind nicht Teil dieser Stellungnahme, da sie häufig außerhalb der Federführung des Bundesinnenministeriums liegen und den Umfang dieser Stellungnahme sprengen würden.

Allerdings zeigt sich hier ein generelles Problem: Es findet anscheinend keine zentrale bzw. ressortübergreifende Steuerung des Schutzes der kritischen Infrastrukturen auf Bundesebene statt. **Es wird gefordert, dass eine zentrale Stelle auf Bundesebene die Steuerung des Schutzes der kritischen Infrastrukturen ressortübergreifend übernimmt.** Diese bisher fehlende Steuerung ist auch in sonstigen Bereichen der Kritis-Gesetzgebung ein Problem, wird aber anhand der Anpassung der Transparenz-, Veröffentlichungs- und Informationspflichten nochmals deutlich.

Zum einen wissen die anderen Ressorts häufig nichts von gesetzlichen Anpassungen in anderen Bereichen. Beispielhaft kann hier auf die Änderung des § 79 Absatz 3 Satz 1 Nummer 4 TKG durch das TKG-Änderungsgesetz[1] hingewiesen werden (Bereitstellung von Informationen über kritische Anlagen an Dritte über das Gigabit-Grundbuch). Der dortige Wortlaut unterscheidet sich deutlich von dem hier vorliegenden Transparenzanpassungsgesetz sowie von der Grundregel des neuen § 30 VwVfG. Diese Diskrepanz hat der VKU auch bereits im Gesetzgebungsverfahren in seiner Stellungnahme[2] angemerkt.

Ohne eine zentrale Stelle auf Bundesebene zur Steuerung des Schutzes der kritischen Infrastrukturen werden die Verbände und andere maßgeblichen Stakeholder nicht systematisch eingebunden in die Kritis-Gesetzgebung bzw. die Anpassungen der weiteren Transparenzregelungen. Beispielhaft deutlich wird dies durch den Hinweis auf die in der Abstimmung befindlichen Änderungen von Transparenz-, Veröffentlichungs- und Informationspflichten im „Entwurf eines Gesetzes zur Modernisierung des Städtebau- und Raumordnungsrechts.“[3] Ohne diesen Hinweis wären wohl die meisten Verbände und Unternehmen nicht davon ausgegangen, dass hier ebenfalls Änderungen von Transparenz-,

[1] BT-Drs. 21/8277.
[2] https://www.vku.de/vku-positionen/kommunaler-breitbandausbau/vku-stellungnahme-zum-entwurf-der-bundesregierung-fuer-ein-tkg-aenderungsgesetz-2026/.
[3] BT-Drs. 21/6588.

Veröffentlichungs- und Informationspflichten vorgenommen werden. Es ist davon auszugehen, dass sich dies wiederholen wird, wenn jedes Bundesressort ohne zentrale Steuerung Transparenzpflichten anpasst.

III. Änderung der Länderregelungen anstoßen

Neben der Vielzahl der noch zu überprüfenden Bundesregeln müssen auch die Transparenz-, Veröffentlichungs- und Informationspflichten der Länder überprüft und angepasst werden. Die Mehrzahl der Verwaltungsverfahren werden z.B. nach den Verwaltungsverfahrensgesetzen der Länder geführt, sodass der in Bezug genommene § 30 VwVfG auch in den Bundesländern umgesetzt werden muss. Gleiches gilt z.B. auch für die Informationsfreiheitsgesetze der Länder. Ohne eine Umsetzung auf Länderebene ist durch die Änderung der Bundesgesetze nicht viel gewonnen. Zumindest für die Mitglieder des VKU sind ganz überwiegend die Informationsfreiheitsgesetze der Länder maßgeblich.

Um hier ein zügiges und einheitliches Vorgehen der Länder sicherzustellen, muss der Bund das Thema auch mit Nachdruck bei den Ländern platzieren. Dies könnte z.B. im Rahmen der Innenministerkonferenz passieren.

