

Stellungnahme

September 2026

Regierungsentwurf 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.

Nachrichtendiensten kommt vor diesem Hintergrund eine zentrale Rolle für die Verteidigungsfähigkeit und Resilienz Deutschlands zu. Die 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.

Bitkom begrüßt, dass der Regierungsentwurf gegenüber dem Referentenentwurf an mehreren wichtigen Stellen nachgebessert wurde. Positiv hervorzuheben sind insbesondere die klarere Definition digitaler Dienste und die höheren Schutzanforderungen für Daten in Cloud-Computing-Diensten. Zu begrüßen sind zudem die neuen Schutzklauseln für die Meldestellenfunktion des BSI, der vorgesehene operative Informationsaustausch der Nachrichtendienste mit einzelnen nichtöffentlichen Stellen nach § 50 BVerfSchG-E und § 85 BNDG-E sowie der gesetzliche Kooperationsrahmen bei IT-Angriffen. Dies gilt ebenso für die Möglichkeit, Angriffswerkzeuge nach Erstellung einer Sicherungskopie zu löschen, und für die gestärkte unabhängige Rechtskontrolle. Auch der Wegfall des Kriteriums des

83%

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

»beherrschenden Einflusses« beim verdeckten Zugriff des BND auf Systeme inländischer Anbieter ist zu begrüßen.

Gleichzeitig bleiben erhebliche rechtliche, technische und praktische Fragen offen. Dies gilt insbesondere für Zugriffe auf sensible Inhaltsdaten ohne durchgehend hohe Eingriffsschwellen und unabhängige Vorabkontrolle, für internationale Pflichtenkollisionen sowie für die Herausgabe umfangreicher Systemkopien und verdeckte Zugriffe auf IT-Infrastrukturen von Anbietern. Klärungsbedarf besteht zudem bei Sicherheitsüberprüfungen von Unternehmenspersonal, technischen Ausleitungs- und Zugangspflichten, der Absenkung des Schutzniveaus für bestimmte gespeicherte Kommunikationsinhalte im BNDG-E sowie bei weitreichenden Durchsetzungsbefugnissen, dem Rechtsschutz verpflichteter Unternehmen und dem tatsächlichen Erfüllungsaufwand 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.

Der Bitkom fordert daher eine weitere Präzisierung des Regierungsentwurfs. Notwendig sind insbesondere höhere Eingriffsschwellen und eine unabhängige Vorabkontrolle beim Zugriff auf sensible Inhaltsdaten sowie klare Kollisionsregeln und rechtssichere internationale Übermittlungswege. Darüber hinaus braucht es belastbare Vorgaben zu Zweckbindung, Löschung und Weitergabe übermittelter Daten, ein konsequentes Kooperations- und Subsidiaritätsprinzip bei Eingriffen in IT-Infrastrukturen sowie einen eigenständigen und unmittelbar ausübbarer Rechtsschutz für verpflichtete Unternehmen. Verpflichtende vorsorgliche Sicherheitsüberprüfungen auf Vorrat sollten entfallen. Zugleich muss gesetzlich klargestellt werden, dass Mitwirkungspflichten keine Schwächung sicherer Verschlüsselungs- und Produktarchitekturen verlangen dürfen. Für Schwachstelleninformationen des BSI braucht es ein stärkeres gesetzliches Schutzregime einschließlich eines geregelten Vulnerabilities-Equities-Prozesses. Der Erfüllungsaufwand der Wirtschaft muss realistisch ermittelt und die nachgewiesenen tatsächlichen Kosten vollständig erstattet werden.

2. Einordnung des Regierungsentwurfs

Bitkom hat den Referentenentwurf zur Reform des Nachrichtendienstrechts bereits im Juli 2026 kommentiert und dabei insbesondere die Auswirkungen der neuen Auskunftspflichten und Mitwirkungspflichten auf die Digitalwirtschaft adressiert. Vor diesem Hintergrund richtet die vorliegende Stellungnahme den Blick gezielt auf diejenigen Regelungen, die für Unternehmen der Digitalwirtschaft weiterhin besondere rechtliche, technische oder operative Auswirkungen entfalten. Im Mittelpunkt stehen dabei die praktische Umsetzbarkeit neuer Auskunftspflichten und Mitwirkungspflichten, ihr Zusammenspiel mit bestehenden gesetzlichen und vertraglichen Verpflichtungen sowie die erforderlichen Schutzmechanismen bei staatlichen Eingriffen in Daten und IT-Infrastrukturen. Die Stellungnahme fokussiert damit auf den aus Sicht der Digitalwirtschaft wesentlichen Anpassungsbedarf und erhebt keinen Anspruch auf eine abschließende Bewertung des gesamten Regierungsentwurfs.

3. Begrüßenswerte Weiterentwicklungen

Bitkom bewertet positiv, dass der Regierungsentwurf an mehreren Stellen einen klareren und konsolidierten Rechtsrahmen für die Tätigkeit der Nachrichtendienste schaffen will. Die Zusammenführung bislang verstreuter Regelungen, das abgestufte Schwellensystem sowie die stärkere unabhängige Kontrolle können zu mehr Normenklarheit, Vorhersehbarkeit und Rechtssicherheit beitragen.

Mehr Rechtssicherheit schafft insbesondere die nun ausdrücklich vorgenommene Anknüpfung des Begriffs der digitalen Dienste an § 1 Abs. 4 Nr. 1 des Digitale-Dienste-Gesetzes. Für das BVerfSchG-E erfolgt dies in § 11 Abs. 1 Nr. 1 Buchst. b, für das BNDG-E in § 12 Abs. 2 Nr. 6. Eine zentrale Kritik am Referentenentwurf wird damit aufgegriffen. Die gesetzliche Bezugnahme schafft mehr Klarheit darüber, welche Dienste von den entsprechenden Verpflichtungen erfasst werden.

Der besonderen Sensibilität von Inhaltsdaten in Cloud-Computing-Diensten trägt der Regierungsentwurf nun deutlich stärker Rechnung. § 11 Abs. 5 BVerfSchG-E und § 13 Abs. 6 BNDG-E knüpfen Auskünfte über Daten, die Nutzerinnen und Nutzer in Cloud-Computing-Diensten verarbeiten, nun an deutlich höhere Anforderungen. Damit wird der besonderen Sensibilität dieser Daten stärker Rechnung getragen. Diese Differenzierung ist aus Sicht von Bitkom ausdrücklich zu begrüßen.

Auch beim Schutz besonders sensibler institutioneller Funktionen enthält der Regierungsentwurf wichtige zusätzliche Sicherungen. Nach § 10 Abs. 7 Nr. 2 BVerfSchG-E und § 10 Abs. 4 Nr. 2 BNDG-E greifen Übermittlungspflichten nicht, wenn eine Übermittlung im Widerspruch zu den Aufgaben des BSI als Meldestelle nach den §§ 4 und 5 des BSI-Gesetzes stünde. Damit wird die besondere Vertrauensfunktion des BSI gegenüber Wirtschaft und Verwaltung stärker berücksichtigt. Ebenfalls positiv sind zusätzliche institutionelle Sicherungen bei Betriebsuntersagungen. § 71 Abs. 2 BVerfSchG-E verlangt hierfür das Einvernehmen mit dem Bundesministerium für Digitales und Staatsmodernisierung. Nach § 134 Abs. 2 BNDG-E ist das Einvernehmen mit der Bundesnetzagentur erforderlich. Dass derartige besonders weitreichende Maßnahmen nicht ohne die Beteiligung fachlich zuständiger Stellen erfolgen sollen, stärkt die Verhältnismäßigkeitsprüfung und trägt den möglichen Auswirkungen auf digitale Infrastrukturen besser Rechnung.

