bitkom

Stellungnahme

November 2026

Transparenz-Anpassungsgesetz

Allgemein

Angesichts der angespannten Sicherheitslage und zunehmender hybrider Bedrohungen ist es richtig und notwendig, bestehende Transparenz-, Veröffentlichungs- und Informationspflichten auf mögliche Sicherheitsrisiken zu überprüfen. Die mit dem Referentenentwurf verfolgte Zielsetzung, den Schutz kritischer Infrastrukturen durch gezielte Anpassungen bestehender Regelungen zu stärken, wird daher begrüßt. Öffentlich zugängliche Informationen können Ausspähung, Sabotage und Anschläge erleichtern. Dies gilt insbesondere, wenn durch die Zusammenführung einzelner, für sich genommen wenig sensibler Angaben Rückschlüsse auf Lage, Auslegung, Kapazitäten oder Verwundbarkeiten kritischer Infrastrukturen möglich werden. Die vorgesehenen Änderungen sind ein wichtiger erster Schritt, reichen für einen umfassenden Schutz kritischer Infrastrukturen jedoch nicht aus. Erforderlich ist ein sektorübergreifender Ansatz, der über punktuelle Anpassungen einzelner Vorschriften hinausgeht und den Schutz sicherheitsrelevanter Informationen mit technischen und organisatorischen Sicherheitsmaßnahmen sowie der Stärkung der Resilienz kritischer Infrastrukturen verbindet.

Allerdings führt eine Einschränkung von Transparenz nicht automatisch zu einem höheren Sicherheitsniveau. Lage und grundlegende Eigenschaften vieler kritischer Infrastrukturen sind bereits öffentlich erkennbar oder aus anderen Quellen erschließbar. Mithilfe KI-gestützter Auswertungen können zudem aus anderweitig verfügbaren Informationen Hinweise auf mögliche Schwachstellen abgeleitet werden. Daher sollte besonders sorgfältig geprüft werden, ob die Beschränkung einzelner Informationen gegenüber solchen Erkenntnismöglichkeiten einen zusätzlichen Sicherheitsgewinn erzielt. Zusätzliche Beschränkungen sind deshalb vor allem dort sinnvoll, wo sie die Verfügbarkeit tatsächlich sicherheitskritischer Informationen wirksam begrenzen. Auch die Löschung bereits veröffentlichter Daten sollte hinsichtlich ihres konkreten Sicherheitsgewinns bewertet werden, da bestehende Kopien und anderweitig verfügbare Informationen dadurch nicht zwangsläufig verschwinden. Entscheidend ist, dass Informationsbeschränkungen einen tatsächlichen Beitrag zum Schutz kritischer Infrastrukturen leisten und nicht lediglich vermeintliche Sicherheit schaffen. Sie können technische und organisatorische Schutzmaßnahmen, Redundanzen sowie eine belastbare Betriebs- und Wiederanlaufplanung ergänzen, aber nicht ersetzen.

82%

der deutschen Unternehmen halten es für wahrscheinlich, dass es in Deutschland zu einer ernsthaften Krise infolge hybrider Angriffe kommt.
(Bitkom, 2026)

Zugleich sind verlässliche Infrastrukturinformationen für Planung, Bau, Betrieb, Instandhaltung und Gefahrenabwehr unverzichtbar. Infrastrukturbetreiber, Hersteller, Wartungs- und Servicedienstleister, Bauunternehmen, Planungsbüros und Einsatzkräfte benötigen teilweise zeitkritischen Zugang zu entsprechenden Daten. Insbesondere dürfen Auskünfte zu konkreten Netzanschlussvorhaben, die für die Standort- und Anschlussplanung zwingend erforderlich sind, durch zusätzliche Beschränkungen nicht erschwert werden. Pauschale Einschränkungen können unbeabsichtigte Schäden begünstigen, notwendige Planungsprozesse behindern und die Betriebssicherheit beeinträchtigen. Es sollte deshalb zwischen der öffentlichen Bereitstellung von Informationen und ihrer zweckgebundenen Übermittlung an berechtigte Stellen differenziert werden. Dies gilt insbesondere auch für sensible Informationen über digitale Betriebs- und Zugangsstrukturen, etwa Fernwartungszugänge und Sicherheitskonfigurationen, die vor öffentlicher Offenlegung geschützt, Betreibern und autorisierten Dienstleistern für Wartung, Störungsbehebung und Wiederanlauf jedoch unter angemessenen Sicherheitsvorkehrungen zugänglich bleiben müssen. Auch außerhalb der formalen KRITIS-Einstufung kann ein besonderer Schutzbedarf bestehen. Dieser sollte anhand klarer und nachvollziehbarer Kriterien festgestellt werden, ohne daraus pauschale Einschränkungen gesetzlicher Informationsansprüche abzuleiten.