IV. Kritische Infrastrukturen / Anlagen als besonderes Schutzgut anerkennen

Viele Normen, die Transparenz-, Veröffentlichungs- und Informationspflichten statuieren, verlangen die Abwägung gegenläufiger Interessen. **Der VKU fordert, den Schutz kritischer Infrastrukturen / Anlagen als überragendes öffentliches Interesse gesetzlich zu verankern.** Dies würde die Schutzinteressen der kritischen Infrastrukturen / Anlagen ganz maßgeblich in allen diesen Normen stärken. Zudem würde dies auch die Abwägungsentscheidungen in anderen Verwaltungsnormen zugunsten des Schutzes der kritischen Infrastrukturen / Anlagen positiv beeinflussen. Die Auswirkungen sind vielfältig und erstrecken sich über eine Vielzahl von Rechtsgebieten. Für die entsprechende Norm im Telekommunikationsrecht (§ 1 Abs. 1 S. 2 TKG) hat das Bundesministeriums für Digitales und Staatsmodernisierung eine entsprechende Handreichung veröffentlicht.[4]

So richtig es ist, den Ausbau von öffentlichen Telekommunikationsnetzen in das überragende öffentliche Interesse zu stellen, desto befremdlicher erscheint es, dass der Schutz der kritischen Infrastrukturen / Anlagen dies nicht bereits ist. Es drängt sich ein deutlicher Wertungswiderspruch auf, wenn der Ausbau öffentlicher Telekommunikationsnetze als wichtiger angesehen wird, als der Schutz der kritischen Infrastrukturen / Anlagen, insbesondere wenn man dies im Zusammenhang mit der Landes- bzw. Bündnisverteidigung sieht. Im Bundeswehr-Infrastrukturbeschleunigungsgesetz[5] wird im Zusammenhang mit

[4] Siehe: https://bmds.bund.de/themen/digitale-infrastrukturen/telekommunikationsrecht-und-sicherheit/tkg-das-ueberragende-oeffentliche-interesse.
[5] BT-Drs. 21/8409.

der Landes- und Bündnisverteidigung ein überragendes öffentliches Interesse für den Bau und Betrieb gewisser Infrastrukturen vorgesehen (§ 4 Bundeswehrbaugesetz).

Das Gesetzgebungsverfahren zum Transparenzgesetz bietet somit politisch eine gute Möglichkeit, den Schutz der kritischen Infrastrukturen / Anlagen nochmals besonders zu akzentuieren und gegenüber den Bürgern und der Verwaltung besonders herauszustellen.

§ 1a KRITIS-Dachgesetz
Maßnahmen zur Steigerung der Resilienz von Infrastrukturen,

1. die durch Gesetz oder aufgrund eines Gesetzes als kritische Anlage bestimmt worden sind oder
2. die besonders schutzbedürftig zur Wahrung der öffentlichen Sicherheit sind,

liegen im überragenden öffentlichen Interesse. Im Verhältnis zu anderen im überragenden öffentlichen Interesse liegenden Belangen ist im Einzelfall abzuwägen, welcher Belang Vorrang hat.

V. Schutz über den gesamten Datenlebenszyklus gewährleisten

Der Schutz kritischer Infrastrukturen darf nicht erst bei der Veröffentlichung sicherheitsrelevanter Informationen einsetzen. Bereits ihre Erhebung, Übermittlung, Zusammenführung und zentrale Speicherung können zusätzliche Risiken schaffen. Dies gilt insbesondere für Datenbestände, die Informationen verschiedener Unternehmen, Infrastruktursektoren oder Verwaltungsebenen verbinden und dadurch ein sektorübergreifendes Lagebild ermöglichen. Häufig müssen die Mitgliedsunternehmen des VKU beispielsweise sehr sensible Informationen an staatliche Stellen herausgeben, wobei vollkommen unklar ist, wie diese Informationen durch die staatlichen Stellen gesichert werden. Als Beispiel wird auf den Cyberangriff auf das Berliner Landesnetz im August 2026 hingewiesen, infolgedessen nach unseren Informationen auch äußerst sensible Daten von Mitgliedsunternehmen des VKU abgeflossen sind.

Es wird deshalb gefordert, dass staatliche Stellen mindestens für sicherheitsrelevante Infrastrukturdaten verbindlichen Vorgaben zur Datenminimierung, Zweckbindung, sicheren Übermittlung, Speicherung, Zugriffssteuerung und Löschung unterliegen und diese Vorgaben auch nachweisbar einhalten.

VI. Bereits veröffentlichte Infrastrukturdaten überprüfen und erforderlichenfalls entfernen

Ein wirksamer Schutz kritischer Infrastrukturen darf sich nicht auf künftige Veröffentlichungen beschränken. Zahlreiche sicherheitsrelevante Informationen sind bereits auf

Internetseiten, in Registern, Planungsunterlagen, Datenportalen und Archiven öffentlich verfügbar. Durch verbesserte Möglichkeiten zur automatisierten Recherche, Verknüpfung und Auswertung kann sich die Sicherheitsrelevanz auch älterer Datenbestände nachträglich erhöhen.