Für die Zusammenarbeit zwischen Nachrichtendiensten und Wirtschaft schafft der Regierungsentwurf zugleich neue Ansatzpunkte für einen stärker operativ ausgerichteten Informationsaustausch. Bitkom begrüßt in diesem Zusammenhang die Möglichkeiten zur Information von Öffentlichkeit und Fachkreisen nach § 45 BVerfSchG-E und § 69 BNDG-E. Von besonderer Bedeutung für einen operativen Austausch mit der Wirtschaft sind jedoch die weitergehenden Regelungen in § 50 BVerfSchG-E und § 85 BNDG-E. Sie ermöglichen unter gesetzlich bestimmten Voraussetzungen die gezielte Übermittlung personenbezogener Daten an inländische nichtöffentliche Stellen, unter anderem zum Schutz der Sicherheit in der Informationstechnik und zum Schutz von Unternehmen vor sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten. Damit wird eine wichtige Grundlage für einen CTIP-orientierten Austausch geschaffen, bei dem konkrete und handlungsrelevante Erkenntnisse gezielt an betroffene Unternehmen weitergegeben werden können.

Diese Übermittlungsbefugnisse sollten im weiteren Gesetzgebungsverfahren erhalten bleiben.

Ein praxisrelevanter Fortschritt liegt zudem im vorgesehenen Kooperationsrahmen bei informationstechnischen Angriffen nach § 12 BVerfSchG-E und § 14 BNDG-E.

Besonders wichtig ist dabei die Möglichkeit, im System gespeicherte Angriffswerkzeuge oder durch den Angriff beschaffte Daten nach Erstellung einer Sicherungskopie zu löschen. Diese Regelung schafft die notwendige Rechtsgrundlage für eine schnelle Remediation betroffener Systeme und sollte im weiteren Gesetzgebungsverfahren ausdrücklich erhalten bleiben.

Die vorgesehene Stärkung des Unabhängigen Kontrollrats setzt zugleich einen wichtigen rechtsstaatlichen Akzent. Hervorzuheben sind insbesondere die administrative Kontrolle der Datenverarbeitung sowohl des Bundesamtes für Verfassungsschutz als auch des Bundesnachrichtendienstes nach § 32 UKRatG-E sowie die Möglichkeit unangekündigter Kontrollen im Rahmen des Prüfprogramms nach § 26 UKRatG-E. Die Vorabkontrolle nach § 27 UKRatG-E ermöglicht zudem eine eigenständige Prüfung der Rechtmäßigkeit und verbindliche Maßgaben für die Durchführung der jeweiligen Maßnahme. Diese Kontrollarchitektur sollte konsequent auch für den Rechtsschutz verpflichteter Unternehmen nutzbar gemacht werden.

Eine zentrale Grenze staatlicher Mitwirkungspflichten wahrt der Regierungsentwurf bislang beim Schutz sicherer Verschlüsselung. Ein allgemeines Entschlüsselungs- oder Backdoor-Mandat ist nicht vorgesehen. Diese rote Linie muss im weiteren Gesetzgebungsverfahren zwingend erhalten bleiben und sollte ausdrücklich im Gesetzestext abgesichert werden.

An einer besonders eingriffsintensiven Stelle wurde der Regierungsentwurf gegenüber dem Referentenentwurf zudem substantiell korrigiert. Die in § 32 Abs. 2 BNDG-E zunächst vorgesehene Möglichkeit eines Zugriffs aufgrund eines »beherrschenden Einflusses« auf einen Anbieter ist im Regierungsentwurf entfallen. Die verbleibenden Fallgruppen knüpfen stattdessen insbesondere an die Nichterfüllung eines rechtmäßigen verpflichtenden Ersuchens oder an konkrete operative Geheimhaltungsrisiken an. Die Streichung des Kriteriums des »beherrschenden Einflusses« ist aus Sicht des Bitkom ausdrücklich zu begrüßen und sollte im weiteren Verfahren erhalten bleiben.

4. Allgemeine und querschnittliche Anmerkungen

4.1 Transparenz und Kontrolle

Der Regierungsentwurf sieht mit den §§ 11 bis 15 BVerfSchG-E sowie den §§ 12 bis 16 BNDG-E weitreichende Auskunftspflicht und Mitwirkungspflichten privater Unternehmen vor. Zugleich fehlen weiterhin hinreichende öffentliche Informationen darüber, in welchem Umfang private Unternehmen tatsächlich in Anspruch genommen werden.

Für eine belastbare Evaluierung der neuen Regelungen sollte nachvollziehbar sein, wie häufig Unternehmenspflichten zur Anwendung kommen, welche Datenkategorien betroffen sind, welche Kosten entstehen und wie häufig unabhängige Kontrollmechanismen greifen. Die in § 34 BVerfSchG-E und § 97 BNDG-E vorgesehene unabhängige Vorabkontrolle besonders eingriffsintensiver Maßnahmen ist hierfür ein wichtiger Ausgangspunkt, ermöglicht aber noch keine hinreichende Transparenz über die tatsächliche Inanspruchnahme der Wirtschaft. Bitkom regt daher einen jährlichen Transparenzbericht des Unabhängigen Kontrollrats über die Inanspruchnahme privater Unternehmen an. Dieser sollte aggregierte und anonymisierte Angaben zur Zahl der Auskunftersuchen, zu betroffenen Datenkategorien, ersuchenden Behörden, Vorabkontrollverfahren, Normkonflikten und Entschädigungsleistungen enthalten. Zudem sollte Unternehmen ermöglicht werden, nach Ablauf angemessener Sperrfristen aggregierte Angaben über die Anzahl der an sie gerichteten Auskunftersuchen in eigenen Transparenzberichten zu veröffentlichen, soweit keine überwiegenden Sicherheitsinteressen entgegenstehen.

4.2 Normkonflikte mit EU-Recht, ausländischem Recht und Kundenverträgen

Der Regierungsentwurf knüpft Unternehmenspflichten teilweise daran, dass ein Unternehmen in Deutschland eine Niederlassung hat oder hier Leistungen erbringt beziehungsweise an deren Erbringung mitwirkt. Für das BVerfSchG-E ergibt sich dies insbesondere aus § 11 Abs. 2, für das BNDG-E aus § 16 Abs. 1. Damit können auch internationale Anbieter und grenzüberschreitende Konzernstrukturen von den Pflichten erfasst werden.

Bitkom unterstützt das Ziel eines Level Playing Field. Vergleichbare Dienste sollten vergleichbaren rechtlichen Anforderungen unterliegen. Eine Anknüpfung allein an den Markort kann insbesondere bei grenzüberschreitend tätigen Unternehmen zu konkurrierenden Verpflichtungen und unauflösbaren Rechtskonflikten führen. Dies betrifft insbesondere Konflikte zwischen deutschen Auskunfts- und Geheimhaltungspflichten, europäischem Datenschutzrecht, zwingendem ausländischem Recht und vertraglichen Informationspflichten gegenüber Kundinnen und Kunden. § 9 Abs. 3 BVerfSchG-E sieht weitreichende Mitteilungsverbote vor. § 11 Abs. 2 Satz 3 BVerfSchG-E enthält zwar eine Ausnahme von der Geheimhaltungspflicht, wenn eine Stelle keine Niederlassung in Deutschland hat und das Recht ihres Sitzstaates der Geheimhaltung entgegensteht. Diese Ausnahme löst die Problematik jedoch nicht vollständig, insbesondere wenn ein international tätiges Unternehmen eine Niederlassung in Deutschland unterhält oder andere zwingende Rechtspflichten betroffen sind. In solchen Fällen sollte daher das Herkunftslandprinzip maßgeblich sein.

Der Bitkom fordert eine umfassende gesetzliche Kollisionsregel. Eine Freistellung darf sich nicht allein auf die Geheimhaltungspflicht beziehen, sondern muss auch die Auskunfts- oder Mitwirkungspflicht selbst erfassen, soweit deren Erfüllung gegen zwingendes Unionsrecht oder zwingendes Recht eines anderen Staates verstoßen würde. Eine solche Regelung darf zudem nicht auf Unternehmen ohne deutsche

Niederlassung beschränkt sein. Auch international tätige Unternehmen mit einer Niederlassung in Deutschland können in unauflösbare Pflichtenkollisionen geraten.

Soweit eine unmittelbare Erfüllung des Ersuchens wegen entgegenstehenden Rechts nicht möglich ist, sollten rechtssichere staatliche Kanäle genutzt werden. Hierzu zählen, soweit für den jeweiligen Sachverhalt einschlägig, Verfahren der internationalen Rechtshilfe wie Mutual Legal Assistance Treaties (MLAT), die europäischen e-Evidence-Instrumente sowie einschlägige EU-US-Regelungen für den grenzüberschreitenden Datenzugang. Der Gesetzgeber sollte diese Instrumente ausdrücklich benennen und ein Verfahren vorsehen, über das Normkonflikte vor einer Datenübermittlung verbindlich geklärt werden können. Auch das Verhältnis zu zwingenden Informationspflichten gegenüber Kundinnen und Kunden muss ausdrücklich geregelt werden.

