AG KRITIS

Arbeitsgruppe Kritische Infrastrukturen

Stellungnahme zum Referentenentwurf des BMI zur Anpassung von Transparenzpflichten vom 30.09.2026

Version 1.1 - zuletzt editiert am 12.11.2026

Inhaltsverzeichnis

Arbeitsgruppe Kritische Infrastrukturen....3
Vorbemerkung....4
Grundsätzliche Bewertung: Geheimhaltung ist kein Resilienzkonzept....4
Artikel 1 - Änderung des Energiewirtschaftsgesetzes....6
Artikel 2 - Änderung des Informationsfreiheitsgesetzes....7
Regelungsgehalt und Widerspruch zwischen Normtext und Begründung....7
Fehlende Erforderlichkeit....8
Unbestimmtheit und Reichweite....9
Transparenz als Voraussetzung von Resilienz....10
Forderungen zu Artikel 2....11
Artikel 3 - Änderung des Versorgungsrücklagegesetzes....11
Artikel 4 - Änderung des Gerichtsverfassungsgesetzes....11
Artikel 5 - Änderung des Arbeitsgerichtsgesetzes....12
Artikel 6 - Änderung des Fünften Buches Sozialgesetzbuch....12
Artikel 7 - Änderung des Elften Buches Sozialgesetzbuch....13
Evaluierung und Verfahren....13
Fazit....13

Arbeitsgruppe Kritische Infrastrukturen

Dieses Dokument wurde von Mitgliedern der unabhängigen Arbeitsgruppe Kritische Infrastrukturen (AG KRITIS) erstellt.

Wir haben uns im Frühjahr 2018 erstmals zusammengefunden, um Ideen und Anregungen zur Erhöhung der Resilienz und Sicherheit kritischer Dienstleistungen von Betreibern kritischer Infrastrukturen im Sinne des Gemeinwohls zu entwickeln. Unser Ziel ist es, die Versorgungssicherheit der deutschen Bevölkerung zu erhöhen, indem wir die Bewältigungskapazitäten des Staates zur Bewältigung von Großschadenslagen, die durch Cyberangriffe hervorgerufen wurden, ergänzen und erweitern wollen. Unsere Arbeitsgruppe ist unabhängig von Staat, Verwaltung oder wirtschaftlichen Interessen.

Die AG KRITIS besteht aus ca. 23 Fachleuten und Experten, die sich mit Kritischen Infrastrukturen (KRITIS) beruflich beschäftigen, zum Beispiel durch Planung, Aufbau, Betrieb sowie Beratung, Forschung oder Prüfung der beteiligten Systeme und Anlagen.
Unser Engagement ist getrieben von der Motivation, unabhängig von wirtschaftlichen Interessen eine nachhaltige Verbesserung der Sicherheit jener Anlagen kooperativ mit allen Beteiligten herbeizuführen und damit im Katastrophenfall die öffentliche Sicherheit zu verbessern. Wir sind kein Wirtschaftsverband oder Unternehmen und haben daher auch und insbesondere keine Sponsoren.

Uns eint, dass wir durch unsere Arbeit unabhängig voneinander zu dem Schluss gekommen sind, dass die Ressourcen der Bundesrepublik Deutschland zur Bewältigung von Großschadenslagen auf Grund von informations- und operationstechnischen Vorfällen im Bereich der Kritischen Infrastrukturen nicht ausreichen. In der Folge sind resultierende Krisen oder Katastrophen nicht oder kaum zu bewältigen. Es sollen daher Wege gefunden werden, das Eintreten gravierender Folgen dieser Vorfälle durch schnelles und kompetentes Handeln zu verhindern oder zumindest abzuschwächen und eine Regelversorgung in kürzest möglicher Zeit wieder sicherzustellen.

Vorbemerkung

Die AG KRITIS teilt das Anliegen des Entwurfs ausdrücklich: Kritische Infrastrukturen sind verletzlich, und ihr Schutz verdient gesetzgeberische Aufmerksamkeit. Wir widersprechen jedoch der Grundannahme, dass weniger Transparenz zu mehr Sicherheit führt. Der Entwurf verfolgt in seinem Kern, insbesondere in Artikel 2, einen Ansatz der Sicherheit durch Geheimhaltung, der in der Informationssicherheit seit Jahrzehnten als untauglich gilt und der auch für physische Infrastrukturen nicht trägt. Die Artikel 4 bis 7 bewerten wir dagegen im Grundsatz positiv und regen lediglich Präzisierungen an. Zu Artikel 3 nehmen wir nicht Stellung.

