bitkom

Stellungnahme

Juli 2026

Entwurf eines Gesetzes zur Reform des Nachrichtendienstrechts

Zusammenfassung

Die Bedrohungslage für die Bundesrepublik Deutschland hat sich in den vergangenen Jahren deutlich verschärft. Hybride Angriffe, Cyberoperationen und die gezielte Destabilisierung staatlicher, wirtschaftlicher und gesellschaftlicher Strukturen sind zu einer dauerhaften sicherheitspolitischen Herausforderung geworden. Acht von zehn Unternehmen rechnen inzwischen mit einer ernsthaften Krise in Deutschland infolge hybrider Angriffe. Nachrichtendiensten kommt vor diesem Hintergrund eine zentrale Rolle für die Verteidigungsfähigkeit und Resilienz Deutschlands zu. Die anstehende Reform des Nachrichtendienstrechts kann deshalb einen wichtigen Beitrag leisten, um ihre Handlungsfähigkeit an die veränderte Gefährdungslage anzupassen.

Die Reform steht zugleich nicht für sich allein. Zusammen mit weiteren sicherheitspolitischen Vorhaben, etwa dem Gesetz zur Stärkung der Cybersicherheit, dem Gesetz zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit sowie dem Gesetz zur Einführung einer IP-Adressspeicherung und zur Weiterentwicklung der Befugnisse zur Datenerhebung im Strafverfahren, zeichnet sich eine umfassende Neuordnung der deutschen Sicherheitsarchitektur ab. Eine solche Neuaufstellung kann nur dann tragfähig sein, wenn sie rechtsstaatlich präzise, technisch realistisch und in enger Abstimmung mit den betroffenen Akteuren erfolgt. Dies gilt insbesondere dort, wo staatliche Befugnisse tief in digitale Geschäftsmodelle, IT-Infrastrukturen und Datenverarbeitungsprozesse privater Unternehmen eingreifen.

Der vorliegende Referentenentwurf wird diesem Anspruch in seiner jetzigen Fassung noch nicht gerecht. Er begründet weitreichende Auskunfts- und Mitwirkungspflichten für Unternehmen, lässt jedoch zentrale Fragen offen: welche Unternehmen konkret verpflichtet werden, welche Datenarten erfasst sind, wie weit eine rechtliche Verfügungsbefugnis reicht und wie mit Daten umzugehen ist, die Unternehmen lediglich als Auftragsverarbeiter für Dritte verarbeiten. Besonders kritisch bewertet Bitkom zudem vorgesehene Zugriffsmöglichkeiten auf technische Informationen, Systemkopien und laufende IT-Infrastrukturen. Solche Maßnahmen können

83%

der deutschen Unternehmen rechnen mit einer ernsthaften Krise in Deutschland durch hybride Angriffe. (Bitkom, 2026)

hochsensible Unternehmens- und Kundendaten betreffen und erhebliche Betriebsrisiken auslösen. Sie dürfen daher nur auf klarer gesetzlicher Grundlage, unter strengen Sicherheitsvorgaben, mit eindeutiger Zweckbindung und als letztes Mittel erfolgen.

Bitkom fordert eine grundlegende Präzisierung des Entwurfs. Erforderlich sind klare Begriffsbestimmungen, eine saubere Abgrenzung von Verantwortlichen und Auftragsverarbeitern, belastbare Vorgaben zu Zweckbindung, Löschung und Weitergabe übermittelter Daten, ein Subsidiaritäts- und Kooperationsprinzip beim Zugriff auf IT-Infrastrukturen, angemessene Verfahrensgarantien bei Sanktionen sowie eine realistische Ermittlung des Erfüllungsaufwands für die Wirtschaft.

Die Modernisierung des Nachrichtendienstrechts muss Sicherheit stärken, ohne Rechtsunsicherheit, unverhältnismäßige Belastungen oder eine Schwächung des Vertrauens in den Digitalstandort Deutschland zu erzeugen.

2. Vorbemerkung zum Verfahren

Bitkom begrüßt grundsätzlich das Ziel des Bundesministeriums des Innern, das Nachrichtendienstrecht zu modernisieren, verfassungsgerichtliche Vorgaben umzusetzen und die Aufklärungs- und Kontrollstrukturen der Nachrichtendienste weiterzuentwickeln.

Das gewählte Beteiligungsverfahren wird der Bedeutung des Vorhabens jedoch nicht gerecht. Der Referentenentwurf umfasst mehr als 700 Seiten und betrifft zentrale Fragen der digitalen Infrastruktur, der Unternehmensmitwirkung, des Datenschutzes, der IT-Sicherheit sowie der internationalen Wettbewerbsfähigkeit des Digitalstandorts Deutschland. Die Frist zur Kommentierung bis zum 14. Juli ist vor diesem Hintergrund deutlich zu kurz.

Eine sachgerechte Bewertung der technischen, rechtlichen und wirtschaftlichen Auswirkungen ist innerhalb weniger Arbeitstage kaum möglich. Dies gilt insbesondere, da der Entwurf zahlreiche neue oder erheblich erweiterte Pflichten für Unternehmen vorsieht. Die kurze Frist erschwert eine fundierte Beteiligung der betroffenen Wirtschaft und birgt das Risiko, dass wesentliche Praxisfolgen im weiteren Verfahren nicht ausreichend berücksichtigt werden.

Bitkom wird das Gesetzgebungsverfahren dennoch konstruktiv begleiten und bringt sich mit dieser Stellungnahme in das Verfahren ein. Aufgrund der kurzen Rückmeldefrist konzentriert sich die Stellungnahme auf besonders relevante Punkte aus Sicht der Digitalwirtschaft; eine abschließende Bewertung des gesamten Entwurfs ist damit nicht verbunden.

3. Begrüßenswerte Regelungsansätze

Bitkom bewertet positiv, dass der Entwurf an mehreren Stellen einen klareren und konsolidierten Rechtsrahmen für die Tätigkeit der Nachrichtendienste schaffen will. Positiv hervorzuheben sind insbesondere die vorgesehene Informationsweitergabe der

Dienste an Wirtschaft und Fachkreise (§§ 45, 51 BVerfSchG-E; § 85 BNDG-E), der gesetzliche Kooperationsrahmen bei informationstechnischen Angriffen (§ 12 BVerfSchG-E; § 14 BNDG-E) sowie die Möglichkeit, Angriffswerkzeuge nach Herstellung einer Sicherungskopie zu löschen (§ 12 Abs. 5 BVerfSchG-E; § 14 Abs. 4 BNDG-E).