Dies gilt auch für die Rollenverteilung zwischen Verantwortlichen und Auftragsverarbeitern. In komplexen Cloud-, Hosting- und Managed-Service-Strukturen verfügen Auftragsverarbeiter häufig weder über die rechtliche Entscheidungsbefugnis noch über den vollständigen Kontext der verarbeiteten Daten. Ersuchen sollten daher grundsätzlich vorrangig an den datenschutzrechtlichen Verantwortlichen gerichtet werden, soweit dessen Inanspruchnahme rechtlich und tatsächlich möglich ist.

In diesen Fällen muss der Auftragsverarbeiter von der Haftung gegenüber seinem Auftraggeber freigestellt werden, sofern er einem rechtmäßigen Ersuchen nachkommt. Bitkom fordert eine gesetzliche Klarstellung, dass die Erfüllung einer behördlichen Auskunftspflicht keinen Verstoß gegen vertragliche Geheimhaltungs- oder Datenschutzvereinbarungen begründet.

Bitkom fordert einen gesetzlichen Auflösungsmechanismus für solche Kollisionsfälle. Solange ein Unternehmen nachweislich und unverzüglich die Auflösung einer Pflichtenkollision betreibt, darf weder ein Zwangsgeld nach § 71 Abs. 3 BVerfSchG-E noch eine Betriebsuntersagung verhängt werden. Es sollte eine unabhängige Stelle (etwa der Unabhängige Kontrollrat) befugt sein, im Kollisionsfall eine verbindliche Entscheidung über den Vorrang zu treffen.

4.3 Zweckbindung, Löschung und Weitergabe übermittelter Daten

Für Unternehmen ist nicht nur entscheidend, unter welchen Voraussetzungen sie Daten übermitteln müssen. Ebenso wichtig ist, was nach der Übermittlung mit diesen Daten geschieht.

Der Regierungsentwurf enthält verschiedene Zweckbindungs-, Kontroll- und Löschregelungen. Dazu gehören insbesondere die allgemeinen Weiterverarbeitungsregelungen nach § 36 BVerfSchG-E und § 52 BNDG-E sowie weitere Vorgaben zur Löschung und Übermittlung. Im BNDG-E regelt § 70 ausdrücklich die Zweckbindung übermittelter personenbezogener Daten. Für Daten aus der technischen Aufklärung enthalten insbesondere die §§ 64 bis 66 BNDG-E zusätzliche Vorgaben. Angesichts der Sensibilität der betroffenen Unternehmens-, Kunden- und

Infrastrukturdaten ist jedoch ein konsistentes Schutzniveau über sämtliche einschlägigen Befugnisse hinweg erforderlich.

Der Bitkom fordert daher durchgängige und klare Vorgaben 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 jeweiligen Zweck nicht mehr erforderlich sind. Eine Weitergabe an andere Behörden oder ausländische Stellen muss besonders begründet, dokumentiert und auf das erforderliche Maß begrenzt werden.

4.4 Erfüllungsaufwand der Wirtschaft

Der im Regierungsentwurf angesetzte Erfüllungsaufwand der Wirtschaft erscheint weiterhin nicht plausibel. Für das Bedienen von Ersuchen des Bundesnachrichtendienstes nach den §§ 12 ff. BNDG-E werden lediglich rund 50.000 Euro zusätzliche Aufwände pro Jahr angesetzt. Für entsprechende Ersuchen des Bundesamtes für Verfassungsschutz enthält der Entwurf ausdrücklich keine valide Schätzung. Demgegenüber prognostiziert der Regierungsentwurf allein für das Bundesamt für Verfassungsschutz Haushaltsausgaben ohne Erfüllungsaufwand in Höhe von jährlich 269 Mio. Euro zuzüglich noch nicht bezifferter Personalmittel sowie einen einmaligen Mehrbedarf von rund 97 Mio. Euro. Diese Größenordnungen verdeutlichen, dass auch auf Seiten der verpflichteten Unternehmen eine belastbare und differenzierte Aufwandsermittlung erforderlich ist.

Bitkom fordert daher eine transparente Neuerhebung des Erfüllungsaufwands unter Einbeziehung der tatsächlich betroffenen Unternehmen. Dabei sind insbesondere die erwartete Anzahl und Komplexität der Ersuchen, technische Implementierungen, der Personal- und Rechtsprüfungsaufwand, Sicherheitsüberprüfungen, Dokumentationspflichten und erforderliche Bereitschaftsstrukturen zu berücksichtigen. Zugleich müssen die Kostenerstattungsregelungen vereinheitlicht werden. Die Beschränkung der Entschädigung nach § 11 Abs. 7 Satz 3 BVerfSchG-E auf die Vorgaben des Justizvergütungs- und -entschädigungsgesetzes wird dem tatsächlichen Aufwand komplexer technischer Auskunft- und Mitwirkungsleistungen nicht gerecht. Diese Beschränkung sollte gestrichen und die Erstattung nach dem Vorbild des § 16 Abs. 4 BNDG-E auf die vollständigen, nachgewiesenen tatsächlichen Kosten umgestellt werden.

4.5 Antwortfristen auf Auskunftersuchen

Auskunfts- und Mitwirkungspflichten können nur dann zuverlässig erfüllt werden, wenn die gesetzlichen Anforderungen mit den tatsächlichen betrieblichen Abläufen vereinbar sind.

§ 16 Abs. 3 BNDG-E verpflichtet die betroffenen Stellen ausdrücklich dazu, einem Ersuchen unverzüglich und vollständig zu entsprechen. Im BVerfSchG-E findet sich für die Unternehmenspflichten nach den §§ 11 bis 15 keine entsprechende ausdrückliche Regelung. Die Gesetzesbegründung geht jedoch davon aus, dass öffentlich-rechtliche Pflichten allgemein unverzüglich und vollständig zu erfüllen sind. 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 in Anlehnung an die e-Evidence-Verordnung ein Regelzeitraum von zehn Tagen vorgesehen werden.

5. Übergreifende Anmerkungen zu Unternehmenspflichten 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. 1 Nr. 1 Buchst. b, Abs. 3 Nr. 2 Buchst. b und Abs. 5 BVerfSchG-E sowie § 12 Abs. 2 Nr. 6 und § 13 Abs. 1 und 6 BNDG-E: Zugriff auf Inhaltsdaten digitaler Dienste und Cloud-Computing-Dienste

Bitkom begrüßt ausdrücklich, dass der Regierungsentwurf die Anforderungen für Auskünfte über Daten erhöht, die Nutzerinnen und Nutzer in Cloud-Computing-Diensten verarbeiten. § 11 Abs. 5 BVerfSchG-E und § 13 Abs. 6 BNDG-E knüpfen den Zugriff auf solche Daten an die Voraussetzungen der jeweiligen Befugnisse für Eingriffe in informationstechnische Systeme. Damit wird eine wesentliche Kritik am Referentenentwurf aufgegriffen. Die Verarbeitung von Daten in Cloud-Umgebungen kann besonders sensible Inhalte betreffen, darunter vertrauliche Kommunikation, Geschäftsgeheimnisse, Gesundheitsdaten, Unternehmensdaten oder andere schutzwürdige Informationen. Es ist daher richtig, derartige Zugriffe nicht wie gewöhnliche Bestands- oder Nutzungsdaten zu behandeln, sondern sie an höhere Eingriffsvoraussetzungen und Kontrollmechanismen zu knüpfen.

Offen bleibt jedoch die Behandlung sensibler Inhaltsdaten anderer digitaler Dienste. Nach § 11 Abs. 3 Nr. 2 Buchst. b BVerfSchG-E umfasst die qualifizierte Auskunft weiterhin auch Inhalte von Nutzungen. Vergleichbare qualifizierte Auskunftersuchen gegenüber digitalen Diensten sind im BNDG-E in § 13 vorgesehen. Auch außerhalb klassischer Cloud-Computing-Dienste können solche Inhalte erhebliche Rückschlüsse auf Kommunikation, Verhalten, Interessen, Geschäftsbeziehungen und persönliche Lebensführung ermöglichen.