Grundsätzliche Bewertung: Geheimhaltung ist kein Resilienzkonzept

Die Begründung des Entwurfs formuliert unter Abschnitt A. I. die Zielsetzung wie folgt:

> „Soweit erforderlich ist für ausgewählte KRITIS eine Umkehr des bestehenden Regel-Ausnahme-Verhältnisses vorzusehen, die einen Vorrang des Schutzes von KRITIS vor dem Transparenzinteresse verwirklicht. Zu prüfen sind auch Löschungen von Daten. Denn Informationen, die Aufklärung über die Lage und Auslegung kritischer Infrastrukturen geben, dürfen potenziellen Angreifern nicht zugänglich sein. Der Sicherheit der kritischen Infrastrukturen ist zum Schutz der Bürgerinnen und Bürger gegenüber anderen Informationsinteressen der Vorrang einzuräumen.“

Diese Zielsetzung beruht auf drei Annahmen, die aus fachlicher Sicht nicht haltbar sind. Erstens unterstellt sie, dass sich Lage und Auslegung kritischer Infrastrukturen überhaupt geheim halten lassen. Das ist nicht der Fall. Kritische Infrastruktur ist gebaute Umwelt. Umspannwerke, Kabel- und Leitungstrassen, Netzknoten, Wasserwerke, Hochbehälter, Klärwerke, Funkmasten, Stellwerke, Brücken und Rechenzentren stehen im öffentlichen Raum und sind dort für jede Person mit geringer fachlicher Vorbildung erkennbar. Wer ein Semester Elektrotechnik, Versorgungstechnik oder Bauingenieurwesen studiert hat, kann die neuralgischen Punkte eines städtischen Versorgungsnetzes im Stadtbild identifizieren, mit und ohne technische Hilfsmittel. Wer den Ansatz des Entwurfs zu Ende denkt, müsste konsequenterweise Studierende dieser Fächer vor Studienbeginn einer Sicherheitsüberprüfung unterziehen. Ein entschlossener Angreifer ist auf amtliche Auskünfte nicht angewiesen; ein Antrag nach dem Informationsfreiheitsgesetz ist im Übrigen ein langsames, formalisiertes und aktenkundiges Verfahren und damit ein denkbar ungeeignetes Aufklärungsinstrument. Die in der Begründung bemühte Zusammenschau einzeln unbedenklicher Informationen ändert daran nichts, denn diese Zusammenschau ist aus der sichtbaren Wirklichkeit ohnehin jederzeit möglich. Der Entwurf benennt keinen einzigen Fall, in dem eine nach dem Informationsfreiheitsgesetz erteilte Auskunft einen Angriff ermöglicht oder erleichtert hätte.

Zweitens verengt die Zielsetzung die Gefährdungslage auf vorsätzliche Angriffe. Sabotage ist jedoch nicht die häufigste Ursache von Versorgungsstörungen. Die weit überwiegende Zahl der Störungen entsteht ohne kriminellen Hintergrund, etwa durch Beschädigungen bei Tiefbauarbeiten, durch technisches Versagen, Alterung oder Extremwetter. Die einzelne Störung lässt sich nicht verhindern, eine hundertprozentige Sicherheit gibt es nicht. Verhindern lässt sich aber, dass aus einer einzelnen Störung ein Versorgungsausfall wird. Die entscheidende Frage ist daher nicht, wer eine Störung verursacht, sondern ob das System sie verkraftet. Das ist eine Frage von Redundanz, Instandhaltung, Ersatzteilbevorratung und Wiederanlaufplanung, nicht von Geheimhaltung. Ein Netz, dessen Sicherheit davon abhängt, dass niemand seine Schwachstellen kennt, ist nicht sicher, sondern lediglich unbeobachtet.