Darüber hinaus darf der Schutz sensibler Informationen nicht erst bei ihrer Veröffentlichung ansetzen. Bereits ihre Erhebung, Übermittlung, Zusammenführung und zentrale Speicherung können zusätzliche Risiken schaffen. Dies gilt insbesondere für sektorübergreifende Datenbestände sowie für und die Einbindung externer Dienstleister soweit hierfür keine angemessenen Schutzanforderungen bestehen. Daher wird ein konsequent risikobasierter Ansatz empfohlen, der der Datenminimierung sowie aggregierten, abstrahierten oder anonymisierten Angaben Vorrang einräumt, soweit der jeweilige Zweck damit erreicht werden kann. Ergänzend sind verbindliche Anforderungen an Zugriff, Speicherung, Weitergabe und Löschung erforderlich. Wo eine ausreichende Absicherung nicht möglich ist und die Datenübermittlung erhebliche Sicherheitsrisiken begründet oder Geschäftsgeheimnisse gefährdet, sollte ein ausdrückliches Recht zur Verweigerung der Übermittlung auch gegenüber Behörden vorgesehen werden. Gesetzlich erforderliche Sicherheitsmeldungen und notwendige Informationsflüsse müssen dabei gewährleistet bleiben.

Der Referentenentwurf sollte deshalb sicherstellen, dass zusätzliche Schutzvorgaben verhältnismäßig und rechtssicher ausgestaltet sind, notwendige Informationsflüsse nicht unverhältnismäßig einschränken und keine unnötigen regulatorischen Belastungen schaffen. An diesen Anforderungen sollten sich die vorgesehenen Änderungen im Einzelnen messen lassen.

Besonderheiten weiterer kritischer Infrastrukturen

Die sektorspezifischen Transparenz- und Datenlieferpflichten für Telekommunikationsnetze bleiben im vorliegenden Referentenentwurf unberücksichtigt. Dabei wurden die entsprechenden Pflichten für Netzbetreiber in den vergangenen Jahren stetig ausgeweitet. Mit den im Rahmen der TKG-Novelle 2026

vorgesehenen Anpassungen des Gigabit-Grundbuchs drohen weitere Verschärfungen. Angesichts zunehmender hybrider Bedrohungen darf eine möglichst umfassende zentrale Verfügbarkeit von Infrastrukturinformationen nicht länger der alleinige Maßstab für die Weiterentwicklung des Gigabit-Grundbuchs sein. Vielmehr muss der tatsächliche Schutzbedarf der betroffenen Daten stärker berücksichtigt werden. Dies gilt auch für Angaben zu eingesetzten Netzkomponenten und deren Herstellern, soweit sich daraus Rückschlüsse auf Verwundbarkeiten ergeben können. Insbesondere birgt die zentrale Zusammenführung detaillierter Daten erhebliche Sicherheitsrisiken, wenn dadurch sektorübergreifende Lagebilder entstehen, etwa durch die Verknüpfung von Telekommunikations- und Stromnetzdaten. Informationspflichten sollten deshalb auf einen eindeutig bestimmten gesetzlichen Zweck und das hierfür erforderliche Maß begrenzt werden. Hierzu sollten insbesondere die europarechtlich vorgesehenen Ausnahmen von Datenlieferpflichten für kritische Infrastrukturen an das Gigabit-Grundbuch beziehungsweise den darin enthaltenen Infrastrukturatlas umfassend genutzt werden.