Bitkom fordert daher, für besonders sensible Inhaltsdaten digitaler Dienste ein einheitlich hohes Schutzniveau sicherzustellen. Für den Zugriff auf »Inhalte von Nutzungen« nach § 11 Abs. 3 Nr. 2 Buchst. b BVerfSchG-E sollte die höhere Schwelle einer besonders erheblich beobachtungsbedürftigen Bedrohung gelten. Die derzeit

vorgesehene Schwelle einer wenigstens erheblich beobachtungsbedürftigen Bedrohung wird der Sensibilität dieser Daten nicht in allen Fällen gerecht.

Zugleich darf die unabhängige Vorabkontrolle nicht davon abhängen, ob der jeweilige Dienst formal als Cloud-Computing-Dienst im Sinne des § 2 Nr. 4 BSI-Gesetzes eingeordnet wird. Vergleichbar sensible Inhaltsdaten anderer digitaler Dienste müssen einem vergleichbaren Kontrollniveau unterliegen. Maßgeblich für Schutzwelle und Vorabkontrolle sollte die Eingriffsintensität der Datenerhebung sein und nicht allein die technische oder regulatorische Einordnung des Dienstes. Zudem sollte klargestellt werden, dass Ersuchen vorrangig an den Verantwortlichen und nicht an reine Auftragsverarbeiter zu richten sind, soweit dies rechtlich und technisch möglich ist.

5.2 Zu § 12 Abs. 1 bis 4 BVerfSchG-E und § 14 Abs. 1 bis 3 BNDG-E: Technische Informationen, personenbezogene Daten, Systemkopien und Data at Source

Die nach § 12 Abs. 1 BVerfSchG-E und § 14 Abs. 1 BNDG-E herauszugebenden technischen Informationen können hochsensibel sein. Sie können Rückschlüsse auf Netzarchitekturen, Sicherheitsmechanismen, Protokolldaten, Angriffserkenntnisse, Kundensysteme, Schwachstellen und interne Schutzmaßnahmen der betroffenen Unternehmen ermöglichen.

Bitkom fordert daher, gesetzlich klarzustellen, dass solche Informationen nur über gesicherte Schnittstellen übermittelt und beim Empfänger ausschließlich in einer angemessen gesicherten Verarbeitungsumgebung verarbeitet werden dürfen. Zugriff, Verarbeitung und Weitergabe müssen einem strengen Need-to-know-Prinzip folgen und auf klar definierten Berechtigungs- und Protokollierungskonzepten beruhen. Besonders eingriffsintensiv ist weiterhin die Möglichkeit nach § 12 Abs. 2 BVerfSchG-E und § 14 Abs. 2 BNDG-E, Kopien von Teilen informationstechnischer Systeme herauszuverlangen, wenn eine gezielte Auskunft technisch nicht möglich oder nicht zumutbar ist. Positiv ist, dass insbesondere im BNDG-E zusätzliche Anforderungen und eine Vorabkontrolle für entsprechende Herausgabeverlangen vorgesehen sind. Gleichwohl bleibt der Begriff der »Teile des informationstechnischen Systems« weit. In mandantenfähigen Cloud- und Hosting-Umgebungen besteht das Risiko, dass neben angriffsbezogenen Informationen auch Daten unbeteiligter Dritter oder anderer Kunden miterfasst werden.

Bitkom fordert daher, die Herausgabe von Systemkopien auf technisch isolierbare und für den konkreten Zweck erforderliche Datenbestände zu begrenzen. Daten anderer Mandanten und unbeteiligter Dritter dürfen nicht miterfasst werden, soweit sie technisch abtrennbar sind. Vorrang muss grundsätzlich die Auskunft oder Analyse durch den Betreiber selbst haben. Das Prinzip »Data at Source« ist in solchen Konstellationen regelmäßig sicherer, zielgenauer und grundrechtsschonender als die Übermittlung umfangreicher Systemkopien.

Kritisch bleibt insbesondere § 12 Abs. 4 Satz 3 BVerfSchG-E. Danach kann die Löschung nicht erforderlicher Daten unter bestimmten Voraussetzungen unterbleiben, wenn

deren Trennung nicht oder nur mit unververtretbarem Aufwand möglich ist. Gerade bei umfangreichen Systemkopien muss sichergestellt werden, dass für die konkrete Aufklärung nicht erforderliche Daten unverzüglich ausgesondert und gelöscht werden. Für vom BND im Rahmen von § 36 BNDG-E erhobene Kopien sieht § 65 Abs. 4 BNDG-E demgegenüber ausdrücklich eine unverzügliche Prüfung und Löschung weiterer personenbezogener Daten vor.

Bitkom fordert daher die Streichung des § 12 Abs. 4 Satz 3 BVerfSchG-E. Die Möglichkeit, nicht erforderliche personenbezogene Daten allein wegen eines als unververtretbar bewerteten Trennungsaufwands weiter vorzuhalten, schwächt die Begrenzungswirkung der gesetzlichen Löschpflicht gerade bei besonders umfangreichen Systemkopien. Hilfsweise sollte die Regelung an das Schutzniveau des § 65 Abs. 4 BNDG-E angeglichen und eine unverzügliche Prüfung, Aussonderung und Löschung nicht erforderlicher personenbezogener Daten verbindlich vorgeschrieben werden.

Unverändert begrüßt Bitkom in diesem Zusammenhang die Möglichkeit nach § 12 Abs. 5 BVerfSchG-E beziehungsweise § 14 Abs. 4 BNDG-E, Angriffswerkzeuge nach Herstellung einer Sicherungskopie aus dem betroffenen System zu löschen. Damit wird eine schnelle Remediation rechtlich abgesichert. Die Regelung sollte deshalb ausdrücklich erhalten bleiben.

5.3 Zu §§ 12 und 24 BVerfSchG-E sowie §§ 14 und 36 BNDG-E: Subsidiarität und Betreiberbeteiligung bei Eingriffen in laufende IT- und Netzwerkinfrastrukturen

Bitkom begrüßt, dass der Regierungsentwurf und seine Begründung an verschiedenen Stellen subsidiäre Elemente enthalten und eine vorrangige Informationsgewinnung ohne invasive Eingriffe in Systeme anlegen.

Dies zeigt sich insbesondere im Verhältnis von § 12 zu § 24 BVerfSchG-E sowie von § 14 zu § 36 BNDG-E. Ein unmittelbarer Zugriff durch den jeweiligen Nachrichtendienst auf informationstechnische Systeme soll grundsätzlich erst möglich sein, wenn die erforderlichen Informationen nicht oder nicht ohne Gefährdung des Zwecks der Maßnahme durch Auskunft beziehungsweise Mitwirkung des Betreibers gewonnen werden können.

Dieser Ansatz sollte jedoch konsequent und einheitlich für sämtliche Maßnahmen gelten, die laufende IT- und Netzwerkinfrastrukturen betreffen.

Eingriffe in solche Systeme können erhebliche Betriebsrisiken verursachen. In Cloud-, Hosting-, Telekommunikations- und Managed-Service-Umgebungen können sie über das eigentliche Zielobjekt hinauswirken und die Verfügbarkeit oder Integrität von Systemen unbeteiligter Kunden beeinträchtigen.

Bitkom fordert daher ein ausdrückliches und durchgängiges Subsidiaritäts- und Kooperationsprinzip. Eingriffe in laufende Betriebsinfrastruktur dürfen nur erfolgen, wenn die erforderlichen Erkenntnisse nicht durch weniger eingriffsintensive Maßnahmen gewonnen werden können, insbesondere durch die Auswertung bereits

vorhandener Protokolldaten, Auskünfte des Betreibers oder eine technische Analyse unter Einbindung des betroffenen Unternehmens. Die Betreiber verfügen regelmäßig über die besten Kenntnisse ihrer Systeme, Datenflüsse, Mandantenstrukturen und Sicherheitsmechanismen. Ihre Einbindung ist deshalb nicht nur grundrechtsschonender, sondern auch operativ sicherer. Der Betreiber sollte vor einem Eingriff über Umfang und technische Durchführung der Maßnahme informiert und soweit möglich einbezogen werden. Soweit eine vorherige Unterrichtung den Zweck der Maßnahme gefährden würde, sollte eine nachträgliche Unterrichtung vorgesehen werden.

