Stellungnahme

Zum Referentenentwurf eines Gesetzes zur Reform des Nachrichtendienst-rechts

Bundesverband der Deutschen Industrie e.V.

Stand: 14.07.2026

Inhaltsverzeichnis

Zusammenfassung

Der Referentenentwurf eines Gesetzes zur Reform des Nachrichtendienstrechts umfasst eine Neufassung des Bundesverfassungsschutzgesetzes (BVerfSchG-E) und des BND-Gesetzes (BNDG-E). Ziel des Entwurfs ist es, Vorgaben der verfassungsgerichtlichen Rechtsprechung umzusetzen, die Aufklärungs- und Weiterverarbeitungsfähigkeiten der Nachrichtendienste an die veränderte Bedrohungslage anzupassen und die Kontrolle der Nachrichtendienste neu zu ordnen. Für den BDI ist der Entwurf von besonderer Bedeutung, weil wirtschaftliche Sicherheit heute untrennbar mit der nationalen Sicherheitsarchitektur verbunden ist. Vor dem Hintergrund hybrider Bedrohungen stehen Unternehmen, Forschungseinrichtungen, Kritische Infrastrukturen, Lieferketten und technologische Schlüsselbereiche zunehmend im Fokus von Spionage, Sabotage und Cyberangriffen. Die Fähigkeit von Wirtschaft und Industrie, auch unter Krisen- und Bedrohungsbedingungen leistungs- und funktionsfähig zu bleiben, ist daher ein zentraler Baustein für die Sicherheits- und Verteidigungsfähigkeit Deutschlands.

Ein wirksamer Informationsaustausch zwischen Sicherheitsbehörden und Wirtschaft kann hierzu einen wichtigen Beitrag leisten. Bereits in seiner Stellungnahme vom 03.12.2020 zum damaligen Entwurf zur Änderung des BND-Gesetzes hat der BDI hervorgehoben, dass die Nachrichtendienste einen wichtigen Beitrag zum Schutz von Unternehmen, Beschäftigten und wirtschaftlichen Interessen Deutschlands vor Spionage, Sabotage und anderen sicherheitsrelevanten Bedrohungen leisten können. Der nun vorliegende Entwurf trägt der veränderten Bedrohungslage Rechnung und berücksichtigt wirtschaftliche Sicherheit, technologische Souveränität, Versorgungssicherheit und den Schutz Kritischer Infrastrukturen stärker als bisher.

Gleichzeitig bedürfen die im Entwurf vorgesehenen Auskunfts- und Mitwirkungspflichten in mehreren Bereichen einer Nachschärfung. Dies betrifft insbesondere die fehlende Abgrenzung zwischen eigener Verfügungsbefugnis und Auftragsverarbeitung, ungelöste Normkonflikte mit europäischem Recht, die notwendige Konkretisierung der Subsidiaritätsvorgaben bei Eingriffen in laufende Infrastruktur, unzureichende Regelungen zum Beschäftigtendatenschutz bei Sicherheitsüberprüfungen, die ungeklärte Reichweite von Auskunftspflichten innerhalb internationaler Unternehmensgruppen sowie fehlende Zweckbindungs- und Löschungsregelungen für übermittelte Daten. Der BDI verbindet seine grundsätzliche Unterstützung des Reformvorhabens mit der Erwartung, dass diese Punkte im weiteren Gesetzgebungsverfahren aufgegriffen und präzisiert werden.

Bundesverband der Deutschen Industrie e.V.

Lobbyregisternummer
R000534

Hausanschrift
Breite Straße 29
10178 Berlin
Postanschrift
11053 Berlin

Ansprechpartner
Kerstin Petretto
T:49 3020281710
E-Mail:
k.petretto@bdi.eu

Internet
www.bdi.eu

1. Einleitung

Der BDI begrüßt insbesondere, dass wirtschaftliche Sicherheit, technologische Souveränität, Versorgungssicherheit, Kritische Infrastrukturen und kritische Technologien im Entwurf als relevante Bezugsgrößen der nachrichtendienstlichen Aufklärung berücksichtigt werden.