Auch im Bereich der Eisenbahninfrastruktur sind die besonderen betrieblichen Anforderungen zu berücksichtigen. Die Nutzung kritischer Eisenbahninfrastruktur darf nicht dazu führen, dass Eisenbahnverkehrsunternehmen zusätzliche Sicherheits-, Prüf-, Dokumentations- oder Nachweispflichten für Infrastrukturen auferlegt werden, für deren Betrieb andere Unternehmen verantwortlich sind. Gleichzeitig muss der für einen sicheren und zuverlässigen Schienenverkehr erforderliche Informationsaustausch zwischen Eisenbahnverkehrsunternehmen, Eisenbahninfrastrukturunternehmen, und zuständigen Behörden sowie mit den beauftragten Herstellern und Dienstleistern gewährleistet bleiben. Dies betrifft insbesondere Informationen zur Betriebsführung, Verkehrsplanung, zum Störungsmanagement, zu Umleitungen sowie zum Krisen- und Wiederanlaufmanagement. Es wird daher empfohlen, in der Gesetzesbegründung vorsorglich klarzustellen, dass aus den vorgesehenen Regelungen keine zusätzlichen materiellen Betreiberpflichten für Eisenbahnverkehrsunternehmen sowie für Hersteller und Dienstleister der eingesetzten Bahntechnik entstehen und bestehende betriebsnotwendige Informationsansprüche nicht eingeschränkt werden.

Artikel 1 – Änderung des Energiewirtschaftsgesetzes

§§ 12f, 17c, 111e und 111g EnWG

Die vorgesehenen Anpassungen der §§ 12f und 111g EnWG werden grundsätzlich begrüßt. Allerdings beschränkt sich der Referentenentwurf auf einzelne Vorschriften, während weitere Informations-, Transparenz- und Veröffentlichungspflichten an zahlreichen Stellen des EnWG und der darauf beruhenden Rechtsverordnungen bestehen. Diese punktuelle Anpassung birgt die Gefahr fortbestehender Schutzlücken und unterschiedlicher Schutzmaßstäbe. Ergänzend sollte daher ein übergreifender Schutzvorbehalt im EnWG verankert werden, der sämtliche gesetzlichen Informations-, Datenbereitstellungs- und Veröffentlichungspflichten berücksichtigt.

Sicherheitsrelevante Angaben sollten nicht öffentlich zugänglich gemacht werden, wenn sie einzeln oder in Verbindung mit anderen verfügbaren Informationen Rückschlüsse auf kritische Anlagen, neuralgische Netzpunkte, Redundanzen oder strukturelle Verwundbarkeiten ermöglichen. Der Schutz sollte Elektrizitäts-, Gas-, Wasserstoff- und Wärmeinfrastrukturen sowie die hierfür erforderlichen Informations- und Kommunikationstechnologien im jeweils einschlägigen Rechtsrahmen erfassen.

Die Neufassung des § 12f Absatz 2 EnWG, wonach die Herausgabe netzknotenpunktscharfer Einspeise- und Lastdaten sowie technischer Netzinformationen künftig neben der bereits erforderlichen Fachkunde auch die Erforderlichkeit für die jeweilige Aufgabenerfüllung voraussetzt, ist zu begrüßen. Die stärkere Zweckbindung begrenzt die Weitergabe sensibler Informationen gegenüber der bisherigen Regelung. Allerdings sollte sichergestellt werden, dass auch die ersatzweise herauszugebenden typisierten Datensätze keine sicherheitskritischen Rückschlüsse ermöglichen. Die bislang ausdrücklich vorgesehene Anonymisierung sollte daher beibehalten werden.