Zudem muss gewährleistet werden, dass Maßnahmen keine kaskadierenden Effekte auslösen oder die Verfügbarkeit von Diensten für unbeteiligte Dritte gefährden.

Bitkom fordert eine gesetzliche Haftungsfreistellung des Betreibers gegenüber seinen Kunden und Vertragspartnern für Schäden, die durch einen hoheitlich angeordneten oder durchgeführten Eingriff in seine Systeme verursacht werden und die der Betreiber weder veranlasst noch durch Unterlassen ermöglicht hat. Für Schäden und Folgen, die dem Betreiber selbst durch den hoheitlichen Eingriff entstehen, greifen die allgemeinen Grundsätze der Staatshaftung (Art. 34 GG i.V.m. § 839 BGB) bzw. des enteignungsgleichen Eingriffs sowie der (Vollzugs-)Folgenbeseitigung. Eine spezialgesetzliche Entschädigungsregelung im Reformgesetz ist daher systematisch nicht erforderlich – wohl aber die Klarstellung, dass die Befolgung einer behördlichen Anordnung den Betreiber von seiner vertraglichen Leistungspflicht und Haftung gegenüber Dritten befreit (vergleichbar § 8 Abs. 3 BSIG).

Dieses Subsidiaritätsprinzip muss ausdrücklich auch den verdeckten Zugriff nach § 32 Abs. 2 BNDG-E erfassen. Der Regierungsentwurf ermöglicht einen Zugriff auf informationstechnische Systeme inländischer Anbieter ohne deren Wissen unter anderem dann, wenn einem rechtmäßigen verpflichtenden Auskunftersuchen nicht nachgekommen wird oder konkrete tatsächliche Anhaltspunkte dafür bestehen, dass ein Ersuchen offengelegt und dadurch der Zweck der Maßnahme gefährdet würde. Gerade ein solcher verdeckter Zugriff kann erhebliche Risiken für die Integrität und Verfügbarkeit produktiver Infrastrukturen auslösen und sollte deshalb nur zulässig sein, wenn weniger eingriffsintensive Möglichkeiten tatsächlich ausscheiden.

Bitkom begrüßt zugleich ausdrücklich, dass das im Referentenentwurf enthaltene Kriterium des »beherrschenden Einflusses« im Regierungsentwurf entfallen ist. Damit wird eine besonders weit gefasste Zugriffsmöglichkeit zurückgenommen. Diese Streichung sollte im weiteren Gesetzgebungsverfahren erhalten bleiben.

5.4 Zu § 13 Abs. 6 BVerfSchG-E sowie § 13 Abs. 7 BNDG-E: Sicherheitsüberprüfung und Geheimschutz bei Unternehmenspersonal

Die Regelungen zur Sicherheitsüberprüfung von Unternehmenspersonal werfen weiterhin erhebliche praktische Fragen auf. § 13 Abs. 6 BVerfSchG-E verpflichtet Anbieter von Telekommunikationsdiensten unter anderem dazu, geeignetes Personal vorzuhalten, das bereit ist, sich einer einfachen Sicherheitsüberprüfung zu unterziehen.

Bei qualifizierten Ersuchen oder deren Ankündigung müssen die für die Durchführung vorgesehenen Personen unverzüglich ausgewählt und einer Sicherheitsüberprüfung unterzogen werden. Vergleichbare Vorgaben enthält § 13 Abs. 7 BNDG-E. Dort kann der Bundesnachrichtendienst zudem anordnen, dass Sicherheitsüberprüfungen bereits als organisatorische Vorkehrung für künftige Überwachungsmaßnahmen durchgeführt werden.

Bitkom unterstützt Geheimschutz und einen vertrauensvollen, sicheren Umgang mit sensiblen Ersuchen. Sicherheitsüberprüfungen 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.

Vorsorgliche Sicherheitsüberprüfungen sollten auf einen klar begrenzten Kreis tatsächlich sicherheitskritisch eingesetzter Beschäftigter beschränkt bleiben. Pauschale, anlasslose oder unbegrenzte Sicherheitsüberprüfungen »auf Vorrat« sind abzulehnen.

Die in § 13 Abs. 7 Satz 4 BNDG-E vorgesehene Befugnis des Bundesnachrichtendienstes, Sicherheitsüberprüfungen bereits als organisatorische Vorkehrung für künftige Überwachungsmaßnahmen anzuordnen, sollte gestrichen werden. Für vergleichbare vorsorgliche Anordnungsbefugnisse im BVerfSchG-E sollte Entsprechendes gelten.

Davon zu unterscheiden ist die Möglichkeit eines Unternehmens, für einen klar begrenzten Kreis tatsächlich sicherheitskritisch eingesetzter Personen frühzeitig und freiwillig Sicherheitsüberprüfungen anzustoßen. Dies kann für Unternehmen sinnvoll sein, die kurzfristig auf konkrete Ersuchen reagieren oder regelmäßig sicherheitskritische Leistungen erbringen müssen. Sicherheitsüberprüfungen sollten mit Zustimmung der betroffenen Beschäftigten, unter klaren gesetzlichen Voraussetzungen, mit angemessenen Übergangsfristen und bei vollständiger Kostenerstattung erfolgen. Verfahrensdauer, Zuständigkeiten, die Übertragbarkeit bestehender Sicherheitsüberprüfungen sowie deren behördenübergreifende Anerkennung sollten verbindlich geregelt werden.

Dabei muss berücksichtigt werden, dass die tatsächliche Verfügbarkeit sicherheitsüberprüften Personals nur begrenzt im Einflussbereich des verpflichteten Unternehmens liegt. Ein Arbeitnehmer kann seine Bereitschaft zur Sicherheitsüberprüfung jederzeit widerrufen. Eine generische Vorprüfung der grundsätzlichen Bereitschaft ist zwar möglich, stellt jedoch keine Verfügbarkeit im Bedarfsfall sicher. Unternehmen können daher organisatorische Vorsorge treffen, die dauerhafte Verfügbarkeit sicherheitsüberprüften Personals aber weder organisatorisch noch vertraglich vollständig gewährleisten.

Zudem muss der persönliche und sachliche Anwendungsbereich der Verpflichtung gesetzlich klar definiert werden. Die Aufnahme eines Unternehmens in den Kreis der verpflichteten Stellen nach § 12 BNDG-E darf nicht dazu führen, dass umfangreiche Teile der Belegschaft vorsorglich einer Sicherheitsüberprüfung unterzogen werden können. Erfasst werden dürfen nur Beschäftigte, deren konkrete Tätigkeit einen unmittelbaren Bezug zur Durchführung der gesetzlich bestimmten Maßnahmen

aufweist. Da die Erfüllung der Verpflichtung damit teilweise außerhalb des Einflussbereichs des verpflichteten Unternehmens liegt, darf eine Nichterfüllung in diesen Fällen nicht zu einer Sanktionierung nach § 74 BVerfSchG-E führen. Entscheidend sollte vielmehr sein, ob das Unternehmen die ihm möglichen und zumutbaren organisatorischen Maßnahmen getroffen hat. Bitkom schlägt daher vor, § 13 Abs. 6 BVerfSchG-E um folgende Klarstellung zu ergänzen:

»Der Verpflichtung nach Satz 2 ist genügt, wenn der Verpflichtete nachweist, dass er die ihm möglichen organisatorischen Maßnahmen ergriffen hat, insbesondere Redundanzplanung und Verfügbarkeitsüberwachung für Beschäftigte mit abgeschlossener Sicherheitsüberprüfung. Ein Verstoß liegt nicht vor, wenn die Nichterfüllung auf dem Widerruf der Bereitschaft durch den Arbeitnehmer beruht und der Verpflichtete unverzüglich Ersatz bereitstellt.«

Ferner sollte eine maximale Verfahrensdauer gesetzlich festgelegt werden. Die tatsächlichen Bearbeitungszeiten betragen derzeit durchschnittlich drei Monate für die einfache Sicherheitsüberprüfung (SÜ1) und sechs bis neun Monate für die erweiterte Sicherheitsüberprüfung (SÜ2) nach der SÜG-Reform vom Januar 2026. Diese Zeiträume sind mit der in § 13 Abs. 6 BVerfSchG-E vorgesehenen »unverzüglichen« Benennung von sicherheitsüberprüftem Personal nicht vereinbar.