Bund, Länder und zuständige Behörden sollten verpflichtet werden, bestehende Veröffentlichungen und öffentlich zugängliche Datenbestände regelmäßig auf ihre aktuelle Sicherheitsrelevanz zu überprüfen. Ergibt die Prüfung, dass Informationen allein oder in Verbindung mit weiteren Datenquellen ein Sicherheitsrisiko begründen, müssen sie nachträglich entfernt, anonymisiert, aggregiert oder in ihrer Detailtiefe reduziert werden können. **Betreiber kritischer oder besonders schutzbedürftiger Infrastrukturen müssen einen ausdrücklichen gesetzlichen Anspruch erhalten, mit dem sie die Überprüfung und erforderlichenfalls die Entfernung sicherheitsrelevanter Informationen gegenüber staatlichen Stellen oder auch privaten Anbietern von Informationsplattformen erzwingen können.**

VII. Änderung des Informationsfreiheitsgesetzes

Wie aus der Gesetzesbegründung hervorgeht, wird sich für die Änderung des § 3 IFG an dem neuen § 30 VwVfG orientiert. Es wird ausdrücklich begrüßt, dass die dort eingebrachte allgemeine Grundregel auch auf das hier vorliegende Transparenzgesetz übertragen werden soll.

Wichtig ist allerdings, dass es nicht zu einer Abweichung im Wortlaut der maßgeblichen Regelungen kommt, denn anderenfalls wird in der Praxis die Frage gestellt, ob die Auslegung auch eine andere sein soll. So bezieht § 30 Nr. 2 VwVfG z.B. neben der öffentlichen Sicherheit auch die Funktionsfähigkeit der Infrastruktur in die Abwägung ein, während bei § 3 Nr. 9 IFG-RefE nur die öffentliche Sicherheit in die Abwägung einbezogen wird. **Ggf. erfordert dies eine Anpassung des § 30 VwVfG.**

Die neue Regelung des § 3 Nr. 9 IFG-RefE schließt den Anspruch auf Informationszugang in zwei Varianten aus: Hinsichtlich kritischer Infrastrukturen (Var. 1) und hinsichtlich sonstiger besonders schutzbedürftiger Infrastrukturen (Var. 2). In beiden Varianten besteht Anpassungsbedarf.

1. Ausschluss kritischer Infrastrukturen (§ 3 Nr. 9 Var. 1 IFG-RefE)

Hinsichtlich Infrastrukturen, die durch Rechtsvorschrift als kritische Infrastruktur bestimmt worden sind, schränkt § 3 Nr. 9 Var. 1 IFG-RefE den Informationsanspruch ein. Laut Gesetzesbegründung fallen unter den Begriff der kritischen Infrastruktur zum Beispiel die im BSIG und Kritis-Dachgesetz als kritische Anlagen definierten Infrastrukturen (S. 20). Es verbleibt unklar, warum im Gesetzeswortlaut nicht schlicht der Begriff der kritischen Anlage gewählt wird. Der Begriff der kritischen Infrastruktur wurde im Zuge der Anpassungen über das Kritis-Dachgesetz einheitlich in den Begriff der kritischen Anlage

geändert. **Der Begriff der kritischen Infrastruktur sollte also durch den Begriff der kritischen Anlage im Gesetzestext ersetzt werden. In der Gesetzesbegründung sollte darauf hingewiesen werden, dass hiermit kritische Anlage im Sinne von § 2 Nr. 3 Kritis-DachG iVm. § 5 Kritis-DachG gemeint sind** (siehe auch der Verweis in § 2 Nr. 22 BSIG). So wird eindeutig geregelt, was unter diese Norm fällt.

Es ist zudem davon auszugehen, dass nicht nur die kritischen Anlagen gemeint sind, die durch Rechtsverordnung (BSI-Kritisverordnung bzw. die zukünftige Kritisverordnung nach § 5 Abs. 1 Kritis-DachG) definiert werden, sondern auch solche kritischen Anlagen, die durch Einzelfallentscheidung (Verwaltungsakt) als solche bestimmt werden (vgl. § 5 Abs. 3-7 Kritis-DachG). Dass die kritischen Anlagen / Infrastrukturen nur durch Rechtsvorschrift (also wohl nicht durch Einzelfallentscheidung / Verwaltungsakt) bestimmt werden, ist wohl einem Redaktionsversehen geschuldet. **Er wird gefordert, dass die kritischen Anlagen durch Gesetz oder aufgrund eines Gesetzes bestimmt worden sind.** Diese Formulierung wird auch vom TKG-Änderungsgesetz[6] in § 79 Abs. 3 Nr. 4 TKG-RegE gewählt.