Drittens übersieht die Zielsetzung, dass eine Vielzahl von Stellen Infrastrukturdaten legitim und zeitkritisch benötigt. Unternehmen des Breitband- und Glasfaserausbaus, Tiefbauunternehmen, Rettungsdienste und Feuerwehren sowie die Betreiber der jeweils anderen Sparten (Strom, Gas, Wasser, Abwasser, Telekommunikation) sind auf verlässliche Lage- und Auslegungsdaten angewiesen. Je restriktiver und unsicherer der Zugang zu diesen Daten wird, desto häufiger werden gerade jene unbeabsichtigten Schäden, die schon heute die Störungsstatistik dominieren. Die im Entwurf angekündigte Ausdehnung des Ansatzes auf das Bundesimmissionsschutzgesetz, das Baugesetzbuch und das Raumordnungsgesetz lässt befürchten, dass dieser Zielkonflikt systematisch zulasten der Betriebssicherheit entschieden wird.

Die zusätzlich angekündigte Prüfung von Löschungen bereits veröffentlichter Daten halten wir für wirkungslos. Einmal veröffentlichte Informationen lassen sich nicht zurückholen; sie liegen in Archiven, Kartendiensten und Kopien vor. Eine Löschung trifft allein die rechtstreuen Nutzer und erzeugt eine Scheinsicherheit, die im ungünstigsten Fall echte Schutzmaßnahmen verdrängt.

Unsere zentrale Sorge lautet daher: Geheimhaltung entzieht den Zustand der Infrastruktur der öffentlichen und fachlichen Kontrolle. Sie nützt in der Praxis vor allem dem Einsparen von Kosten und damit dem Verfall, nicht der Resilienz.

Artikel 1 - Änderung des Energiewirtschaftsgesetzes

Nach der Neufassung des § 12f Absatz 2 EnWG genügt für die Herausgabe netzknotenpunktscharfer Einspeise- und Lastdaten nicht mehr ein berechtigtes Interesse. Antragsteller müssen künftig neben der Fachkunde darlegen, dass die Daten zur Erfüllung ihrer jeweiligen Aufgaben erforderlich sind. Die Begründung stellt klar, dass ein abstraktes Interesse nicht ausreicht und der Zweck im konkreten Aufgabenbereich des Antragstellers begründet liegen muss. Damit wird der Kreis derjenigen, die die Netzentwicklungsplanung unabhängig überprüfen können, enger gezogen. Unabhängige Wissenschaft, Fachjournalismus und ehrenamtlich arbeitende Fachgremien verfügen nicht ohne Weiteres über eine „Aufgabe“ im Sinne der Vorschrift. Gerade die externe Überprüfung der Netzplanung ist aber ein Beitrag zur Versorgungssicherheit. Wir regen an, im Gesetzestext oder zumindest in der Begründung klarzustellen, dass auch wissenschaftliche, publizistische und zivilgesellschaftliche Prüfzwecke eine Aufgabe im Sinne des § 12f Absatz 2 Nummer 1 darstellen.

Die Neufassung des § 111g Absatz 2 Satz 9 EnWG wandelt eine Einvernehmensregelung in ein Veröffentlichungsverbot um und dehnt es auf Gas- und Wasserstoffsysteme aus. Das Tatbestandsmerkmal der Eignung, „die Sicherheit und Ordnung zu gefährden“, ist dabei sehr weit und unbestimmt. Wir empfehlen, das Verbot an eine von der Bundesnetzagentur zu dokumentierende Gefährdungseinschätzung zu knüpfen und die Veröffentlichung aggregierter oder typisierter Daten ausdrücklich zuzulassen, wie es § 12f Absatz 2 Satz 4 des Entwurfs für die Herausgabe bereits vorsieht.

Wir weisen darauf hin, dass es sich um eine schleichende Einschränkung handelt, die in der Summe mit den übrigen Artikeln Gewicht erhält.

Artikel 2 - Änderung des Informationsfreiheitsgesetzes

Wir unterstützen den Schutz kritischer Infrastrukturen, lehnen die vorgesehene pauschale Ausnahme vom Informationszugang jedoch ab. Der Informationszugang darf nur eingeschränkt werden, wenn eine konkrete Sicherheitsgefahr dargelegt ist. Teilzugang und Schwärzungen müssen Vorrang vor der vollständigen Ablehnung haben. Nur so lassen sich Sicherheit und Transparenz zugleich verwirklichen.