Auch die Neufassung des § 111g Absatz 2 Satz 9 EnWG, mit der die bisherige Einvernehmensregelung durch ein verbindliches Veröffentlichungsverbot ersetzt und der Anwendungsbereich auf Gas- und Wasserstoffversorgungssysteme erweitert wird, ist grundsätzlich sinnvoll. Allerdings ist das bereits bestehende Tatbestandsmerkmal der Eignung, die „Sicherheit und Ordnung zu gefährden“, weit gefasst. Angesichts des nun verbindlichen Veröffentlichungsverbots sollte dessen Anwendung an eine nachvollziehbare und von der Bundesnetzagentur zu dokumentierende Gefährdungsbewertung geknüpft werden. Zugleich sollte klargestellt werden, dass ausreichend aggregierte, typisierte oder anonymisierte Angaben weiterhin veröffentlicht werden können, sofern keine sicherheitsrelevanten Rückschlüsse möglich sind. Die bereits bestehenden Schutzmechanismen für Betriebs- und Geschäftsgeheimnisse sollten entsprechend auch für sicherheitsrelevante Informationen gelten.

Diese Schutzmaßstäbe sollten auch bei weiteren energiewirtschaftlichen Transparenzpflichten berücksichtigt werden. Insbesondere sollten die im parallel beratenen Netzanschlusspaket vorgesehenen Veröffentlichungspflichten nach § 17c Absatz 1 EnWG-E auf mögliche Sicherheitsrisiken überprüft werden. Die öffentliche Bereitstellung von Informationen über verfügbare Netzanschlusskapazitäten ist für die Standort- und Anschlussplanung erforderlich. Zugleich können detaillierte geografische Angaben sicherheitskritische Rückschlüsse auf Netzengpässe und sensible Versorgungsbereiche ermöglichen. Daher sollte unter Berücksichtigung der unionsrechtlichen Veröffentlichungspflichten geprüft werden, welche Informationen öffentlich bereitgestellt werden müssen und welche sicherheitsrelevanten technischen Detaildaten ausschließlich qualifizierten und berechtigten Empfängern zweckgebunden zugänglich gemacht werden sollten. Die unionsrechtlich vorgesehenen Vorbehalte zum Schutz der öffentlichen Sicherheit und der Vertraulichkeit sollten dabei konsequent genutzt werden.

Über die vorgesehenen Änderungen hinaus sollten auch die behördlichen Erhebungs- und Übermittlungspflichten, insbesondere nach § 12f Absatz 1 und § 111g Absätze 1

und 4 EnWG, auf ihre Erforderlichkeit und die bestehenden Schutzvorkehrungen überprüft werden. Soweit eine Datenübermittlung erhebliche Sicherheitsrisiken begründet oder Geschäftsgeheimnisse gefährdet und diese Risiken nicht durch geeignete Schutzmaßnahmen vermieden werden können, sollte ein ausdrückliches Recht zur Verweigerung der Übermittlung vorgesehen werden. Erforderliche Datenübermittlungen sollten unter verbindlichen Anforderungen an Zweckbindung, Zugriff und Weitergabe erfolgen.

Ergänzender Regelungsbedarf besteht zudem beim Marktstammdatenregister nach § 111e EnWG. Öffentlich zugängliche Angaben zu Anlagenstandorten, Betreibern, Leistungen, Netzzuordnungen und technischen Stammdaten können in ihrer Kombination sicherheitsrelevant sein. Der Schutz kritischer Anlagen sollte daher nicht von einem aufwendigen Einzelnachweis der besonderen Schutzbedürftigkeit durch die Betreiber abhängen. Es wird empfohlen, § 15 Absatz 1 Satz 1 Nummer 1 Buchstabe c MaStRV dahingehend anzupassen, dass für sicherheitsrelevante Daten kritischer Anlagen grundsätzlich eine besondere Schutzbedürftigkeit angenommen wird und ein zusätzlicher Nachweis durch den Betreiber entfällt. Entsprechende Daten sollten von der öffentlichen Darstellung ausgenommen werden. Eine räumlich aggregierte Veröffentlichung, etwa auf Gemeinde- oder Postleitzahlenebene, sollte möglich bleiben, sofern auch durch die Verknüpfung mit anderen öffentlich verfügbaren Informationen keine sicherheitsrelevanten Rückschlüsse auf einzelne Anlagen entstehen.