Weiterhin kritisch ist die in § 13 Abs. 6 BVerfSchG-E vorgesehene Verweisung auf die allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz für den Umgang mit VS-NfD. Die Verschlusssachenanweisung adressiert in erster Linie die Bundesverwaltung und ist auf die Abläufe privater Unternehmen nur eingeschränkt übertragbar. Bitkom hält es daher für sachgerechter, für Unternehmen auf die Vorgaben des Geheimschutzes in der Wirtschaft zurückzugreifen. Anstelle der VSA sollte auf Anlage 4 des Handbuchs für den Geheimschutz in der Wirtschaft (VS-NfD-Merkblatt des BMWi) verwiesen werden. Die speziell auf Unternehmen zugeschnittenen Regelungen schaffen Klarheit über die einzuhaltenden Anforderungen und reduzieren Umsetzungsunsicherheiten.

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

Die vorgesehenen technischen Mitwirkungspflichten für Anbieter von Telekommunikationsdiensten müssen eng begrenzt und eindeutig ausgestaltet werden. Dies gilt insbesondere für die Ausleitung von Kommunikationsinhalten, die Unterstützung bei Umleitungen, die Bereitstellung technischer Informationen sowie den Zugang zu Einrichtungen.

Bitkom begrüßt ausdrücklich, dass kein allgemeines Entschlüsselungs- oder Backdoor-Mandat vorgesehen ist. Dieser Schutz darf jedoch nicht allein der praktischen Auslegung der Mitwirkungspflichten überlassen bleiben. Im Gesetzestext sollte deklaratorisch klargestellt werden, dass die Auskunft-, Ausleitungs-, Umleitungs- und Unterstützungspflichten keine Verpflichtung begründen, Verschlüsselungsverfahren zu schwächen, zusätzliche Backdoors oder Klartextzugänge zu schaffen,

kryptografische Schlüssel außerhalb bestehender rechtlicher Zugriffsmöglichkeiten offenzulegen oder sichere Produkt- und Systemarchitekturen strukturell zu verändern. Dies muss auch für moderne Sicherheitsarchitekturen wie Zero-Trust-Modelle, Mutual TLS und vergleichbare Ende-zu-Ende abgesicherte Kommunikationsbeziehungen gelten.

Die gesetzlichen Anforderungen müssen zudem hinreichend bestimmen, welche technischen, organisatorischen und personellen Leistungen von den Unternehmen verlangt werden können. Insbesondere die in § 13 Abs. 5 BVerfSchG-E und § 13 Abs. 5 BNDG-E vorgesehenen Verpflichtungen zu sonstiger Unterstützung dürfen nicht zu unbegrenzten technischen Mitwirkungspflichten führen. Für die verpflichteten Unternehmen muss eindeutig erkennbar sein, welche technischen Informationen bereitzustellen sind, welche konkreten Unterstützungsleistungen verlangt werden können und wo die Grenzen der Mitwirkung liegen. Erforderlich sind klare Vorgaben zu Umfang und Grenzen der Mitwirkung, zu sicheren Verfahren sowie zur Verantwortungsverteilung zwischen der ersuchenden Behörde und dem verpflichteten Unternehmen.

Ausleitungs- und Mitwirkungspflichten sollten technikneutral, standardisiert und interoperabel umgesetzt werden. Soweit technische Schnittstellen oder Verfahren erforderlich sind, sollten anerkannte Standards, insbesondere etablierte ETSI-Verfahren, zugrunde gelegt werden. Proprietäre Einzellösungen und unterschiedliche technische Anforderungen verschiedener Behörden würden den Umsetzungsaufwand erhöhen und zusätzliche Sicherheitsrisiken schaffen. Die im Regierungsentwurf zusätzlich vorgesehenen Anpassungen des Telekommunikationsgesetzes und der Telekommunikations-Überwachungsverordnung unterstreichen die Notwendigkeit eines kohärenten und technisch einheitlichen Umsetzungsrahmens.

Cloud-Anbieter, die keine klassischen Telekommunikationsdienste wie Mobilfunk, Festnetz oder Internetzugang als eigenständiges Produkt erbringen, jedoch aufgrund eingebetteter Kommunikations-, Messaging- oder Connectivity-Funktionen bei der Bundesnetzagentur als Anbieter von Telekommunikationsdiensten gemeldet sind, befinden sich in einer Doppelregulierung durch TK-Recht und Cloud-Recht. Die erhöhte Schutzwelle des § 13 Abs. 6 BNDG-E darf nicht dadurch umgangen werden, dass Behörden denselben Anbieter über die TK-Route mit niedrigerer Schwelle in Anspruch nehmen.

Bitkom fordert daher gesetzliche Klarstellungen in drei Punkten: Für Cloud-Anbieter mit eingebetteten Kommunikationsfunktionen muss die speziellere Norm (§ 13 Abs. 6 BNDG-E) Vorrang haben, soweit es um den Zugriff auf vom Nutzer verarbeitete Applikationsdaten geht. Die Duldungspflicht nach § 170 TKG muss für mandantenfähige Cloud-Rechenzentren auf das verhältnismäßig erforderliche Maß beschränkt werden, um den Betrieb und die Integrität unbeteiligter Mandanten nicht zu gefährden. Die Einstufung als interpersoneller Telekommunikationsdienst (§ 3 Nr. 24 TKG) darf nicht allein aufgrund untergeordneter Nebenfunktionen erfolgen, die der Nutzerbenachrichtigung oder Systemkommunikation dienen.

Kritisch bewertet Bitkom darüber hinaus die Ausgestaltung des § 38 Abs. 2 Nr. 2 Buchst. a BNDG-E. Danach greift die höhere Eingriffsschwelle bei personenbezogenen Daten, die Inhalte interpersoneller Kommunikation darstellen, nur noch, wenn diese

»ohne Begrenzung auf einzelne nicht laufende Kommunikationsvorgänge« erhoben werden sollen. Damit gilt das erhöhte Schutzniveau nicht in gleicher Weise für gezielt erhobene gespeicherte Inhalte einzelner bereits abgeschlossener Kommunikationsvorgänge. Angesichts der regelmäßig hohen Sensibilität auch solcher Kommunikationsinhalte ist diese Differenzierung nicht überzeugend. Bitkom regt an, die höhere Eingriffsschwelle für gespeicherte Inhalte interpersoneller Kommunikation unabhängig davon vorzusehen, ob sich die Maßnahme auf einzelne nicht laufende Kommunikationsvorgänge beschränkt.

5.6 Zu § 71 Abs. 2 und 3 BVerfSchG-E sowie § 134 Abs. 2 und 3 BNDG-E: Betriebsuntersagung und Zwangsgeld

Bitkom begrüßt, dass der Regierungsentwurf die Anforderungen an Betriebsuntersagungen gegenüber dem Referentenentwurf verschärft und zusätzliche fachliche Beteiligung vorsieht.

Nach § 71 Abs. 2 BVerfSchG-E kann das Bundesministerium des Innern den Betrieb eines Unternehmens ganz oder teilweise untersagen, wenn mildere Eingriffe zur Durchsetzung rechtmäßigen Verhaltens nicht ausreichen. Dafür ist nun das Einvernehmen mit dem Bundesministerium für Digitales und Staatsmodernisierung erforderlich. Für den BND sieht § 134 Abs. 2 BNDG-E eine entsprechende Befugnis des Bundesverwaltungsamts im Einvernehmen mit der Bundesnetzagentur vor.

Die Betriebsuntersagung bleibt dennoch ein außerordentlich weitreichendes Instrument. Bei Betreibern digitaler Infrastruktur können entsprechende Maßnahmen erhebliche Auswirkungen auf unbeteiligte Kunden, kritische Geschäftsprozesse und die Verfügbarkeit digitaler Dienste haben. Dies gilt insbesondere für Cloud-, Hosting- und Telekommunikationsanbieter sowie Anbieter, deren Dienste von kritischen Infrastrukturen genutzt werden.