Regelungsgehalt und Widerspruch zwischen Normtext und Begründung

Der Änderungsbefehl ist in sich nicht schlüssig. Er lautet, in § 3 Nummer 1 werde nach Nummer 8 eine Nummer 9 angefügt. § 3 Nummer 1 IFG ist jedoch in Buchstaben gegliedert, während die Nummern 1 bis 8 die Gliederungsebene des § 3 selbst bilden. Eine Nummer 9 hinter Buchstabe g ergäbe keinen Sinn; gemeint sein kann nur eine neue Nummer 9 des § 3 IFG im Anschluss an die bisherige Nummer 8. Wir gehen im Folgenden von diesem Verständnis aus und regen an, das Redaktionsversehen im weiteren Verfahren zu bereinigen, zumal ein Gesetz, das den Informationszugang beschränkt, zumindest über die Fundstelle der Beschränkung zweifelsfrei informieren sollte.

In dieser Fassung lautet die Norm: Der Anspruch auf Informationszugang besteht nicht hinsichtlich Infrastrukturen, die durch Rechtsvorschrift als kritische Infrastrukturen bestimmt worden sind oder die besonders schutzbedürftig zur Wahrung der öffentlichen Sicherheit sind. Das ist eine vollständige Bereichsausnahme ohne jede Gefährdungs- oder Nachteilsprüfung, vergleichbar der Ausnahme für die Nachrichtendienste in § 3 Nummer 8 IFG. Die Begründung zu Artikel 2 behauptet dagegen, die Vorschrift ermögliche es, von einer Herausgabe abzusehen, „soweit das Bekanntwerden der Information nachteilige Auswirkungen haben kann“. Diese Einschränkung findet sich im Normtext nicht. Sie entstammt dem Einleitungssatz des § 3 Nummer 1 IFG, der nur für dessen Buchstaben a bis g gilt und auf eine eigenständige Nummer 9 keine Anwendung findet. Normtext und Begründung beschreiben mithin zwei verschiedene Regelungen. Hinzu kommt, dass die Darstellung des Erfüllungsaufwands (lfd. Nr. 3.3) der Änderung „lediglich klarstellenden Charakter“ zuschreibt, während die Begründung von der Schließung einer Schutzlücke spricht. Beides zugleich kann nicht zutreffen.

In der Fassung des Normtextes bewirkt die Regelung genau die in der Zielsetzung angekündigte Umkehr des Regel-Ausnahme-Verhältnisses: Die informationspflichtige Stelle muss nicht mehr prüfen und begründen, sondern kann jeden Antrag mit Infrastrukturbezug pauschal ablehnen.

Das ist ein erheblicher Rückschritt für die Transparenz staatlichen Handelns und nach unserer Auffassung nicht verhältnismäßig.

Fehlende Erforderlichkeit

Das Informationsfreiheitsgesetz enthält bereits passgenaue Ausschlussgründe für sicherheitsrelevante Informationen. § 3 Nummer 1 Buchstabe c IFG schützt Belange der inneren und äußeren Sicherheit. § 3 Nummer 2 IFG schließt den Anspruch aus, wenn das Bekanntwerden der Information die öffentliche Sicherheit gefährden kann. § 3 Nummer 4 IFG schützt Informationen, die einer Geheimhaltungs- oder Vertraulichkeitspflicht unterliegen, einschließlich eingestufter Verschlusssachen. Hinzu treten spezialgesetzliche Geheimhaltungsvorschriften, etwa im BSI-Gesetz, sowie der nach dem Entwurf bereits erweiterte § 30 VwVfG.

Die Begründung setzt sich allein mit § 3 Nummer 1 Buchstabe c IFG auseinander und erwähnt § 3 Nummer 2 IFG nicht, obwohl dieser Ausschlussgrund mit dem Maßstab des „Gefährdenkönnens“ gerade die Fälle erfasst, um die es dem Entwurf geht. Die behauptete Schutzlücke wird damit nicht belegt. Als einziger Beleg dient ein Beschluss des Verwaltungsgerichts Potsdam aus dem Jahr 2015 zu Botschaftsfahrzeugen, der weder kritische Infrastrukturen betrifft noch zeigt, dass ein Schaden eingetreten wäre. Er zeigt lediglich, dass ein Gericht von einer Behörde eine nachvollziehbare Begründung verlangt hat. Dass die Verwaltung ihre Ablehnungen begründen muss, ist jedoch kein Defizit des geltenden Rechts, sondern dessen Kern. Die Prüfung anhand gesetzlich vorgegebener Gründe ist genau der Mechanismus, der die notwendige Abwägung zwischen Transparenzinteresse und Infrastrukturschutz gewährleistet. Der in der Begründung beklagte Begründungsaufwand ist der Preis rechtsstaatlicher Verwaltung; er lässt sich durch Anwendungshinweise und Fallgruppen mindern, ohne den Anspruch selbst zu beseitigen.