2. Sonstige besonders schutzbedürftige Infrastrukturen (§ 3 Nr. 9 Var. 2 IFG-RefE)

In Bezug auf Infrastrukturen, die besonders schutzbedürftig zur Wahrung der öffentlichen Sicherheit sind, schränkt § 3 Nr. 9 Var. 2 IFG-RefE den Informationsanspruch ein.

Die Grundidee, Infrastrukturen / Anlagen auch unterhalb der Kritis-Schwellenwerte zu schützen ist richtig, muss aber noch weiter ausdifferenziert werden.

Die Gesetzesbegründung gibt keine systematischen Anhaltspunkte, welche Infrastrukturen damit gemeint sein können. Es werden in der Gesetzesbegründung lediglich eine Vielzahl von einzelnen Infrastrukturen aufgezählt, die erfasst sein können, ohne die Frage zu beantworten, ob sie es auch sind. Ohne Anspruch auf Vollständigkeit sollte in der Gesetzesbegründung klargestellt werden, dass die **folgenden Eigenschaften der Infrastrukturen maßgeblich sind für die Abwägung**:

- Betrieb der Infrastruktur durch größenunabhängig regulierten Betreiber von Energieversorgungsnetzen (§ 5c Abs. 1 Nr. 1 EnWG) oder von öffentlichen Telekommunikationsnetzen (§ 165 Abs. 2 TKG);
- Betrieb der Infrastruktur durch ein Unternehmen, das durch das NIS2-Umsetzungsgesetz reguliert ist (also insbesondere besonders wichtige und wichtige Einrichtungen nach § 28 BSIG)
- Die Infrastruktur wurde unternehmensintern identifizierte und klassifiziert als besonders schutzbedürftig. Ggf. kann sich an der Logik der Identifizierung von Schwachstellen in Verteilnetzen orientiert werden, so wie sie gerade durch die Verbände / Behörden / Ministerien erarbeitet werden.
- Infrastrukturen in Zusammenhang mit den lebens- oder verteidigungswichtigen Einrichtungen nach SÜG / SÜFV

[6] BT-Drs. 21/8277.

Es könnte auch **darüber nachgedacht werden, ob eine Verordnungsermächtigung vorgesehen** wird, damit im Ernstfall schnell darauf reagiert werden kann, welche Informationen über welche Infrastrukturen genau geschützt werden sollen. Auch **staatliche Auslegungshilfen** können in der Praxis dazu führen, dass Behörden die Normen einheitlich und somit vorhersehbar auslegen.

Regelungsvorschlag:

§ 3 IFG
Schutz von besonderen öffentlichen Belangen

Der Anspruch auf Informationszugang besteht nicht, […]

Nr. 9 hinsichtlich Infrastrukturen, die durch die **durch Gesetz oder aufgrund eines Gesetzes** ~~Rechtsvorschrift~~ als kritische **Anlagen** ~~Infrastrukturen~~ bestimmt worden sind oder die besonders schutzbedürftig zur Wahrung der öffentlichen Sicherheit sind.“

VIII. Änderung des Energiewirtschaftsgesetzes (§ 12f EnWG)

Durch die Neufassung von § 12f Abs. 3 EnWG RefE dürfen zukünftig sicherheitsrelevante Daten von der Regulierungsbehörde nicht mehr herausgegeben werden. Diese Regelung wird begrüßt, allerdings sollte **in der Gesetzesbegründung der Begriff „sicherheitsrelevant“ konkretisiert werden**. Den Netzbetreibern sollte die Möglichkeit eingeräumt werden, Dokumente entsprechend zu klassifizieren. Ist diese Klassifizierung vorgenommen, sollte dies zu einer (widerlegbaren) Vermutung führen, dass die Daten auch tatsächlich sicherheitsrelevant sind und dementsprechend nicht herausgegeben werden dürfen.

VERBAND KOMMUNALER UNTERNEHMEN e.V.

Bei Rückfragen oder Anmerkungen steht Ihnen zur Verfügung:

Wolf Buchholz
Senior-Fachgebietsleiter Kritische Infrastruktur und Cybersicherheit
Abteilung Recht, Finanzen und Steuern

Telefon: +49 30 58580-317
E-Mail: buchholz@vku.de