Ebenfalls begrüßt Bitkom die angestrebte Konsolidierung bisher verstreuter Regelungen, das im Entwurf angelegte abgestufte Schwellensystem sowie die damit verbundene Stärkung von Normenklarheit und Vorhersehbarkeit. Positiv ist zudem, dass die Prüfung der Rechtmäßigkeit eines Ersuchens grundsätzlich bei der ersuchenden Behörde liegt und Anbieter dadurch nicht selbst in die Rolle einer materiellen Rechtmäßigkeitsprüfung gedrängt werden.

Darüber hinaus ist die Stärkung der unabhängigen Kontrolle durch den Unabhängigen Kontrollrat ausdrücklich positiv zu bewerten. Gleiches gilt für den Umstand, dass der Entwurf kein allgemeines Entschlüsselungs- oder Backdoor-Mandat vorsieht. Diese rote Linie muss im weiteren Verfahren zwingend erhalten bleiben.

4. Allgemeine und querschnittliche Anmerkungen

4.1 Transparenz und Kontrolle

Der Entwurf weitet die Auskunfts- und Mitwirkungspflichten privater Unternehmen erheblich aus. Zugleich fehlen hinreichende Transparenz- und Berichtspflichten über Umfang, Häufigkeit und Kosten dieser Inanspruchnahme. Ohne entsprechende Daten ist eine belastbare Evaluierung der neuen Regelungen kaum möglich.

Bitkom regt daher einen jährlichen Transparenzbericht des Unabhängigen Kontrollrats über die Inanspruchnahme privater Unternehmen an. Dieser sollte aggregierte und anonymisierte Angaben zur Zahl der Auskunftsersuchen, zu betroffenen Datenkategorien, ersuchenden Behörden, Vorabkontrollverfahren, Normkonflikten und Entschädigungsleistungen enthalten. Zudem sollte Unternehmen ermöglicht werden, nach Ablauf einer angemessenen Sperrfrist aggregierte Angaben über die Anzahl der an sie gerichteten Auskunftsersuchen in eigenen Transparenzberichten zu veröffentlichen, sofern keine überwiegenden Sicherheitsinteressen entgegenstehen.

4.2 Normkonflikte mit EU-Recht, ausländischem Recht und Kundenverträgen

Der Entwurf lässt an mehreren Stellen offen, wie Unternehmen mit Konflikten zwischen deutschen Auskunfts- und Geheimhaltungspflichten, europäischem Datenschutzrecht, ausländischen gesetzlichen Pflichten und vertraglichen Informationspflichten gegenüber Kunden umgehen sollen. Dies betrifft insbesondere Cloud-, Hosting- und Managed-Service-Anbieter mit internationalen Kunden- und Konzernstrukturen. Unternehmen können verpflichtet sein, Kunden über staatliche Zugriffe zu informieren. Gleichzeitig können nationale Geheimhaltungspflichten eine

solche Information untersagen. Der Entwurf bietet für diese Kollisionslagen noch keinen ausreichend geordneten Ausweg.

Bitkom fordert daher klare Kollisionsregeln. Unternehmen dürfen nicht gezwungen werden, entweder gegen deutsches Recht oder gegen zwingende europäische, ausländische oder vertragliche Pflichten zu verstoßen. Erforderlich ist ein Verfahren, das eine rechtssichere Klärung solcher Konflikte ermöglicht, etwa durch gerichtliche Überprüfung oder eine Vorlage an den Unabhängigen Kontrollrat. Parallel dazu müssen mögliche Konflikte über internationale Abkommen gelöst werden, die durch die Europäische Kommission verhandelt werden.

4.3 Zweckbindung, Löschung und Weitergabe übermittelter Daten

Der Entwurf regelt zwar die Voraussetzungen von Auskunfts- und Mitwirkungspflichten, enthält aber nicht durchgängig ausreichende Vorgaben zum weiteren Umgang mit den übermittelten Daten. Für Unternehmen ist jedoch entscheidend, zu welchem Zweck Daten verwendet werden, wann sie gelöscht werden und ob sie an andere Behörden oder ausländische Stellen weitergegeben werden.

Bitkom fordert klare Regelungen zu Zweckbindung, Löschung, Dokumentation und Weitergabe. Eine Zweckänderung darf nur auf Grundlage einer eigenständigen gesetzlichen Ermächtigung erfolgen. Übermittelte Daten sind zu löschen, sobald sie für den Erhebungszweck nicht mehr erforderlich sind. Eine Weitergabe an andere Behörden oder ausländische Stellen muss besonders begründet und dokumentiert werden.

4.4 Erfüllungsaufwand der Wirtschaft

Der im Entwurf angesetzte Erfüllungsaufwand der Wirtschaft erscheint nicht plausibel. Angesichts der vorgesehenen Pflichten, möglicher technischer Anpassungen, zusätzlicher Prozesse, Sicherheitsüberprüfungen, Rechtsprüfungen und Dokumentationsanforderungen ist eine Belastung der gesamten Wirtschaft im niedrigen fünfstelligen Bereich pro Jahr nicht nachvollziehbar.

Bitkom fordert daher eine transparente und realistische Neuerhebung des Erfüllungsaufwands unter Einbeziehung der betroffenen Unternehmen. Dabei sind insbesondere die erwartete Anzahl von Ersuchen, die betroffenen Datenarten, technische Umsetzungsanforderungen, Personalaufwand, Sicherheitsüberprüfungen, Rechtsprüfung, Dokumentation und mögliche Bereitschaftsstrukturen zu berücksichtigen.