Zu demselben Ergebnis ist die Berliner Beauftragte für Datenschutz und Informationsfreiheit in ihrer Stellungnahme vom 6. März 2026 zur parallelen Berliner Regelung gelangt, deren Lektüre wir ausdrücklich empfehlen.[1] Sie legt dar, dass die bestehenden, an der Gefährdungslage orientierten Ausschlussgründe den Schutz von Sicherheitsinteressen verlässlich gewährleisten, ohne die Allgemeinheit von jeglichen Informationen zu kritischer Infrastruktur auszuschließen, und warnt vor einer Rückkehr zu einer „Kultur des Amtsgeheimnisses“. Diese Bewertung lässt sich auf den Bundesentwurf übertragen.

1 Berliner Beauftragte für Datenschutz und Informationsfreiheit, Stellungnahme vom 6. März 2026 zum Entwurf eines Gesetzes zur Änderung des Berliner Datenschutzgesetzes und weiterer Rechtsvorschriften (Drs. 19/2999), Abschnitt II, https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2026/20260309-BlnBDI-Stellungnahme-BlnDSG-AEndG.pdf

Unbestimmtheit und Reichweite

Die neue Nummer 9 nennt zwei Gruppen von Infrastrukturen, für die der Informationszugang entfallen soll: zum einen Infrastrukturen, „die durch Rechtsvorschrift als kritische Infrastrukturen bestimmt worden sind“, zum anderen Infrastrukturen, „die besonders schutzbedürftig zur Wahrung der öffentlichen Sicherheit sind“. Beide Gruppen sind für sich genommen zu weit gefasst.

Die erste Gruppe umfasst alle Anlagen, die nach dem KRITIS-Dachgesetz, dem BSI-Gesetz und den zugehörigen Verordnungen als kritisch gelten, und damit weite Teile der Sektoren Energie, Wasser, Ernährung, Gesundheit, Transport und Verkehr, Informationstechnik und Telekommunikation, Finanz- und Versicherungswesen sowie Entsorgung. Da der Normtext an die Infrastruktur als solche und nicht an die Sensibilität der einzelnen Information anknüpft, wären auch Informationen ohne jeden Sicherheitsbezug ausgenommen, etwa zu Kosten, Fördermitteln, Aufsichtsmaßnahmen, Umwelt- und Ressourcenverbrauch oder zum Instandhaltungsstau.

Die zweite Gruppe geht noch weiter. Sie erfasst beliebige weitere Infrastrukturen, die in keiner Rechtsvorschrift als kritisch bestimmt sind, sofern sie als „besonders schutzbedürftig“ angesehen werden. Das Gesetz legt weder fest, nach welchen Kriterien sich diese Schutzbedürftigkeit bemisst, noch, wer sie feststellt. Ob die Voraussetzung vorliegt, beurteilt die Stelle, die über den Antrag entscheidet, selbst. Die in der Begründung enthaltene, ausdrücklich nicht abschließende Aufzählung schützenswerter Informationen reicht von Standorten und Trassen über Kapazitäten bis zu Fahrzeugen und Objekten und verdeutlicht, dass eine Begrenzung nicht beabsichtigt ist. Eine derart offene Ausnahme genügt den Anforderungen an die Bestimmtheit einer Anspruchsbeschränkung nicht.

Transparenz als Voraussetzung von Resilienz

Dass der Verweis auf den Infrastrukturschutz bereits heute genutzt wird, um sich berechtigter öffentlicher Kontrolle zu entziehen, zeigt die Strom- und Wasserversorgung besonders deutlich.