So nennt § 3 Abs. 3 BNDG-E die inländische und europäische Wirtschaft und Wissenschaft, die Versorgung mit wesentlichen Rohstoffen, Energien und kritischen Technologien sowie die Sicherheit von Weltrauminfrastruktur als relevante Bezugsgrößen der Auslandsaufklärung (vgl. § 3 Abs. 3 BNDG-E, S. 81 f.). Darüber hinaus erfasst § 3 Abs. 4 BNDG-E hybride Einflussnahmen, unerlaubten Außenwirtschaftsverkehr, disruptive Technologien, wehrtechnische Technologien, Technologien der künstlichen Intelligenz sowie krisenhafte Entwicklungen im Ausland als erhebliche Bedrohungsfelder (vgl. § 3 Abs. 4 Nr. 2, 3, 5 und 6 BNDG-E, S. 81 f.). Positiv hervorzuheben ist zudem, dass der Entwurf sowohl den Schutz Kritischer Infrastrukturen als auch die Stabilität wirtschaftlicher Strukturen berücksichtigt. Während § 4 Abs. 3 Nr. 2 Buchst. c BNDG-E die Funktionsfähigkeit Kritischer Infrastrukturen als herausgehobenes Bedrohungsziel nennt, erfasst § 4 Abs. 5 Nr. 2 BNDG-E Bedrohungslagen mit möglichen erheblichen Auswirkungen auf die wirtschaftliche Struktur Deutschlands (vgl. § 4 Abs. 3 Nr. 2 Buchst. c und § 4 Abs. 5 Nr. 2 BNDG-E, S. 82 f.).

Besonders hervorzuheben sind die Regelungen zum Informationsaustausch mit der Wirtschaft. Mit § 85 BNDG-E verankert der Entwurf den Informationsaustausch mit nichtöffentlichen Stellen im BND-Gesetz. Aus Sicht des BDI trägt dies der wachsenden Bedeutung des präventiven Wirtschaftsschutzes Rechnung und stärkt die Voraussetzungen für einen strukturierten Informationsaustausch zwischen Sicherheitsbehörden und Wirtschaft. Als zulässige Übermittlungszwecke nennt die Vorschrift unter anderem die Sicherstellung der Funktionsfähigkeit Kritischer Infrastrukturen, den Schutz der Sicherheit in der Informationstechnik sowie den Schutz der Wirtschaft gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten (vgl. § 85 Abs. 1 Nr. 2 Buchst. c, e und f BNDG-E). Damit wird der Informationsaustausch mit nichtöffentlichen Stellen im BND-Gesetz konkreter verankert als bisher.

Auch die Vorschriften des BVerfSchG-E stärken den präventiven Wirtschafts- und Wissenschaftsschutz. § 45 Abs. 1 BVerfSchG-E sieht vor, dass das Bundesamt für Verfassungsschutz Öffentlichkeit und Fachkreise über präventiven Wirtschafts- und Wissenschaftsschutz informieren kann (vgl. §

45 Abs. 1 BVerfSchG-E, S. 51). Zudem ermöglicht § 51 Abs. 1 Nr. 3 BVerfSchG-E Übermittlungen an inländische nichtöffentliche Stellen unter anderem zum Schutz Kritischer Infrastrukturen, der Sicherheit in der Informationstechnik sowie von Wirtschaftsunternehmen und Wissenschaftseinrichtungen vor sicherheitsgefährdenden und geheimdienstlichen Tätigkeiten (vgl. § 51 Abs. 1 Nr. 3 Buchst. a bis d BVerf-SchG-E, S. 54 f.).

Dies stärkt die Voraussetzungen für einen präventiven Wirtschaftsschutz und den Austausch sicherheitsrelevanter Erkenntnisse zwischen Sicherheitsbehörden und Wirtschaft.

2. Auftrag und Befugnisse der Nachrichtendienste mit Blick auf Wirtschaftsschutz

BND: Konkretisierung wirtschaftlicher Bedrohungsziele im Auslandsaufklärungsauftrag

Nach § 2 Abs. 1 BNDG-E ist Aufgabe des BND die nachrichtendienstliche Auslandsaufklärung. Er sammelt und bewertet danach erforderliche Informationen über das Ausland, die von außen- oder sicherheitspolitischer Bedeutung für Deutschland sind, mit dem Ziel der Früherkennung von Bedrohungen für besonders gewichtige Rechtsgüter. Der Entwurf ordnet den BND damit weiterhin als Auslandsnachrichtendienst ein.