4.5 Redaktionelle und systematische Inkonsistenzen

Der Entwurf weist an einzelnen Stellen redaktionelle und systematische Unschärfen auf. So soll das Artikel-10-Gesetz aufgehoben werden, während an anderer Stelle weiterhin auf das Artikel-10-Gesetz verwiesen wird. Solche Inkonsistenzen müssen im weiteren Verfahren bereinigt werden. Gerade bei einem Reformgesetz dieser

Tragweite ist eine widerspruchsfreie, verständliche und systematisch saubere Gesetzesfassung unerlässlich. Unklare oder fehlerhafte Verweise führen in der Praxis zu Rechtsunsicherheit und erschweren die Umsetzung durch Unternehmen.

4.6 Antwortfristen auf Auskunftsersuchen

Der Entwurf sieht an verschiedenen Stellen sehr kurze Reaktionszeiten auf Auskunfts- und Mitwirkungspflichten vor beziehungsweise lässt offen, innerhalb welcher Fristen Unternehmen Ersuchen praktisch erfüllen müssen. Die Antwortfristen müssen sich jedoch an den tatsächlichen betrieblichen Möglichkeiten der betroffenen Unternehmen orientieren.

Eine Verpflichtung zur Beantwortung innerhalb weniger Stunden würde faktisch den Aufbau dauerhafter Bereitschafts- und Erreichbarkeitsstrukturen erfordern, die in vielen Unternehmen bislang nicht vorhanden sind. Bitkom regt daher an, angemessene und praxistaugliche Antwortfristen vorzusehen. Soweit keine akute Gefahr im Verzug vorliegt, sollte ein Regelzeitraum von bis zu 72 Stunden vorgesehen werden.

5. Übergreifende Anmerkungen zu parallelen Regelungen im BVerfSchG-E und BNDG-E

Die nachfolgenden Anmerkungen betreffen Regelungskomplexe, die im BVerfSchG-E und BNDG-E weitgehend parallel angelegt sind. Bitkom behandelt diese Punkte gemeinsam, um Wiederholungen zu vermeiden. Die jeweils betroffenen Vorschriften werden in den Überschriften ausdrücklich benannt.

5.1 Zu § 11 Abs. 3 Nr. 2 Buchst. b, Abs. 5 BVerfSchG-E und § 13 BNDG-E - Zugriff auf Inhaltsdaten digitaler Dienste

Kritisch bewertet Bitkom, dass der Entwurf den Zugriff auf »Inhalte von Nutzungen« digitaler Dienste ermöglicht, ohne diese Daten einem dem Fernmeldegeheimnis vergleichbaren Schutzregime zu unterstellen. Die Gleichsetzung von Inhaltsdaten mit einfachen Bestandsdaten verkennt deren Grundrechtsrelevanz und steht im Widerspruch zu globalen Standards und Normen (s. TGA-Grundsätze der OECD). Inhaltsdaten digitaler Dienste sind regelmäßig hoch grundrechtsrelevant. Sie können Rückschlüsse auf Kommunikation, Verhalten, Interessen, Geschäftsbeziehungen und persönliche Lebensführung zulassen.

Die Gleichbehandlung solcher Inhaltsdaten mit einfachen Bestands- oder Nutzungsdaten wird ihrer Eingriffsintensität nicht gerecht. Der Zugriff auf Inhalte digitaler Dienste darf nicht zu einer faktischen Absenkung des Schutzes vertraulicher Kommunikation und der durch Art. 10 GG geprägten Schutzstandards führen. Für den Zugriff auf Inhalte von Nutzungen digitaler Dienste sollte daher eine unabhängige

vorherige Kontrolle vorgesehen werden. Zudem sollte die Zugriffsschwelle auf besonders erhebliche Bedrohungslagen begrenzt werden.

5.2 Zu § 11 Abs. 1 Nr. 1 Buchst. b BVerfSchG-E und § 12 Abs. 2 Nr. 6 BNDG-E - Begriff »Digitale Dienste«

Der Begriff »Digitale Dienste« ist im Entwurf nicht hinreichend präzise bestimmt. Unklar bleibt, ob und in welchem Umfang Cloud-Infrastruktur, Hosting-Dienste, Managed Services, IT-Sicherheitsdienstleister, Beratungs- und Implementierungsdienstleister oder reine Auftragsverarbeiter erfasst sind. Ohne eine klare Definition können Unternehmen nicht rechtssicher beurteilen, ob sie Verpflichtete im Sinne der Normen sind. Bitkom fordert daher eine eindeutige gesetzliche Begriffsbestimmung oder eine klare Anknüpfung an bestehende europäische Rechtsakte. Zugleich muss klargestellt werden, dass Ersuchen vorrangig an den Verantwortlichen und nicht an reine Auftragsverarbeiter zu richten sind, solange eine Inanspruchnahme des Verantwortlichen rechtlich und technisch möglich ist.

5.3 Zu § 11 Abs. 2 BVerfSchG-E und § 16 Abs. 1 BNDG-E - Marktortprinzip, internationale Anbieter und Pflichtenkollisionen

Der Entwurf knüpft Unternehmenspflichten teilweise an das Marktortprinzip an. Dadurch können auch Anbieter ohne deutsche Niederlassung oder Unternehmen mit internationalen Konzernstrukturen erfasst werden. Dies kann zu erheblichen Pflichtenkollisionen mit ausländischem Recht, europäischem Datenschutzrecht, völkerrechtlichen Grundsätzen, transatlantischen Datenzugriffsregimen und vertraglichen Verpflichtungen gegenüber Kunden führen.

Bitkom unterstützt das Ziel eines Level Playing Field. Vergleichbare Dienste sollten vergleichbaren Pflichten unterliegen. Dies darf jedoch nicht dazu führen, dass Unternehmen in unauflösbare Rechtskonflikte geraten. Die Kollisionsregelungen des Entwurfs müssen daher vervollständigt werden. Eine Freistellung von der Auskunftspflicht muss vorgesehen werden, soweit zwingendes ausländisches Recht entgegensteht. Dies muss auch für Unternehmen mit deutscher Niederlassung gelten, sofern sie aufgrund internationaler Konzernstrukturen oder Kundenverträge rechtlich gebunden sind.