Betreiber größerer Rechenzentren sind nach dem Energieeffizienzgesetz verpflichtet, Daten zu ihrem Strom- und Wasserverbrauch zu veröffentlichen. Nach einer Recherche des SWR vom 6. November 2026 kommt mutmaßlich mehr als die Hälfte der rund 30 größten Betreiber dieser Pflicht nicht nach; im Nationalen Rechenzentrumsregister ist von den 100 größten Rechenzentren nur etwa jedes vierte verzeichnet.[2] Der Branchenverband begründet die Zurückhaltung unter anderem mit dem Schutz digitaler Infrastruktur. Verbrauchskennzahlen eines Rechenzentrums verschaffen einem Angreifer jedoch keinen Vorteil. Sie sind dagegen unverzichtbar für die öffentliche Debatte darüber, wie knappe Netzkapazitäten und in vielen Regionen knapper werdendes Grundwasser verteilt werden, also für Fragen, die die Versorgungssicherheit der Bevölkerung unmittelbar berühren. Da große Rechenzentren als kritische Anlagen bestimmt sind, könnte mit der vorgesehenen Nummer 9 künftig jeder Antrag auf Zugang zu den bei Bundesbehörden vorliegenden Verbrauchsdaten ohne weitere Prüfung abgelehnt werden. Die Regelung würde damit ein bestehendes Vollzugsdefizit gesetzlich absichern.

Die Trinkwassernotversorgung liefert ein zweites Beispiel. Die Standorte der Notbrunnen des Bundes werden grundsätzlich nicht veröffentlicht; ein entsprechender Antrag nach dem Informationsfreiheitsgesetz aus den Reihen der AG KRITIS wurde 2021 unter Hinweis auf die zivile Verteidigungsfähigkeit abgelehnt.[3] Die Geheimhaltung hat diese Anlagen nicht geschützt, sondern ihren Verfall begünstigt. In Berlin waren nach Angaben der Berliner Wasserbetriebe von 2.091 Notbrunnen 553 nicht einsatzbereit.[4] In einer bundesweiten Abfrage von CORRECTIV bei allen 401 Kreisen und kreisfreien Städten machte nur gut ein Zehntel der antwortenden Kommunen überhaupt Angaben zum Zustand ihrer Anlagen, davon meldete gut ein Viertel eine nicht vollständige Einsatzfähigkeit; ein Großteil verwies auf die Sensibilität der Informationen oder schwieg.[5] Wo niemand nachfragen darf, fehlt der Druck, Mittel für Wartung

2 SWR/tagesschau.de, „Trotz gesetzlicher Verpflichtung Verbrauch vieler Rechenzentren nicht öffentlich einsehbar“, 6. November 2026, https://www.tagesschau.de/investigativ/swr/rechenzentren-transparenz-wasserverbrauch-stromverbrauch-100.html

3 Bescheid vom 15. September 2021 zu Standorten der Trinkwassernotbrunnen, veröffentlicht bei FragDenStaat, https://media.frag-den-staat.de/files/foi/628804/20211509_IFG_Notbrunnen_geschwaerzt.pdf

4 Angabe des Sprechers der Berliner Wasserbetriebe, zitiert nach web.de, „Wasserversorgung im Krisenfall“, https://web.de/magazine/wissen/wissenschaft-technik/wasserversorgung-krisenfall-deutschland-notfaelle-geruestet-41300176

5 CORRECTIV, Recherche zur kommunalen Krisenvorsorge, Oktober 2026, https://correctiv.org/?p=296443

und Instandsetzung bereitzustellen. Im Krisenfall ist die Bevölkerung dann auf Anlagen angewiesen, deren Standort sie nicht kennt und deren Funktionsfähigkeit niemand überprüft hat.

Beide Beispiele belegen, was für alle Sektoren gilt: Der Informationszugang ist ein Instrument der Qualitätssicherung. Er ermöglicht es Parlamenten, Medien, Wissenschaft und Fachöffentlichkeit, Investitionsstau, Vollzugsdefizite und Fehlplanungen zu erkennen, bevor sie in einer Krise sichtbar werden.

Forderungen zu Artikel 2

Wir fordern, Artikel 2 ersatzlos zu streichen und stattdessen die konsequente Anwendung der bestehenden Ausschlussgründe durch Anwendungshinweise und Fallgruppen für die informationspflichtigen Stellen zu unterstützen.

Sollte der Gesetzgeber an einer ausdrücklichen Regelung festhalten, muss diese als weiterer Buchstabe in § 3 Nummer 1 IFG gefasst, auf durch Rechtsvorschrift bestimmte kritische Anlagen beschränkt und an eine konkrete, von der Behörde darzulegende Gefährdung geknüpft werden. Die zweite Alternative der „besonders schutzbedürftigen“ Infrastrukturen ist zu streichen. Eine sachgerechte Fassung könnte lauten: Der Anspruch auf Informationszugang besteht nicht, wenn und soweit das Bekanntwerden der Information aufgrund konkreter, von der informationspflichtigen Stelle darzulegender Anhaltspunkte die Sicherheit einer durch Rechtsvorschrift als kritische Anlage bestimmten Infrastruktur gefährden würde; § 7 Absatz 2 bleibt unberührt.