Die für die Wirtschaft relevante Präzisierung folgt aus §§ 3 und 4 BNDG-E. § 3 Abs. 3 BNDG-E nennt als erhebliche Bedrohungsziele die inländische und europäische Wirtschaft und Wissenschaft, die Versorgung mit wesentlichen Rohstoffen und Gütern, Energien sowie kritischen Technologien und die Sicherheit von Weltrauminfrastruktur. § 3 Abs. 4 BNDG-E benennt als erhebliche Bedrohungsfelder unter anderem hybride Einflussnahmen, unerlaubten Außenwirtschaftsverkehr, aufkommende disruptive Technologien, wehrtechnische Technologien, Technologien der künstlichen Intelligenz und krisenhafte Entwicklungen im Ausland.

Aus Sicht des BDI trägt diese Konkretisierung der veränderten Bedrohungslage Rechnung. Ausländische Spionage, Sabotage, hybride Einflussnahmen, Cyberangriffe und geostrategische Abhängigkeiten betreffen zunehmend auch Unternehmen, Forschungseinrichtungen, Lieferketten, kritische Technologien und Kritische Infrastrukturen. Wirtschaftliche Sicherheit wird damit als Bestandteil der nationalen Sicherheitsarchitektur adressiert.

Kritische Infrastrukturen und wirtschaftliche Funktionsfähigkeit als Teil nationaler Resilienz

§ 4 BNDG-E hebt bestimmte Bedrohungen von erheblicher Bedeutung weiter hervor. Für den BDI sind insbesondere drei Regelungen relevant. § 4 Abs. 3 Nr. 1 BNDG-E nennt die Gesamtverteidigung der Bundesrepublik Deutschland und verbündeter Staaten. § 4 Abs. 3 Nr. 2 Buchst. c BNDG-E nennt die Funktionsfähigkeit Kritischer Infrastrukturen. § 4 Abs. 5 Nr. 2 BNDG-E erfasst Bedrohungslagen, die zu einer wesentlichen Beeinträchtigung der allgemeinen Sicherheitslage, der wirtschaftlichen Struktur oder der grundlegenden gesellschaftlichen Strukturen Deutschlands führen können.

Diese Normen verbinden den Schutz staatlicher Handlungsfähigkeit mit dem Schutz wirtschaftlicher und infrastruktureller Funktionsfähigkeit. Der Entwurf bildet damit eine Entwicklung ab, die der BDI in seinen bisherigen Positionen hervorgehoben hat: Kritische Infrastrukturen, industrielle Kapazitäten, Wertschöpfungs- und Lieferketten sind Teil nationaler Resilienz und Gesamtverteidigung. Die Einbeziehung Kritischer Infrastrukturen, Lieferketten und wirtschaftlicher Strukturen trägt zugleich der Erkenntnis Rechnung, dass Wirtschaft und Industrie wesentliche Voraussetzungen für die Sicherheits- und Verteidigungsfähigkeit Deutschlands darstellen.

BND: Übermittlung an Unternehmen nach § 85 BNDG-E

Insbesondere § 85 BNDG-E kommt dabei besondere Bedeutung zu. Die Vorschrift stärkt die Voraussetzungen für einen strukturierten Informationsaustausch zwischen Sicherheitsbehörden und Wirtschaft. Sie ermöglicht unter den gesetzlichen Voraussetzungen die Übermittlung von Erkenntnissen an inländische nichtöffentliche Stellen insbesondere zum Schutz Kritischer Infrastrukturen, der Sicherheit in der Informationstechnik sowie der Wirtschaft.

§ 85 Abs. 1 Nr. 2 BNDG-E nennt als zulässige Übermittlungszwecke unter anderem die Gewährleistung der Sicherheit lebenswichtiger Güter der Allgemeinheit, die Sicherstellung der Funktionsfähigkeit Kritischer Infrastrukturen, den Schutz der Sicherheit in der Informationstechnik sowie den Schutz der Wirtschaft gegen sicherheitsgefährdende oder geheimdienstliche Tätigkeiten (vgl. § 85 Abs. 1 Nr. 2 Buchst. a, c, e und f BNDG-E). Besonders hervorzuheben ist dabei, dass der Schutz der Wirtschaft als eigenständiger Übermittlungszweck genannt wird.

Dies spiegelt die wachsende Bedeutung des präventiven Wirtschaftsschutzes wider. Unternehmen können Bedrohungen durch Spionage, Sabotage, Cy-

berangriffe oder andere Formen sicherheitsgefährdender Einflussnahme nur wirksam begegnen, wenn sicherheitsrelevante Erkenntnisse rechtzeitig und adressatengerecht verfügbar sind. § 85 BNDG-E schafft hierfür eine wichtige Grundlage.