§§ 14d und 14e EnWG

Netzausbaupläne der Verteilernetzbetreiber nach § 14d EnWG und die zugrunde liegenden Regionalszenarien können Rückschlüsse auf lokale Engpässe, Trassenverläufe, Netzauslastungen und geplante Optimierungsmaßnahmen ermöglichen. Auch die Netzentwicklungspläne für Strom nach §§ 12a und 12b EnWG sowie für Gas und Wasserstoff nach §§ 15a ff. EnWG enthalten detaillierte Informationen zu künftigen Netzstrukturen und Ausbaumaßnahmen. Die notwendige Transparenz der Netzplanung sollte gewährleistet bleiben, ohne sicherheitskritische Detailinformationen offenzulegen.

Die gesetzlichen Veröffentlichungspflichten, insbesondere nach § 14e Absatz 4 EnWG, sollten daher daraufhin überprüft werden, inwieweit sie auf das unionsrechtlich erforderliche Maß begrenzt werden können. Hierzu sollten beispielsweise Netzkorridore anstelle konkreter Trassenverläufe sowie Angaben zum Ausbaubedarf anstelle detaillierter technischer Parameter veröffentlicht werden, soweit die Planungs- und Beteiligungszwecke damit erfüllt werden können. Soweit europarechtliche Vorgaben weitergehende Veröffentlichungen verlangen, sollte sich die Bundesregierung für entsprechende Anpassungen auf EU-Ebene einsetzen.

§ 23c EnWG

§ 23c EnWG verpflichtet Strom- und Gasnetzbetreiber zur Veröffentlichung umfangreicher Netzstruktur- und Betriebsdaten, darunter Leitungslängen, Umspannleistungen, Entnahmestellen, geografische Versorgungsflächen und

Jahreshöchstlasten. Hinzu kommen weitere Veröffentlichungspflichten, etwa zu viertelstündlichen Last- und Netzdaten der Übertragungsnetzbetreiber.

Auch wenn einzelne Angaben für sich genommen nicht zwingend sicherheitskritisch sind, können sie in Verbindung mit anderen öffentlich verfügbaren Informationen Rückschlüsse auf Netzstrukturen, Kapazitäten, Auslastungen und besonders sensible Versorgungsbereiche ermöglichen. Der zuvor geforderte übergreifende Schutzvorbehalt sollte daher sämtliche Veröffentlichungspflichten des § 23c EnWG erfassen und nicht auf einzelne Absätze oder Datenfelder beschränkt bleiben. Daten sollten nicht veröffentlicht werden, soweit sie einzeln oder in ihrer Zusammenschau sicherheitskritische Rückschlüsse ermöglichen. Weniger detaillierte Darstellungen sollten möglich bleiben, sofern sie den jeweiligen Informationszweck erfüllen und keine entsprechenden Risiken begründen. Soweit europarechtliche Vorgaben entgegenstehen, sollte die Bundesregierung auf entsprechende Anpassungen hinwirken.

Artikel 2 – Änderung des Informationsfreiheitsgesetzes

Die Zielsetzung, sicherheitsrelevante Informationen über kritische Infrastrukturen vor unbefugter Offenlegung zu schützen, wird grundsätzlich unterstützt. Allerdings ist fraglich, ob hierfür ein zusätzlicher Ausschlussgrund im Informationsfreiheitsgesetz (IFG) erforderlich ist. Bereits § 3 Nummer 1 Buchstabe c, Nummer 2 und Nummer 4 IFG enthalten Ausnahmen zum Schutz der öffentlichen Sicherheit und vertraulicher Informationen. Ergänzend bestehen spezialgesetzliche Geheimhaltungsvorschriften sowie der erweiterte § 30 VwVfG. Das geltende IFG ermöglicht somit bereits, die Herausgabe schutzbedürftiger Informationen abzulehnen oder sensible Angaben nach § 7 Absatz 2 IFG zu schwärzen. Diese Instrumente sind in den behördlichen Anwendungshinweisen ausdrücklich vorgesehen und werden bereits in der Verwaltungspraxis genutzt. Inwieweit diese Regelungen keinen ausreichenden Schutz gewährleisten und welche konkreten Schutzlücken durch die Neuregelung geschlossen werden sollen, wird im Referentenentwurf nicht hinreichend dargelegt.