5.4 Zu § 12 BVerfSchG-E und § 14 BNDG-E - Technische Informationen, personenbezogene Daten, Systemkopien und Löschung

Die nach § 12 BVerfSchG-E und § 14 BNDG-E herauszugebenden technischen Informationen können hochsensibel sein. Sie können Rückschlüsse auf Netzarchitekturen, Sicherheitsmechanismen, Protokolldaten, Angriffserkenntnisse,

Kundensysteme, Schwachstellen und interne Schutzmaßnahmen der betroffenen Unternehmen zulassen. Diese Art von Beschlagnahmungsbefugnis berücksichtigt ungenügend, wie modernes Cloud-Computing funktioniert.

Bitkom fordert daher, gesetzlich klarzustellen, dass solche Informationen nur über gesicherte Schnittstellen übermittelt und beim Empfänger ausschließlich in einer gesicherten Verarbeitungsumgebung verarbeitet werden dürfen. Zugriff, Verarbeitung und Weitergabe müssen einem strengen Need-to-know-Prinzip folgen und auf einem vorab definierten Berechtigungs- und Protokollierungskonzept beruhen.

Soweit im Rahmen solcher Ersuchen personenbezogene Daten betroffen sind, muss zudem klargestellt werden, dass bestehende spezialgesetzliche Auskunftsregime nicht umgangen oder abgesenkt werden. Personenbezogene Daten dürfen nur nach Maßgabe der jeweils einschlägigen gesetzlichen Ermächtigungsgrundlagen herausgegeben werden, insbesondere unter Beachtung der Vorgaben des TDDDG, des TKG und der DSGVO. Für Unternehmen ist diese Klarstellung erforderlich, um rechtssicher beurteilen zu können, welche Daten im Rahmen eines Ersuchens nach § 12 BVerfSchG-E beziehungsweise § 14 BNDG-E herausgegeben werden dürfen. Besonders eingriffsintensiv ist zudem die in § 12 Abs. 2 BVerfSchG-E und § 14 Abs. 2 BNDG-E vorgesehene Verpflichtung zur Herausgabe von Kopien ganzer Teile informationstechnischer Systeme. Der Begriff »Teile des informationstechnischen Systems« ist zu unbestimmt. In mandantenfähigen Cloud- und Hosting-Umgebungen besteht das Risiko, dass nicht nur angriffsbezogene Daten, sondern auch Daten unbeteiligter Dritter oder anderer Kunden miterfasst werden. Bitkom fordert daher, die Herausgabe von Kopien auf technisch isolierbare, angriffsbezogene Datenbestände zu begrenzen. Daten anderer Mandanten und unbeteiligter Dritter dürfen nicht miterfasst werden. Vorrang muss stets die Auskunft oder Analyse durch den Anbieter selbst haben. Das Prinzip »data at source« ist in solchen Konstellationen regelmäßig grundrechtsschonender, sicherer und technisch zielgenauer.

Die in § 12 Abs. 4 Satz 3 BVerfSchG-E vorgesehene Möglichkeit, eine Löschung nicht erforderlicher Daten bei unvertretbarem Aufwand zu unterlassen, ist kritisch zu bewerten. Gerade bei Systemkopien muss sichergestellt sein, dass nicht relevante Daten unverzüglich ausgesondert und gelöscht werden. Bitkom regt daher an, diese Ausnahme zu streichen oder jedenfalls deutlich enger zu fassen. Daten, die für die Aufklärung des konkreten Angriffs nicht erforderlich sind, dürfen nicht dauerhaft in staatlichen Datenbeständen verbleiben. Vergleichbare Löschregelungen im BNDG-E sollten entsprechend eng und grundrechtsschonend ausgestaltet werden.

5.5 Zu §§ 12, 24 BVerfSchG-E und § 36 BNDG-E - Subsidiarität beim Zugriff auf laufende IT- und Netzwerkinfrastruktur

Die vorgesehenen Befugnisse zur Aufklärung informationstechnischer Angriffe und zum Auslesen technischer Angriffsspuren können Eingriffe in laufende IT- und Netzwerkinfrastrukturen erforderlich machen. Solche Eingriffe sind besonders sensibel. Sie können Betriebsrisiken auslösen, über das eigentliche Zielobjekt hinauswirken und

in komplexen Cloud-, Hosting-, Telekommunikations- oder Managed-Service-Umgebungen auch Daten und Systeme unbeteiligter Kunden betreffen.

Bitkom fordert daher ein ausdrückliches Subsidiaritäts- und Kooperationsprinzip für Maßnahmen nach §§ 12, 24 BVerfSchG-E und § 36 BNDG-E. Eingriffe in laufende Betriebsinfrastruktur dürfen nur angeordnet werden, wenn die erforderlichen Erkenntnisse nicht durch weniger eingriffsintensive Maßnahmen gewonnen werden können, insbesondere durch Auswertung bereits gespeicherter Protokolldaten, durch Auskünfte des Betreibers oder durch eine technische Analyse unter Einbindung des betroffenen Unternehmens. Die Betreiber verfügen regelmäßig über die beste Kenntnis ihrer Systeme, Datenflüsse, Mandantenstrukturen und Sicherheitsmechanismen. Eine Einbindung des Betreibers ist daher nicht nur grundrechtsschonender, sondern auch operativ sicherer und zielgenauer. Der Betreiber sollte vor einem Eingriff angehört und über Umfang und technische Durchführung der Maßnahme informiert werden, soweit der Zweck der Maßnahme dadurch nicht vereitelt wird. In Fällen, in denen eine vorherige Unterrichtung ausnahmsweise nicht möglich ist, sollte eine nachträgliche Unterrichtung unverzüglich nachgeholt werden.

Zudem muss gesetzlich ausgeschlossen werden, dass Maßnahmen in laufenden IT- und Netzwerkinfrastrukturen kaskadierende Effekte auslösen oder die Verfügbarkeit von Diensten für unbeteiligte Dritte beeinträchtigen. Der Entwurf sollte daher klare Anforderungen an Verhältnismäßigkeit, technische Durchführung, Dokumentation, Risikominimierung und Betreiberbeteiligung enthalten.