Wirtschaftsschutz ist nicht nur reaktiv zu verstehen. Sicherheitsrelevante Informationen, Indikatoren und Lagebilder entfalten ihren Schutzwert vor allem dann, wenn sie Unternehmen frühzeitig erreichen, eine Bewertung von Risiken für Standorte, Lieferketten, Technologien und Geschäftsprozesse ermöglichen und in konkrete Schutzmaßnahmen übersetzt werden können.

Gleichzeitig ist diese Befugnis nicht nur als punktuelle Informationsweitergabe zu verstehen. Ihr praktischer Mehrwert entsteht erst, wenn Unternehmen Informationen rechtzeitig, verständlich und mit konkretem Handlungsbezug erhalten. Dazu müssen im BND klare Zuständigkeiten definiert, sichere Kommunikationswege etabliert und abgestimmte Geheimschutzverfahren aufgesetzt werden.

BfV: Präventiver Wirtschafts- und Wissenschaftsschutz sowie Übermittlung an Unternehmen

Für das Bundesamt für Verfassungsschutz (BfV) konkretisiert der Entwurf Informations- und Übermittlungsbefugnisse gegenüber Wirtschaft und Wissenschaft. § 45 Abs. 1 BVerfSchG-E sieht vor, dass das BfV Öffentlichkeit und Fachkreise über Bedrohungen und ihre Einstufung sowie über präventiven Wirtschafts- und Wissenschaftsschutz informieren kann. Damit wird präventiver Wirtschafts- und Wissenschaftsschutz als Gegenstand behördlicher Information genannt.

Die Vorschriften des BVerfSchG-E ergänzen damit die im BND-Gesetz vorgesehenen Regelungen zum Informationsaustausch mit der Wirtschaft um eine verfassungsschutzrechtliche Komponente.

§ 51 Abs. 1 Nr. 3 BVerfSchG-E regelt die Übermittlung personenbezogener Daten an inländische nichtöffentliche Stellen. Erfasst sind der Schutz lebenswichtiger und verteidigungsrelevanter Einrichtungen und Kritischer Infrastrukturen (vgl. § 51 Abs. 1 Nr. 3 Buchst. a BVerfSchG-E), der Schutz der Sicherheit in der Informationstechnik (vgl. § 51 Abs. 1 Nr. 3 Buchst. b BVerfSchG-E), der Schutz von Wirtschaftsunternehmen und Wissenschaftseinrichtungen vor sicherheitsgefährdenden und geheimdienstlichen Tätigkeiten (vgl. § 51 Abs. 1 Nr. 3 Buchst. c BVerfSchG-E) sowie der Schutz rechtlich

gewährleisteter Geheimnisse (vgl. § 51 Abs. 1 Nr. 3 Buchst. d BVerfSchG-E).

Der BDI begrüßt die Einbeziehung dieser Schutzbereiche ausdrücklich. Mit § 51 Abs. 1 Nr. 3 BVerfSchG-E wird die Übermittlung personenbezogener Daten an inländische nichtöffentliche Stellen für zentrale Bereiche des präventiven Wirtschafts- und Wissenschaftsschutzes gesetzlich verankert. Die Vorschrift schafft damit eine wichtige Grundlage, um sicherheitsrelevante Erkenntnisse zum Schutz von Unternehmen, Wissenschaftseinrichtungen, Kritischen Infrastrukturen und der Sicherheit in der Informationstechnik frühzeitig und handlungsorientiert weiterzugeben.

Bereits nach geltendem Recht bestehen mit § 22a BVerfSchG Übermittlungsbefugnisse an nichtöffentliche Stellen, unter anderem zum Schutz Kritischer Infrastrukturen und der IT-Sicherheit. Mit § 51 Abs. 1 Nr. 3 BVerfSchG-E wird diese Systematik fortgeführt und um den Schutz von Wirtschaftsunternehmen und Wissenschaftseinrichtungen vor sicherheitsgefährdenden und geheimdienstlichen Tätigkeiten ergänzt.