Kritisch ist insbesondere die weit gefasste Reichweite des vorgesehenen § 3 Nummer 9 IFG. Nach dem Wortlaut könnte bereits der Bezug zu einer kritischen oder anderweitig als besonders schutzbedürftig angesehenen Infrastruktur ausreichen, um den Informationszugang auszuschließen. Eine konkrete Gefährdung durch die Offenlegung der jeweiligen Information wird dagegen nicht vorausgesetzt. Die Gesetzesbegründung stellt hingegen auf mögliche nachteilige Auswirkungen des Bekanntwerdens ab. Dieser Maßstab sollte auch im Gesetzestext ausdrücklich verankert werden. Die zusätzliche Ausnahme für sonstige „besonders schutzbedürftige“ Infrastrukturen geht zudem über den formal bestimmten KRITIS-Bereich hinaus, ohne hinreichend klare Kriterien für ihre Anwendung festzulegen. Auch wenn solche Infrastrukturen einen besonderen Schutzbedarf aufweisen können, rechtfertigt dies keinen pauschalen Ausschluss des Informationszugangs.

Dabei ist zu berücksichtigen, dass Wirtschaft und Politik, insbesondere im Telekommunikationssektor, auf verlässliche behördliche Informationen angewiesen

sind, insbesondere für Ausbau- und Netzanschlussplanungen, die Wahrnehmung regulatorischer Interessen sowie die betriebliche Kontinuitäts- und Krisenplanung. Pauschale Zugangsbeschränkungen könnten diese Prozesse erschweren und damit die Resilienz kritischer Infrastrukturen beeinträchtigen. Auch die öffentliche Kontrolle von Investitionen, Instandhaltung und Versorgungssicherheit sollte nicht ohne konkreten Sicherheitsgewinn eingeschränkt werden.

Es wird daher empfohlen, auf eine pauschale Bereichsausnahme zu verzichten. Sollte an einer ausdrücklichen Regelung festgehalten werden, sollte diese als zusätzlicher Buchstabe in § 3 Nummer 1 IFG ausgestaltet und auf durch Rechtsvorschrift bestimmte kritische Anlagen beschränkt werden. Ein Ausschluss des Informationszugangs sollte nur zulässig sein, wenn konkrete, von der informationspflichtigen Stelle darzulegende Anhaltspunkte dafür vorliegen, dass das Bekanntwerden der Information die Sicherheit der betroffenen Infrastruktur gefährden würde. Die zusätzliche Ausnahme für sonstige „besonders schutzbedürftige“ Infrastrukturen sollte entfallen. Der Änderungsbefehl ist zudem redaktionell zu berichtigen, da § 3 Nummer 1 IFG nach Buchstaben und nicht nach Nummern gegliedert ist.

Der Vorrang des teilweisen Informationszugangs nach § 7 Absatz 2 IFG sollte ausdrücklich im neuen Ausschlussgrund verankert werden. Der Referentenentwurf erkennt mit dem Verweis auf § 27b Absatz 4 VwVfG selbst an, dass eine abstrahierte oder teilweise Offenlegung möglich ist. Sicherheitskritische Angaben zu Schutzvorkehrungen oder konkreten Verwundbarkeiten können durch Schwärzungen ausgenommen werden, während Informationen etwa zu Zustand, Kosten, Aufsicht und Ressourcenverbrauch grundsätzlich zugänglich bleiben sollten. Eine vollständige Ablehnung sollte nur erfolgen, wenn mildere Maßnahmen keinen ausreichenden Schutz gewährleisten.

Artikel 4 und 5 – Änderung des Gerichtsverfassungsgesetzes und des Arbeitsgerichtsgesetzes

Die Ergänzungen des § 172 Nummer 1 GVG und des § 52 Satz 2 ArbGG um die Gefährdung kritischer Infrastrukturen werden begrüßt. Werden in Gerichtsverfahren konkrete Schutzvorkehrungen oder Verwundbarkeiten kritischer Anlagen erörtert, kann der Ausschluss der Öffentlichkeit ein angemessenes Schutzinstrument sein. Positiv ist, dass die vorgesehenen Regelungen eine einzelfallbezogene Entscheidung im pflichtgemäßen Ermessen des Gerichts ermöglichen.