5.6 Zu § 13 Abs. 6 BVerfSchG-E und § 13 Abs. 6 BNDG-E - Sicherheitsüberprüfung von Unternehmenspersonal

Die Regelungen zur Sicherheitsüberprüfung von Unternehmenspersonal werfen erhebliche praktische Fragen auf. Die Pflicht, sicherheitsüberprüfungsbereites Personal vorzuhalten oder gegebenenfalls vorsorglich überprüfen zu lassen, ist im Anwendungsbereich unklar und verursacht erheblichen Aufwand. Bitkom unterstützt Geheimschutz und einen vertrauensvollen, sicheren Umgang mit sensiblen Ersuchen. Sicherheitsüberprüftes und benanntes Personal kann im Sinne eines SPOC-Modells die Qualität und Verlässlichkeit der Zusammenarbeit erhöhen. Voraussetzung ist jedoch ein klarer, begrenzter und praxistauglicher Anwendungsbereich.

Pauschale, anlasslose oder unbegrenzte Sicherheitsüberprüfungen »auf Vorrat« sind abzulehnen. Zugleich sollten Unternehmen die Möglichkeit erhalten, für einen klar begrenzten Kreis sicherheitskritischer Personen frühzeitig Sicherheitsüberprüfungen anzustoßen, wenn ein nachvollziehbarer sachlicher Bezug zu künftigen sicherheitsrelevanten Aufgaben, VS-Aufträgen oder vergleichbaren Tätigkeiten besteht. Dies ist insbesondere für Unternehmen relevant, die kurzfristig auf Ersuchen reagieren oder sicherheitskritische Leistungen erbringen müssen.

Sicherheitsüberprüfungen sollten mit Zustimmung der betroffenen Beschäftigten, unter klaren gesetzlichen Voraussetzungen, mit angemessenen Übergangsfristen und bei vollständiger Kostenerstattung erfolgen. Zudem sollten Verfahrensdauer,

Zuständigkeiten, die Übertragbarkeit bestehender Sicherheitsüberprüfungen sowie deren behördenübergreifende Anerkennung verbindlich geregelt werden.

Zudem sieht der Entwurf in § 13 Abs. 6 BVerfSchG-E vor, dass das verpflichtete Unternehmen Verschlusssachen des Grades VS-NfD (VERSCHLUSSSACHE – NUR FÜR DEN DIENSTGEBRAUCH) nach Maßgabe der gemäß § 35 Abs, 1 SÜG zu erlassenden Verwaltungsvorschrift verarbeitet. Diese Verweisung sehen wir kritisch. Bei der Allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA) handelt es sich um eine Verwaltungsvorschrift des Bundes, welche grundsätzlich keine Außenwirkung auf private Dritte entfaltet. Abgesehen davon adressiert die VSA einen Nutzerkreis in der Sphäre der Bundesverwaltung und enthält Regelungen, die auf private Unternehmen in Teilen nicht sinnvoll anwendbar sind. So laufen die Regelungen des Abschnitts VIII VSA insofern ins Leere, als das BSI private Unternehmen im Rahmen einer Freigabe des Betriebs von VS-IT mangels Zuständigkeit gar nicht unterstützen kann. Des Weiteren ist dem Geheimschutz in der Wirtschaft das Kumulationsprinzip der VSA grundsätzlich fremd, wonach durch Anhäufung von Verschlusssachen eines Grades in Summe ein höheren Geheimhaltungsgrad erzeugt werden kann. Schließlich fehlt es den Bestimmungen der VSA an konkreten Vorgaben über den Umgang mit VS-NfD auf IT.

Wir halten es für sinnvoll, den Besonderheiten in der Behandlung von VS-NfD in der Wirtschaft auch im Kontext des BND-Gesetzes Rechnung zu tragen. Anstelle der VSA sollte auf Anlage 4 des Handbuchs für den Geheimschutz in der Wirtschaft (VS-NfD-Merkblatt des BMWE) verwiesen werden. Der Bezug auf die spezifischen Regelungen für Anwender im privaten Bereich schafft Klarheit über die einzuhaltenden Anforderungen und vermeidet unnötige Risiken hinsichtlich der korrekten Umsetzung der gesetzlichen Anforderungen.

5.7 Zu § 13 Abs. 4 und 5 BVerfSchG-E sowie § 13 Abs. 5 BNDG-E - Ausleitungs-, Umleitungs- und Zugangspflichten

Die vorgesehenen Ausleitungs- und Mitwirkungspflichten für Anbieter von Telekommunikationsdiensten und vergleichbare Anbieter müssen eng begrenzt und technisch eindeutig ausgestaltet werden. Unklarheiten bestehen insbesondere dort, wo Anbieter Inhalte ausleiten, bei Umleitungen mitwirken oder Zugang zu Einrichtungen gewähren sollen.

Bitkom begrüßt ausdrücklich, dass der Entwurf kein allgemeines Entschlüsselungs- oder Backdoor-Mandat enthält. Dies muss gesetzlich eindeutig abgesichert werden. Ausleitungs- und Mitwirkungspflichten dürfen keine Schwächung von Sicherheits- oder Verschlüsselungsarchitekturen verlangen. Es muss klargestellt werden, dass keine Pflicht zur Schaffung von Backdoors, Klartextzugängen oder strukturellen Schwächungen von Verschlüsselung besteht. Dies gilt insbesondere auch für moderne Sicherheitsarchitekturen wie Zero-Trust-Modelle, mutual TLS/mTLS und vergleichbare Ende-zu-Ende abgesicherte Kommunikationsbeziehungen. Technische Mitwirkungspflichten nach § 13 BVerfSchG-E und weiteren einschlägigen Befugnissen dürfen solche Architekturen weder schwächen noch deren Integrität beeinträchtigen.

Zudem sollten Ausleitungs- und Mitwirkungspflichten technikneutral, standardisiert und interoperabel ausgestaltet werden. Soweit technische Schnittstellen oder Verfahren erforderlich sind, sollten diese an anerkannten Standards, insbesondere ETSI-konformen Verfahren, ausgerichtet werden. Proprietäre Einzellösungen und uneinheitliche technische Anforderungen würden den Umsetzungsaufwand erheblich erhöhen und zusätzliche Sicherheitsrisiken schaffen.