Auch die nach § 71 Abs. 3 BVerfSchG-E und § 134 Abs. 3 BNDG-E möglichen Zwangsgelder bis zu einer Million Euro stellen einen erheblichen Eingriff dar.

Eine Betriebsuntersagung darf jedoch ausschließlich als ultima ratio eingesetzt werden. Für § 134 BNDG-E wird dieser Grundsatz bereits in der Gesetzesbegründung ausdrücklich hervorgehoben. Er sollte sowohl dort als auch für die entsprechende Befugnis im BVerfSchG-E unmittelbar im Normtext verankert werden.

Eine Betriebsuntersagung sollte auf wiederholte, vorsätzliche und schwerwiegende Verstöße beschränkt werden. Erforderlich sind eine vorherige Anhörung, eine abgestufte Eskalation der Durchsetzungsmaßnahmen und angemessene Fristen zur Abhilfe. Für die Verhängung eines Zwangsgelds sollte ein Verschuldenserfordernis vorgesehen werden. Zudem sollte die Höhe verhältnismäßig abgestuft und gesetzlich wirksam begrenzt werden, damit die Obergrenze von einer Million Euro nicht unabhängig von Art, Umfang und Verschulden des jeweiligen Verstoßes zur Anwendung kommen kann. Rechtsbehelfe gegen eine Betriebsuntersagung oder ein Zwangsgeld sollten grundsätzlich aufschiebende Wirkung entfalten. Ausnahmen hiervon sollten nur für eng definierte besondere Eilfälle zulässig sein und einer gesonderten Begründung bedürfen. Vor jeder Betriebsuntersagung müssen zudem die

möglichen Folgen für Kunden, kritische Infrastrukturen und die Funktionsfähigkeit digitaler Dienste berücksichtigt werden.

5.7 Zu § 72 BVerfSchG-E und § 135 BNDG-E: Anzeige- und Genehmigungspflichten ausgeschiedener Bediensteter

Die in § 72 BVerfSchG-E und § 135 BNDG-E vorgesehenen Anzeige- und Genehmigungspflichten für ausgeschiedene Bedienstete können weiterhin Auswirkungen auf Unternehmen haben, 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 relevanten dienstlichen Belange klar zu definieren und ein praktikables, zügiges Verfahren sicherzustellen. Für Unternehmen und betroffene Personen muss vorhersehbar sein, welche Tätigkeiten anzeige- oder genehmigungspflichtig sind, unter welchen Voraussetzungen eine Tätigkeit untersagt werden kann und innerhalb welcher Frist eine Entscheidung erfolgt.

6. Spezifische Anmerkungen zum BVerfSchG-E

6.1 Zu § 11 Abs. 3 Satz 2 und Abs. 6 BVerfSchG-E: Ersuchen zu künftig anfallenden Daten

§ 11 Abs. 3 Satz 2 BVerfSchG-E stellt klar, dass eine Verpflichtung zur Speicherung von Daten nur besteht, soweit dies im Einzelfall zur Erfüllung eines konkreten Ersuchens erforderlich ist. § 11 Abs. 6 BVerfSchG-E begrenzt Ersuchen zu künftig anfallenden Daten zudem auf höchstens ein Jahr. Diese Begrenzungen sind grundsätzlich sachgerecht. Gleichwohl können entsprechende Ersuchen erheblichen technischen und organisatorischen Aufwand verursachen und bestehende Löscho- und Data-Retention-Konzepte von Unternehmen berühren.

Bitkom regt daher weitere Präzisierungen dazu an, welche Datenkategorien von zukunftsgerichteten Ersuchen erfasst werden können und nach welchen Kriterien die Dauer einer solchen Verpflichtung im Einzelfall festzulegen ist. Die in § 11 Abs. 6 BVerfSchG-E vorgesehene Höchstdauer von einem Jahr darf dabei nicht zum Regelzeitraum werden. Speicherpflichten müssen strikt auf den konkreten Anlass, die erforderlichen Daten und den unbedingt notwendigen Zeitraum begrenzt bleiben. Zudem muss für Unternehmen eindeutig erkennbar sein, wie sich entsprechende Anordnungen zu bestehenden gesetzlichen Löschpflichten und unternehmensinternen Löschkonzepten verhalten.

Entsprechende Anforderungen müssen ausdrücklich auch für Ersuchen des Bundesnachrichtendienstes gelten. § 17 BNDG-E enthält für Anordnungen, die auch

künftig anfallende Daten erfassen, ebenfalls eine zeitliche Begrenzung auf zwölf Monate. Die Höchstdauer darf auch hier nicht zum Regelfall werden. Jede Anordnung und jede Verlängerung muss sich an der konkreten Erforderlichkeit orientieren und beendet werden, sobald die Voraussetzungen nicht mehr vorliegen. Damit sollte auch für den BND ausdrücklich klargestellt werden, dass aus zukunftsgerichteten Ersuchen keine allgemeine oder anlasslose Vorratsspeicherung entstehen darf.

6.2 Zu § 13 Abs. 7 BVerfSchG-E und § 103 BNDG-E: Eigenständiger Rechtsschutz verpflichteter Anbieter

§ 13 Abs. 7 BVerfSchG-E schließt für bestimmte Ersuchen und deren Vollzug vor der Mitteilung an die betroffene Person den Rechtsweg für diese aus. § 103 BNDG-E enthält eine entsprechende Regelung für bestimmte Auskunftersuchen, strategische Aufklärungsmaßnahmen und Maßnahmen der Telekommunikationsüberwachung.

Die Geheimhaltung laufender Maßnahmen kann erforderlich sein, um deren Zweck, eingesetzte Personen und operative Vorgehensweisen zu schützen. Sie darf jedoch nicht dazu führen, dass ein unmittelbar verpflichtetes Unternehmen keine Möglichkeit besitzt, ein an dieses Unternehmen gerichtetes Ersuchen überprüfen zu lassen. Die Rechtsposition des verpflichteten Anbieters ist von derjenigen der betroffenen Person zu unterscheiden. Unternehmen können durch Ersuchen selbst unmittelbar in eigenen Rechten betroffen sein und erhebliche technische, wirtschaftliche sowie rechtliche Risiken tragen.

Damit neue Mitwirkungspflichten in der Praxis rechtssicher umgesetzt werden können, braucht es zugleich eine eindeutige Verantwortungsverteilung zwischen Behörden und verpflichteten Unternehmen. Die Prüfung der materiellen Voraussetzungen und der Rechtmäßigkeit des Ersuchens muss bei der ersuchenden Behörde liegen. Unternehmen dürfen nicht gezwungen sein, die nachrichtendienstliche Bewertung selbst nachzuvollziehen oder zu ersetzen. Befolgt ein Anbieter ein rechtmäßiges und vollziehbares Ersuchen ordnungsgemäß, muss klargestellt sein, dass ihm aus der behördlichen Rechtmäßigkeitsprüfung keine eigene Haftung entsteht. Dies ist angesichts der gleichzeitig bestehenden Mitteilungsverbote besonders wichtig. Davon unberührt bleiben muss das Recht des Anbieters, offensichtlich rechtswidrige, unverhältnismäßige oder technisch nicht umsetzbare Ersuchen einer unabhängigen Prüfung zuzuführen.

Bitkom fordert deshalb ein eigenständiges und sofort ausübbares Beanstandungs- und Rechtsschutzrecht der Anbieter gegen an sie gerichtete Ersuchen, unabhängig davon, ob und wann die betroffene Person über die zugrunde liegende Maßnahme informiert wird. Der Rechtsschutz muss insbesondere die Rechtmäßigkeit, Verhältnismäßigkeit, Reichweite und technische Umsetzbarkeit des Ersuchens sowie mögliche Normkonflikte erfassen.

Hilfsweise sollte ein gesetzliches Vorlage- und Prüfungsrecht gegenüber dem Unabhängigen Kontrollrat geschaffen werden. Bei ernsthaften Zweifeln an der Rechtmäßigkeit, Verhältnismäßigkeit oder technischen Umsetzbarkeit sollte die Vorlage grundsätzlich aufschiebende Wirkung entfalten. Dies fügt sich in die gestärkte

Kontrollarchitektur des Regierungsentwurfs ein, insbesondere in die anlassunabhängige administrative Kontrolle nach § 32 UKRatG-E und die Kontrollmöglichkeiten nach § 26 UKRatG-E.