Dabei muss der Öffentlichkeitsgrundsatz nach § 169 GVG gewahrt bleiben. Dies gilt insbesondere für Verfahren zu Infrastrukturplanungen, Vergaben oder Aufsichtsmaßnahmen sowie für arbeitsgerichtliche Streitigkeiten, in denen Beschäftigte auf Sicherheitsmängel hinweisen. In solchen Fällen besteht ein berechtigtes Interesse an öffentlicher Kontrolle, das nicht pauschal hinter Sicherheitsinteressen zurücktreten darf. Ein Ausschluss der Öffentlichkeit sollte daher auf das erforderliche Maß und diejenigen Verhandlungsabschnitte begrenzt werden,

in denen tatsächlich sicherheitsrelevante Informationen zur Sprache kommen. Der Ausschluss der gesamten Verhandlung muss eine begründungsbedürftige Ausnahme bleiben.

Artikel 6 und 7 – Änderung des Fünften und Elften Buches Sozialgesetzbuch

Die Ergänzungen des § 217f Absatz 4d SGB V und des § 103a Absatz 8 SGB XI werden grundsätzlich begrüßt. Die Berichte zum Umsetzungsstand der IT-Sicherheitsanforderungen bei einzelnen Kranken- und Pflegekassen enthalten sensible Informationen über Schutzmaßnahmen und mögliche Schwachstellen. Ihr gezielter Schutz vor Veröffentlichung ist daher sachgerecht, ohne den Informationszugang zum Gesundheitswesen insgesamt einzuschränken.

Allerdings darf das vorgesehene Weitergabeverbot den notwendigen Informationsaustausch mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) nicht verhindern. Nach dem Wortlaut des Entwurfs ist eine Übermittlung der Berichte ausschließlich an die in den jeweiligen Vorschriften genannten Stellen vorgesehen. Das BSI ist bislang nicht als Empfänger benannt, obwohl diese Informationen für ein umfassendes Lagebild der IT-Sicherheit im Gesundheitswesen relevant sind. Es wird daher empfohlen, das BSI in beiden Vorschriften als unmittelbaren Empfänger der bereits erhobenen Berichte aufzunehmen. Zumindest sollte ausdrücklich klargestellt werden, dass eine zweckgebundene und angemessen abgesicherte Übermittlung an das BSI weiterhin zulässig bleibt. Zusätzliche Berichtspflichten für einzelne Kranken- und Pflegekassen sollten hierdurch nicht entstehen.

Zudem sollten aggregierte Auswertungen zum Umsetzungsstand der IT-Sicherheitsanforderungen weiterhin veröffentlicht werden dürfen, sofern sie keine sicherheitsrelevanten Rückschlüsse auf einzelne Kranken- oder Pflegekassen ermöglichen. Damit bleibt die öffentliche und parlamentarische Kontrolle gewährleistet, ohne sensible Einzelinformationen offenzulegen.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 700 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber

Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner

Felix Kuhlenkamp | Leiter Sicherheit
T 030 27576-279 | f.kuhlenkamp@bitkom.org

Verantwortliches Bitkom-Gremium

AK Sicherheitspolitik

Copyright

Bitkom 2026

Diese Publikation stellt eine allgemeine unverbindliche Information dar. Die Inhalte spiegeln die Auffassung im Bitkom zum Zeitpunkt der Veröffentlichung wider. Obwohl die Informationen mit größtmöglicher Sorgfalt erstellt wurden, besteht kein Anspruch auf sachliche Richtigkeit, Vollständigkeit und/oder Aktualität, insbesondere kann diese Publikation nicht den besonderen Umständen des Einzelfalles Rechnung tragen. Eine Verwendung liegt daher in der eigenen Verantwortung des Lesers. Jegliche Haftung wird ausgeschlossen. Alle Rechte, auch der auszugsweisen Vervielfältigung, liegen beim Bitkom oder den jeweiligen Rechteinhabern.