Für Maßnahmen der Quellen-TKÜ und Online-Durchsuchung sind enge gesetzliche Leitplanken erforderlich. Solche Maßnahmen dürfen nicht zu Kollateralzugriffen auf unbeteiligte Systeme führen und keine Sicherheitslücken schaffen, offenhalten oder verstetigen. Der Entwurf sollte daher klarstellen, dass technische Mitwirkungspflichten keine Verpflichtung zur Schwächung von IT-Sicherheit, zur Veränderung sicherer Produktarchitekturen oder zur Unterstützung unkontrollierter Eingriffe in Systeme Dritter begründen.

5.8 Zu § 72 Abs. 2 und 3 BVerfSchG-E sowie § 134 Abs. 2 und 3 BNDG-E - Betriebsuntersagung und Zwangsgeld

Die vorgesehenen Durchsetzungsbefugnisse, insbesondere die Möglichkeit einer ganzen oder teilweisen Betriebsuntersagung sowie Zwangsgelder bis zu einer Million Euro, sind unverhältnismäßig weitreichend. Bei Betreibern digitaler Infrastruktur können solche Maßnahmen erhebliche Kollateralfolgen für unbeteiligte Kunden, kritische Geschäftsprozesse und die Verfügbarkeit digitaler Dienste auslösen.

Bitkom erkennt das Interesse an einer wirksamen Durchsetzung rechtmäßiger Ersuchen an. Eine Betriebsuntersagung darf jedoch nicht als reguläres Durchsetzungsmittel gegenüber digitalen Infrastrukturanbietern vorgesehen werden. Sie sollte gestrichen, hilfsweise auf wiederholte, vorsätzliche und schwerwiegende Verstöße begrenzt werden. Erforderlich sind in jedem Fall Anhörung, abgestufte Eskalation, angemessene Fristen zur Nachbesserung und aufschiebend wirkender Rechtsschutz. Für Anbieter kritischer Infrastrukturen, KRITIS-nahe Dienstleister und Betreiber besonders relevanter digitaler Infrastruktur muss ausgeschlossen werden, dass Durchsetzungsmaßnahmen die Verfügbarkeit von Diensten für unbeteiligte Dritte beeinträchtigen.

5.9 Zu Abschnitt E.2, § 11 Abs. 7 BVerfSchG-E und § 16 Abs. 4 BNDG-E - Erfüllungsaufwand und Kostenerstattung

Der im Entwurf angesetzte Erfüllungsaufwand der Wirtschaft erscheint grob unterschätzt. Angesichts der Reichweite der vorgesehenen Pflichten, möglicher technischer Anpassungen, zusätzlicher Prozesse, Bereitschaftsstrukturen, Sicherheitsüberprüfungen und Dokumentationsanforderungen ist eine Belastung der gesamten Wirtschaft im niedrigen fünfstelligen Bereich pro Jahr nicht plausibel.

Bitkom begrüßt, dass der Entwurf Kostenerstattungsregelungen vorsieht. Diese müssen jedoch realistisch ausgestaltet werden. Die Entschädigung sollte auf die vollständigen, nachgewiesenen tatsächlichen Kosten umgestellt werden. Eine Beschränkung auf JVEG-Pauschalen, insbesondere bei strukturiert gespeicherten Daten, wird dem tatsächlichen Aufwand vieler Unternehmen nicht gerecht.

5.10 Zu § 73 BVerfSchG-E und § 135 BNDG-E - Anzeige- und Genehmigungspflichten ausgeschiedener Bediensteter

Die vorgesehenen Anzeige- und Genehmigungspflichten für ausgeschiedene Bedienstete von Bundesamt für Verfassungsschutz und Bundesnachrichtendienst können Rechtsunsicherheit für Unternehmen schaffen, die Fachkräfte mit sicherheitsbehördlichem oder nachrichtendienstlichem Hintergrund gewinnen möchten. Gerade in den Bereichen Cybersicherheit, IT-Sicherheit, Schutz kritischer Infrastrukturen und sicherheitsrelevante Technologien ist ein geordneter Wissenstransfer zwischen Staat und Wirtschaft wichtig.

Bitkom regt daher an, Umfang, Fristen und Reichweite der betroffenen »dienstlichen Belange« klar zu definieren und ein praktikables, zügiges Genehmigungsverfahren vorzusehen. Für Unternehmen und betroffene Personen muss nachvollziehbar sein, welche Tätigkeiten anzeige- oder genehmigungspflichtig sind, wann eine Tätigkeit untersagt werden kann und innerhalb welcher Frist eine Entscheidung erfolgt.

6. Spezifische Anmerkungen zum BVerfSchG-E

6.1 Zu § 11 Abs. 6 BVerfSchG-E - Speicheranordnungen für künftig anfallende Daten

§ 11 Abs. 6 BVerfSchG-E ermöglicht es, anzuordnen, dass bestimmte künftig anfallende Daten für einen begrenzten Zeitraum gesichert werden. Eine solche Verpflichtung kann erheblichen technischen und organisatorischen Aufwand verursachen und bestehende Lösch- und Data-Retention-Konzepte der Unternehmen berühren.

Bitkom fordert daher eine präzisere gesetzliche Ausgestaltung. Der Entwurf sollte klar regeln, welche Datenkategorien betroffen sein können, für welchen Zeitraum eine Speicherung verlangt werden darf, unter welchen Voraussetzungen eine solche Anordnung ergehen kann und welche Anforderungen an die fortlaufende Sicherung neu anfallender Daten während des Anordnungszeitraums gelten. Zugleich muss klargestellt werden, dass Speicheranordnungen eng auf den konkreten Anlass begrenzt bleiben und keine allgemeine Pflicht zur Vorratsspeicherung begründen. Unternehmen müssen rechtssicher beurteilen können, welche Daten sie sichern dürfen, welche Daten sie weiterhin löschen müssen und wie sich eine Anordnung zu bestehenden datenschutzrechtlichen Löschpflichten verhält.

6.2 Zu § 13 Abs. 7 BVerfSchG-E - Rechtswegausschluss bis zur Benachrichtigung

§ 13 Abs. 7 BVerfSchG-E sieht vor, dass gegen bestimmte Ersuchen und deren Vollzug vor der Mitteilung an die betroffene Person der Rechtsweg ausgeschlossen ist.