Dies stärkt die Voraussetzungen für einen frühzeitigen und handlungsorientierten Informationsaustausch zwischen Sicherheitsbehörden und Wirtschaft. Gerade bei Spionage, Sabotage, hybriden Bedrohungen und Cyberangriffen ist es entscheidend, dass sicherheitsrelevante Erkenntnisse zeitnah an betroffene Unternehmen und Einrichtungen weitergegeben werden können.

Ergänzend ist eine Stärkung gemeinsamer Austauschs-, Trainings- und Übungsformate zwischen Sicherheitsbehörden und Wirtschaft sinnvoll. Sie können dazu beitragen, gegenseitiges Verständnis, belastbare Kommunikationswege und praxistaugliche Verfahren im Wirtschaftsschutz weiterzuentwickeln.

3. Behördenzusammenarbeit und Einbindung der Wirtschaft

Der Entwurf stärkt an mehreren Stellen die Zusammenarbeit der Behörden untereinander. § 1 BVerfSchG-E enthält eine Zusammenarbeitspflicht von Bund und Ländern im Verfassungsschutz. § 5 BVerfSchG-E regelt Zentralstellenaufgaben des BfV, einschließlich zentraler Auswertung, Koordinierung und Unterstützung der Landesbehörden. § 6 BVerfSchG-E regelt die gegenseitige Unterrichtung der Verfassungsschutzbehörden und das nachrichtendienstliche Informationssystem.

Für den BND sieht § 10 Abs. 2 BNDG-E Übermittlungspflichten bestimmter öffentlicher Stellen vor. Genannt werden unter anderem BfV und Landesverfassungsschutzbehörden, der Militärische Abschirmdienst, das BSI, die Zentralstelle für Finanztransaktionsuntersuchungen, Polizeien, Zollbehörden, BAMF und Finanzbehörden. §§ 89 bis 94 BNDG-E regeln gemeinsame Dateien mit inländischen öffentlichen Stellen, der Bundeswehr und ausländischen öffentlichen Stellen.

Hybride Bedrohungen, Spionage, Sabotage und Cyberangriffe lassen sich wirksamer bearbeiten, wenn Erkenntnisse nicht in getrennten Zuständigkeitslogiken verbleiben. Für die Wirtschaft ist entscheidend, dass behördliche Kooperation auch zu besseren, verwertbaren Informationen für Unternehmen führt. Die im Entwurf angelegte Behördenzusammenarbeit gilt es daher mit der Einbindung der Wirtschaft zu verknüpfen. Unternehmen verfügen über sicherheitsrelevante Erkenntnisse aus eigenen Netzen, Standorten, Angriffserfahrungen, Lieferketten und Schutzstrukturen. Zugleich sind sie auf aktuelle Lageinformationen der Sicherheitsbehörden angewiesen. Erforderlich ist ein gemeinsames Lageverständnis, das sowohl die staatliche Lagebewertung als auch die Schutz- und Reaktionsfähigkeit der Unternehmen verbessert.

Dafür bietet sich die Prüfung dauerhafter Formate für einen vertraulichen Austausch zwischen Sicherheitsbehörden und Wirtschaft an. Solche Formate könnten Lagebewertungen schneller mit praktischen Erkenntnissen aus Unternehmen, Kritischen Infrastrukturen und Lieferketten abgleichen und Rückmeldungen aus der Wirtschaft strukturiert in die behördliche Lagebewertung einbeziehen. Dies könnte, soweit institutionell geeignet, auch eine strukturierte Einbindung wirtschaftlicher Expertise in bestehende Lage- und Austauschformate (z. B. das GAZ Hybrid) umfassen.

4. Hinweise zur weiteren Ausgestaltung

Aus Übermittlungsbefugnissen müssen verlässliche Austauschverfahren werden

§ 45 und § 51 BVerfSchG-E sowie § 85 BNDG-E schaffen Ansatzpunkte für den Austausch mit Unternehmen. Für die Sicherheitswirkung kommt es auf die praktische Ausgestaltung an. Für einen wirksamen Austausch braucht es klare Regelungen dazu, welche Behörde in welcher Lage welche Unternehmen informiert, über welche sicheren Kanäle dies erfolgt und wie Informati-

onen so aufbereitet werden, dass Unternehmen daraus konkrete Schutzmaßnahmen ableiten können.