7. BSI-Übermittlungspflichten im BVerfSchG-E und BNDG-E

7.1 Zu § 10 Abs. 4 Satz 2 Nr. 2 und Abs. 7 Nr. 2 BVerfSchG-E sowie § 10 Abs. 2 Nr. 2 und Abs. 4 Nr. 2 BNDG-E: BSI-Erkenntnisse zu Schwachstellen und Schutz der Meldestellenfunktion

Der Regierungsentwurf sieht entsprechende Übermittlungspflichten des BSI in beiden Fachgesetzen vor. Nach § 10 Abs. 4 Satz 2 Nr. 2 BVerfSchG-E gehört das BSI unter den dort genannten Voraussetzungen zu den zur Übermittlung an das Bundesamt für Verfassungsschutz verpflichteten öffentlichen Stellen. § 10 Abs. 7 Nr. 2 BVerfSchG-E nimmt hiervon jedoch Fälle aus, in denen die Übermittlung im Widerspruch zu den Aufgaben des BSI als Meldestelle nach den §§ 4 und 5 des BSI-Gesetzes stünde. Parallel verpflichtet § 10 Abs. 2 Nr. 2 BNDG-E das BSI unter den dort genannten Voraussetzungen zur Übermittlung von Informationen an den Bundesnachrichtendienst. Auch hier sieht § 10 Abs. 4 Nr. 2 BNDG-E nun eine Ausnahme vor, wenn die Übermittlung im Widerspruch zu den Aufgaben des BSI als Meldestelle nach den §§ 4 und 5 des BSI-Gesetzes stünde.

Bitkom begrüßt ausdrücklich, dass der Regierungsentwurf die Übermittlungspflichten des BSI gegenüber dem Referentenentwurf auf diese Weise begrenzt. Die neue Schutzklausel ist eine wichtige Verbesserung und trägt der besonderen Rolle des BSI als zentrale Vertrauensstelle für Cybersicherheit Rechnung. Ein wirksamer Informationsaustausch zwischen Sicherheitsbehörden kann für die Lagebewertung bei Cyberangriffen erforderlich sein. Insbesondere koordinierte und internationale Angriffskampagnen können eine behördenübergreifende Einordnung notwendig machen. Gleichzeitig lebt die Zusammenarbeit zwischen Wirtschaft und BSI davon, dass Unternehmen Schwachstellen, Sicherheitsvorfälle und technische Risiken frühzeitig melden können. Dieses Vertrauen darf durch nachrichtendienstliche Übermittlungspflichten nicht beeinträchtigt werden.

Die im Regierungsentwurf geschaffenen Ausnahmen sind ein wichtiger Schritt, reichen aus Sicht von Bitkom jedoch noch nicht aus. Die Schutzregelung sollte nicht lediglich vorsehen, dass eine gesetzliche Übermittlungspflicht in bestimmten Fällen entfällt. Für Informationen, deren Weitergabe die Meldestellen- und Vertrauensfunktion des BSI beeinträchtigen würde, sollte vielmehr ein ausdrückliches gesetzliches Übermittlungsverbot gelten. Nur so ist ausgeschlossen, dass Informationen, deren verpflichtende Weitergabe untersagt ist, auf Grundlage anderer Ermessens- oder Übermittlungsbefugnisse dennoch an Nachrichtendienste gelangen.

Dieses Übermittlungsverbot sollte ausdrücklich sämtliche Schwachstellen- und Vorfallsinformationen erfassen, die das BSI aufgrund seiner vertrauensbasierten Melde- und Koordinierungsfunktionen erhält. Dazu sollten insbesondere Informationen zählen, die über CERT-Bund oder über die Single Reporting Platform an das BSI übermittelt werden. Für Unternehmen muss vor einer Meldung eindeutig erkennbar sein, welchem Verwendungsregime die übermittelten Informationen unterliegen.

Darüber hinaus sollte für den staatlichen Umgang mit Schwachstelleninformationen ein gesetzlich geregelter Vulnerabilities-Equities-Prozess geschaffen werden. Dieser muss transparent festlegen, unter welchen eng begrenzten Voraussetzungen ausnahmsweise andere Sicherheitsinteressen gegenüber einer unverzüglichen Schwachstellenbehebung berücksichtigt werden dürfen. Erforderlich sind klare Entscheidungskriterien, Dokumentations- und Begründungspflichten, zeitliche Befristungen, regelmäßige Neubewertungen sowie eine unabhängige Kontrolle. Grundsätzlich müssen Schwachstellenbehebung, Responsible Disclosure und der Schutz betroffener Systeme Vorrang haben.

Die Unabhängigkeit des BSI in seinen gesetzlichen Aufgaben muss dabei gewahrt bleiben. Dies gilt auch für seine Funktion als Marktüberwachungsbehörde. Artikel 11 Abs. 2 der Verordnung (EU) 2019/1020 verlangt, dass Marktüberwachungsbehörden ihre Befugnisse unabhängig, unparteiisch und unvoreingenommen ausüben. Eine nachrichtendienstliche Nutzung von Informationen, die dem BSI gerade aufgrund seiner Marktüberwachungs-, Melde- oder Vertrauensfunktion bekannt werden, darf diese institutionelle Unabhängigkeit nicht beeinträchtigen.

Schwachstelleninformationen dürfen nicht dazu führen, dass bekannte Sicherheitslücken länger offengehalten, ihre Behebung verzögert oder privatwirtschaftliche IT-Produkte und Infrastrukturen zusätzlichen Risiken ausgesetzt werden. Die § 10 BVerfSchG-E und § 10 BNDG-E dürfen keine Grundlage für die operative Ausnutzung von Schwachstellen schaffen. Die jetzt eingeführten Schutzklauseln sollten deshalb im weiteren Gesetzgebungsverfahren zu einem klaren und belastbaren gesetzlichen Schutzregime weiterentwickelt werden.

8. Schutzmaßnahmen/Erweiterte nachrichtendienstliche Maßnahmen/Aktive Cyberabwehr

8.1 Zu §§ 59 bis 61 BVerfSchG-E sowie §§ 31 Abs. 6, 36 Abs. 2, 39 Abs. 4 und 49 bis 51 BNDG-E

Hinsichtlich der neu geschaffenen Befugnisse zur aktiven Cyberabwehr (§§ 59–61 BVerfSchG-E, §§ 31 Abs. 6, 36 Abs. 2, 39 Abs. 4, 49–51 BNDG-E) möchten wir klarstellend darauf hinweisen, dass die Durchführung aktiver Cyberabwehrmaßnahmen ausschließlich Aufgabe der zuständigen Behörden ist. Eine unmittelbare operative Beteiligung von Telekommunikations- und IT-Unternehmen an

solchen Maßnahmen ist gesetzlich nicht vorgesehen und wird von uns auch nicht so verstanden. Die unterstützende Rolle der Telekommunikationsunternehmen beschränkt sich allenfalls auf eine mittelbare Beteiligung, etwa durch Auskunftserteilung zur Vorbereitung behördlicher Maßnahmen. Die Mitwirkungspflichten sollten im Gesetzestext deutlich begrenzt werden.

9. Fazit

Der Regierungsentwurf enthält gegenüber dem Referentenentwurf wichtige Verbesserungen, lässt aus Sicht der Digitalwirtschaft aber weiterhin zentrale Fragen offen. Entscheidend ist, dass neue Befugnisse mit klaren rechtlichen Grenzen, wirksamer Kontrolle und einer technisch tragfähigen Umsetzung verbunden werden. Dabei müssen insbesondere die Integrität digitaler Infrastrukturen, die Vertrauensfunktion des BSI sowie Rechtssicherheit und Verhältnismäßigkeit für die betroffenen Unternehmen gewahrt bleiben. Bitkom wird das weitere parlamentarische Verfahren konstruktiv begleiten und steht für die weitere Ausgestaltung der Reform im Dialog mit Politik und Verwaltung 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

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.