Bitkom sieht diese Regelung kritisch. Sie kann dazu führen, dass Anbieter gegen an sie gerichtete Ersuchen keinen effektiven Rechtsschutz haben, obwohl sie unmittelbar verpflichtet werden und erhebliche technische, rechtliche oder wirtschaftliche Risiken tragen. Dies betrifft insbesondere Fälle, in denen ein Ersuchen überschießend, technisch nicht erfüllbar oder mit anderen gesetzlichen, europäischen, ausländischen oder vertraglichen Pflichten unvereinbar ist.

Geheimhaltung kann erforderlich sein, um laufende Maßnahmen, eingesetzte Personen und den Zweck einer Maßnahme zu schützen. Sie darf jedoch nicht dazu führen, dass Unternehmen rechtsschutzlos gestellt werden. Anbieter müssen die Möglichkeit haben, die Rechtmäßigkeit, Reichweite und technische Umsetzbarkeit eines an sie gerichteten Ersuchens überprüfen zu lassen.

Bitkom fordert daher ein eigenes, sofort ausübbares Beanstandungs- und Rechtsschutzrecht der Anbieter gegen an sie gerichtete Ersuchen. Zumindest sollte ein Vorlage- und Prüfungsrecht gegenüber dem Unabhängigen Kontrollrat vorgesehen werden. In Fällen, in denen ernsthafte Zweifel an der Rechtmäßigkeit, Verhältnismäßigkeit oder technischen Umsetzbarkeit eines Ersuchens bestehen, sollte dieses Prüfungsrecht aufschiebende Wirkung entfalten.

6.3 Zu § 13 Abs. 5 BVerfSchG-E - Unklare Unterstützungspflichten bei der Umleitung von Telekommunikation

§ 13 Abs. 5 BVerfSchG-E soll Anbieter von Telekommunikationsdiensten verpflichten, die Einbringung technischer Mittel zur Durchführung bestimmter Maßnahmen durch Unterstützung bei der Umleitung von Telekommunikation zu ermöglichen. Hierzu sollen unter anderem Informationen über Netzstrukturen, Telekommunikationsanlagen und Telekommunikationsdienste bereitgestellt sowie sonstige Unterstützungsleistungen erbracht werden. Die Vorschrift ist in ihrer jetzigen Fassung nicht hinreichend verständlich. Es bleibt unklar, worin die konkrete Unterstützungsleistung bestehen soll, welche technischen Informationen im Einzelnen bereitzustellen sind, welche Handlungen von den Verpflichteten erwartet werden und wo die Grenzen der Mitwirkung liegen. Gerade bei Maßnahmen, die Netzstrukturen, Telekommunikationsanlagen und Datenströme betreffen, sind präzise gesetzliche Vorgaben unerlässlich.

Bitkom fordert daher eine grundlegende Präzisierung von § 13 Abs. 5 BVerfSchG-E. Unternehmen müssen eindeutig erkennen können, welche technischen, organisatorischen und personellen Vorkehrungen sie treffen müssen. Die Regelung muss zudem sicherstellen, dass Mitwirkungspflichten nicht zu einer Schwächung von Sicherheits- oder Verschlüsselungsarchitekturen führen und keine Pflicht zur

Schaffung von Backdoors, Klartextzugängen oder strukturellen Schwächungen von Verschlüsselung begründen. Erforderlich sind klare Grenzen der Mitwirkung, ein standardisiertes Verfahren, sichere Übermittlungswege sowie eine eindeutige Verantwortungsverteilung zwischen Behörde und verpflichteten Unternehmen. Ohne diese Präzisierungen entstehen erhebliche Rechts- und Umsetzungsunsicherheiten für die betroffenen Anbieter.

7. Spezifische Anmerkungen zum BNDG-E

7.1 Zu § 10 BNDG-E - Übermittlung von Daten durch öffentliche Stellen an den Bundesnachrichtendienst, insbesondere BSI-Erkenntnisse zu Schwachstellen

§ 10 BNDG-E regelt die Übermittlung von Daten durch inländische öffentliche Stellen an den Bundesnachrichtendienst. Nach der Gesetzesbegründung sollen hiervon ausdrücklich auch Informationen des Bundesamtes für Sicherheit in der Informationstechnik im Zusammenhang mit Cybervorfällen erfasst sein. Dazu zählen auch Erkenntnisse über die technische Funktionsweise von Schwachstellen in IT-Systemen. Damit berührt die Regelung einen hochsensiblen Bereich der deutschen Cybersicherheitsarchitektur.

Bitkom erkennt an, dass ein wirksamer Informationsaustausch zwischen Sicherheitsbehörden für die Lagebewertung bei Cyberangriffen erforderlich sein kann. Gerade koordinierte, internationale Angriffskampagnen können eine behördenübergreifende Einordnung notwendig machen. Eine solche Zusammenarbeit darf jedoch nicht dazu führen, dass Informationen über Schwachstellen vorrangig nachrichtendienstlich nutzbar gemacht werden, statt ihre schnellstmögliche Behebung zu unterstützen. Der Schutz betroffener Systeme, die Schließung von Sicherheitslücken und die Stärkung der Cyberresilienz müssen Vorrang haben.

Das BSI hat den gesetzlichen Auftrag, die IT-Sicherheit in Deutschland zu stärken. Dieser Auftrag lebt in der Praxis in besonderem Maße von Vertrauen und partnerschaftlicher Zusammenarbeit mit der Wirtschaft. Unternehmen teilen Informationen zu Schwachstellen, Sicherheitsvorfällen und technischen Risiken mit dem BSI, weil sie darauf vertrauen können müssen, dass diese Informationen der Behebung von Sicherheitslücken und dem Schutz digitaler Infrastrukturen dienen. Eine verpflichtende Übermittlung solcher Erkenntnisse an den Bundesnachrichtendienst stellt dieses Vertrauensverhältnis in Frage, wenn dadurch der Eindruck entsteht, dass Informationen nicht primär zur Schwachstellenschließung, sondern auch zur nachrichtendienstlichen Nutzung weitergegeben werden.