Der Vorrang des Teilzugangs nach § 7 Absatz 2 IFG ist im Normtext ausdrücklich zu verankern. Der Entwurf selbst erkennt mit dem Verweis auf § 27b Absatz 4 VwVfG an, dass eine abstrahierte oder teilweise Offenlegung möglich und sachgerecht ist; dieser Gedanke muss erst recht für den Informationszugang auf Antrag gelten. Sicherheitsrelevante Detailangaben wie Schutzvorkehrungen oder konkrete Verwundbarkeiten können geschwärzt werden, während Angaben zu Zustand, Kosten, Aufsicht und Ressourcenverbrauch zugänglich bleiben.

Artikel 3 - Änderung des Versorgungsrücklagegesetzes

Zu Artikel 3 nimmt die AG KRITIS nicht Stellung.

Artikel 4 - Änderung des Gerichtsverfassungsgesetzes

Die Ergänzung des § 172 Nummer 1 GVG um die Gefährdung kritischer Infrastrukturen begrüßen wir. Werden in einer Verhandlung konkrete Schutzvorkehrungen oder Verwundbarkeiten einer Anlage erörtert, ist der Ausschluss der Öffentlichkeit ein angemessenes und zielgenaues Mittel. Anders als Artikel 2 knüpft die Regelung an eine Entscheidung im Einzelfall an und belässt sie im pflichtgemäßen Ermessen des Gerichts.

Der Grundsatz der Öffentlichkeit nach § 169 GVG muss dabei gewahrt bleiben. Der Ausschluss darf nur im erforderlichen Maß erfolgen und soll sich auf diejenigen Abschnitte der Verhandlung beschränken, in denen sicherheitsrelevante Einzelheiten tatsächlich zur Sprache kommen. Der Ausschluss für die gesamte Verhandlung muss die begründungsbedürftige Ausnahme bleiben. Wir regen an, dies in der Begründung ausdrücklich festzuhalten, da Verfahren mit Infrastrukturbezug, etwa über Planungen, Vergaben oder Aufsichtsmaßnahmen, regelmäßig von erheblichem öffentlichem Interesse sind.

Die Begründung ist an dieser Stelle zudem widersprüchlich. Sie verlangt zunächst zutreffend eine gewisse Wahrscheinlichkeit für den Eintritt der Gefährdung, lässt es im folgenden Satz aber genügen, dass negative Folgen „zumindest nicht ausgeschlossen“ sind. Dieser zweite Maßstab wäre nahezu immer erfüllt und sollte gestrichen werden. Ferner empfehlen wir, den Begriff der kritischen Infrastrukturen durch einen Verweis auf die Legaldefinition der kritischen Anlagen im KRITIS-Dachgesetz und im BSI-Gesetz zu bestimmen; die Begründung enthält hierzu derzeit nur einen Platzhalter. Redaktionell weisen wir darauf hin, dass kritische Infrastrukturen einem funktionierenden Gemeinwesen dienen und nicht, wie es in der Begründung heißt, einem funktionierenden „Geheimwesen“.

Artikel 5 - Änderung des Arbeitsgerichtsgesetzes

Für die Änderung des § 52 Satz 2 ArbGG gelten unsere Ausführungen zu Artikel 4 entsprechend. Wir begrüßen die Regelung und fordern, dass der Öffentlichkeitsgrundsatz gewahrt bleibt, der Ausschluss also auf das erforderliche Maß und auf die betroffenen Teile der Verhandlung begrenzt wird. Dies ist im arbeitsgerichtlichen Verfahren von besonderem Gewicht, weil Beschäftigte kritischer Infrastrukturen, die auf Sicherheitsmängel hinweisen, andernfalls befürchten müssten, dass der gesamte Rechtsstreit unter Ausschluss der Öffentlichkeit geführt wird.