Eine solche Entwicklung würde die Rolle des BSI als zentrale Vertrauensstelle für Cybersicherheit nachhaltig schwächen. Wenn Unternehmen befürchten müssen, dass gegenüber dem BSI offengelegte Schwachstelleninformationen an den BND weitergeleitet und dort für operative Zwecke genutzt werden könnten, droht dies die Bereitschaft zur freiwilligen, frühzeitigen und umfassenden Zusammenarbeit zu

beeinträchtigen. Damit würde nicht nur das Vertrauen in staatliche IT-Sicherheitsstrukturen beschädigt, sondern auch die Fähigkeit des Staates, Schwachstellen schnell zu erkennen, zu koordinieren und zu schließen.

Bitkom lehnt eine staatlich organisierte oder erleichterte Schwachstellenausnutzung auf Kosten privatwirtschaftlicher IT-Produkte und digitaler Infrastrukturen entschieden ab. Auch eine veränderte sicherheitspolitische Lage rechtfertigt es nicht, Sicherheitslücken in Softwareprodukten, Systemen oder digitalen Infrastrukturen der Wirtschaft offenzuhalten, zu verlängern oder aktiv zu nutzen. Der Staat muss privatwirtschaftliche Investitionen in sichere digitale Produkte schützen und darf sie nicht durch unklare Übermittlungs- und Nutzungsregelungen konterkarieren.

Erforderlich ist daher eine klare gesetzliche Absicherung des Vorrangs von Schwachstellenbehebung, Responsible Disclosure und IT-Sicherheit. Schwachstelleninformationen dürfen nur in einem Rahmen übermittelt werden, der sicherstellt, dass die Schließung der Schwachstelle, der Schutz betroffener Systeme und die Stärkung der Cyberresilienz Vorrang haben. Eine Übermittlung darf insbesondere nicht dazu führen, dass bekannte Sicherheitslücken länger offenbleiben oder für nachrichtendienstliche Zwecke ausgenutzt werden. Insbesondere darf die Übermittlung von Schwachstelleninformationen nicht dazu führen, dass Zero-Day-Schwachstellen zurückgehalten, gehortet oder für operative Zwecke offengehalten werden, statt sie im Wege eines geordneten Responsible-Disclosure-Prozesses schnellstmöglich zu schließen.

Bitkom fordert deshalb eine ausdrückliche Klarstellung, dass § 10 BNDG-E keine Grundlage für die operative Ausnutzung von Schwachstellen durch den Bundesnachrichtendienst schafft. Die Übermittlung von Schwachstelleninformationen muss eng begrenzt, dokumentiert, kontrolliert und eindeutig an den Zweck der Verbesserung der Cybersicherheit gebunden werden. Der Vorrang der Schwachstellenbehebung muss gesetzlich verankert werden.

8. Fazit und weiterer Handlungsbedarf

Bitkom unterstützt das Ziel, das Nachrichtendienstrecht angesichts der verschärften Sicherheits- und Bedrohungslage zu modernisieren und die Handlungsfähigkeit der Nachrichtendienste rechtsstaatlich weiterzuentwickeln. Hybride Angriffe, Cyberoperationen und die gezielte Destabilisierung staatlicher, wirtschaftlicher und gesellschaftlicher Strukturen erfordern leistungsfähige Sicherheitsbehörden und klare rechtliche Grundlagen.

Der vorliegende Entwurf enthält hierfür wichtige Ansätze, bedarf aus Sicht der Digitalwirtschaft jedoch an zentralen Stellen einer deutlichen Präzisierung. Dies gilt insbesondere für die neuen Auskunfts- und Mitwirkungspflichten für Unternehmen, den Zugriff auf Inhaltsdaten digitaler Dienste, den Umgang mit technischen Informationen und Systemkopien, die Reichweite des Marktortprinzips, Speicheranordnungen für künftig anfallende Daten, Sicherheitsüberprüfungen von Unternehmenspersonal, Ausleitungs- und Zugangspflichten, Durchsetzungsbefugnisse sowie Kostenerstattungsregelungen. Erforderlich sind klare Begriffsbestimmungen,

eine saubere Abgrenzung von Verantwortlichen und Auftragsverarbeitern, wirksame Vorgaben zu Zweckbindung, Löschung und Weitergabe übermittelter Daten, ein ausdrückliches Kooperations- und Subsidiaritätsprinzip beim Zugriff auf laufende IT- und Netzwerkinfrastrukturen, praxistaugliche Antwortfristen, effektiver Rechtsschutz für verpflichtete Unternehmen sowie eine realistische Ermittlung des Erfüllungsaufwands. Die Reform darf zudem nicht zu einer Schwächung der IT-Sicherheit führen. Ausleitungs- und Mitwirkungspflichten müssen technikneutral, standardisiert und ohne Verpflichtung zur Schwächung von Verschlüsselung oder sicheren Produktarchitekturen ausgestaltet werden. Ebenso muss gesetzlich abgesichert werden, dass Schwachstelleninformationen vorrangig der Schwachstellenbehebung, Responsible Disclosure und Stärkung der Cyberresilienz dienen und nicht zur operativen Ausnutzung offengehalten oder weitergegeben werden. Die Modernisierung des Nachrichtendienstrechts muss Sicherheit stärken, ohne Rechtsunsicherheit, unverhältnismäßige Belastungen oder eine Schwächung des Vertrauens in den Digitalstandort Deutschland zu erzeugen. Sie muss die Integrität digitaler Infrastrukturen, die Wettbewerbsfähigkeit der Digitalwirtschaft und den Schutz sensibler Unternehmens- und Kundendaten wahren.

Aufgrund der sehr kurzen Rückmeldefrist kann diese Stellungnahme keine abschließende Bewertung des gesamten Entwurfs leisten. Bitkom wird das weitere Gesetzgebungsverfahren konstruktiv begleiten und steht für eine vertiefte Erörterung der Auswirkungen auf die Digitalwirtschaft zur Verfügung.

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 500 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 +49 30 27576-279 | f.kuhlenkamp@bitkom.org

Benjamin Spindeldreier | Junior Manager DefTech & Sicherheit
T +49 30 27576-379 | b.spindeldreier@bitkom.org

Verantwortliches Bitkom-Gremium

AK Sicherheitspolitik
AK Öffentliche Sicherheit