Artikel 6 - Änderung des Fünften Buches Sozialgesetzbuch

Die Ergänzung des § 217f Absatz 4d SGB V bewerten wir im Grundsatz positiv. Der Bericht weist für jede einzelne Krankenkasse den Umsetzungsstand der IT-Sicherheitsrichtlinie und die ergriffenen Maßnahmen aus. Er ist damit eine konkrete Schwachstellenübersicht und ein Musterfall dafür, dass ein eng umrissener, tatsächlich sensibler Informationsbestand gezielt geschützt werden kann, ohne ganze Sektoren dem Informationszugang zu entziehen.

Der vorgesehene Satz 3 hat allerdings eine unbeabsichtigte Nebenwirkung. Er untersagt die Bekanntgabe an andere als die in Satz 1 genannten Stellen und schließt damit dem Wortlaut nach auch die Weitergabe an das Bundesamt für Sicherheit in der Informationstechnik aus, und zwar selbst dann, wenn das Bundesministerium für Gesundheit sie für geboten hält. Für ein belastbares Lagebild der IT-Sicherheit im Gesundheitswesen ist das Bundesamt jedoch auf genau diese Informationen angewiesen. Wir fordern, das Bundesamt für Sicherheit in der Informationstechnik als unmittelbaren Empfänger des Berichts in Satz 1 aufzunehmen, damit die Meldung zur Lagebilderstellung automatisch dort eingeht und nicht von einer Weiterleitung durch ein Ministerium abhängt. Zumindest ist in Satz 3 klarzustellen, dass die Übermittlung an das Bundesamt zulässig bleibt.

Ergänzend regen wir an, das Veröffentlichungsverbot für „aus dem Bericht resultierende Ergebnisse“ auf kassenbezogene Angaben zu beschränken. Aggregierte Aussagen zum Umsetzungsstand im Gesamtsystem geben keine Angriffspunkte preis, ermöglichen aber die parlamentarische und öffentliche Kontrolle des Fortschritts.

Artikel 7 - Änderung des Elften Buches Sozialgesetzbuch

Für die Ergänzung des § 103a Absatz 8 SGB XI gelten die Ausführungen zu Artikel 6 entsprechend. Wir begrüßen den Schutz des Berichts über die IT-Sicherheit der Pflegekassen und fordern auch hier, das Bundesamt für Sicherheit in der Informationstechnik als unmittelbaren Empfänger vorzusehen, zumindest aber die Übermittlung an das Bundesamt ausdrücklich zuzulassen.

Evaluierung und Verfahren

Die Begründung verzichtet auf Befristung und Evaluierung mit dem Hinweis, die Ressorts prüften fortlaufend weiteren Anpassungsbedarf. Eine fortlaufende Suche nach weiteren Einschränkungen ist jedoch keine Evaluierung der bereits getroffenen. Wir fordern, die Wirkungen des Gesetzes nach spätestens drei Jahren unabhängig zu evaluieren und hierfür die

Zahl und die Gründe der auf den Infrastrukturschutz gestützten Ablehnungen statistisch zu erfassen. Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit sollte an dieser Evaluierung beteiligt werden.

Der Entwurf befindet sich erkennbar in einem frühen Stadium; Vorblatt und Begründung enthalten zahlreiche Platzhalter, die Angaben zum Erfüllungsaufwand und zur Vereinbarkeit mit dem Unionsrecht sind unvollständig. Angesichts der angekündigten Ausweitung des Ansatzes auf weitere Fachgesetze und auf die europäische Ebene bitten wir darum, Fachöffentlichkeit und Zivilgesellschaft an den weiteren Schritten frühzeitig und mit angemessenen Fristen zu beteiligen.

Fazit

Der Schutz kritischer Infrastrukturen und die Transparenz staatlichen Handelns sind keine Gegensätze. Wo der Entwurf eng umrissene, tatsächlich sensible Informationen schützt und die Entscheidung im Einzelfall belässt, wie in den Artikeln 4 bis 7, findet er unsere Zustimmung. Wo er das Regel-Ausnahme-Verhältnis umkehrt und ganze Sektoren pauschal dem Informationszugang entzieht, wie in Artikel 2, schwächt er die Kontrolle über den Zustand der Infrastruktur und damit die Resilienz, die er stärken will.

Wirksamer Schutz entsteht durch Redundanz, Instandhaltung und geübte Krisenbewältigung. Die AG KRITIS steht für die fachliche Begleitung des weiteren Verfahrens gern zur Verfügung.