Dies gilt insbesondere für den Austausch im Rahmen der Initiative Wirtschaftsschutz. Die Zusammenarbeit mit BND und BfV ist für die deutsche Industrie ein wichtiger Baustein, um Spionage, Sabotage, hybride Bedrohungen und Cyberangriffe besser zu erkennen und Risiken frühzeitig zu mindern. Der Entwurf kann diese Zusammenarbeit stützen, wenn aus den gesetzlichen Befugnissen ein verlässlicher operativer Austausch entsteht.

Mitwirkungs- und Auskunftspflichten der Wirtschaft klar und verhältnismäßig gestalten

Der Entwurf enthält Auskunfts-, Mitwirkungs- und Unterstützungspflichten gegenüber bestimmten nichtöffentlichen Stellen. Im BVerfSchG-E betrifft dies insbesondere §§ 11 bis 15 BVerfSchG-E, im BNDG-E insbesondere §§ 12 bis 16 BNDG-E. Je nach Regelung können unter anderem Telekommunikationsanbieter, digitale Dienste, Post- und Warenverkehrsdienste, Zahlungsdienste, Verkehrs- und Logistikunternehmen, Kraftfahrzeughersteller sowie Betreiber privater Videoüberwachung im öffentlich zugänglichen Raum betroffen sein.

Der BDI stellt nicht in Frage, dass Sicherheitsbehörden in konkreten Lagen auf Informationen oder Unterstützung bestimmter Unternehmen angewiesen sein können. Wichtig ist jedoch, dass Pflichten klar bestimmt, technisch und organisatorisch erfüllbar, verhältnismäßig und mit angemessenen Kostenregelungen verbunden sind. Sie dürfen kritische Geschäftsprozesse, den Betrieb Kritischer Infrastrukturen oder andere gesetzliche Pflichten der Unternehmen nicht unverhältnismäßig beeinträchtigen. Darüber hinaus müssen Auskunfts- und Mitwirkungspflichten klar nach Adressatenkreis, Unternehmensrolle und rechtlicher Verfügungsbefugnis abgegrenzt werden. Die Pflichten der §§ 11 bis 15 BVerfSchG-E und §§ 12 bis 16 BNDG-E richten sich nicht allgemein an die Wirtschaft, sondern an bestimmte Anbieter, mitwirkende Stellen und Verfügungsberechtigte. In arbeitsteiligen Liefer-, Daten-, Plattform-, Managed-Service- und Cloud-Strukturen kann im Einzelfall unklar sein, ob die verpflichtete Stelle über die betroffenen Informationen rechtlich eigenständig verfügen kann oder diese lediglich im Auftrag Dritter verarbeitet. Der Entwurf sollte daher klarstellen, dass verpflichtete Stellen nur zu Informationen herangezogen werden dürfen, über die sie rechtlich und tatsächlich verfügen können. Andernfalls drohen Rechtsunsicherheit, Haf-

tungsrisiken und Spannungen mit den Rollen- und Verantwortlichkeitsstrukturen der DSGVO.

Fehlt eine solche Klarstellung, können Rechtsunsicherheit sowie Standort- und Wettbewerbsnachteile für in Deutschland tätige Unternehmen entstehen, insbesondere für digitale und sicherheitsrelevante Dienstleister. Dies kann auch das Vertrauen internationaler Kunden beeinträchtigen. Für § 12 BVerfSchG-E bleibt der Kreis der verpflichteten Anbieter weiter zu präzisieren. Zwar erfasst der Wortlaut Anbieter, die informationstechnische Systeme geschäftsmäßig Dritten zur Nutzung überlassen und in Deutschland eine Niederlassung haben oder Leistungen erbringen. Für Unternehmen muss jedoch vorhersehbar sein, ob und in welcher Rolle sie von entsprechenden Ersuchen erfasst werden können. Da § 12 BVerfSchG-E hochsensible technische Informationen zu Angriffsinfrastruktur, Schadprogrammen, Protokolldaten und technisch verbundenen Spuren betrifft, sind für Übermittlung, Verarbeitung und Weitergabe gesicherte Schnittstellen, in gesicherten Umgebungen sowie ein strenges Need-to-know- und Berechtigungskonzept vorzusehen. Eine Miterfassung von Daten unbeteiligter Dritter oder anderer Kundinnen und Kunden ist dabei auszuschließen.

Ein kooperativer Ansatz bei der Aufklärung von Cyberangriffen erscheint hier zielführender als eine primär verpflichtungsorientierte Ausgestaltung. Der Entwurf sollte zudem klarstellen, wie sich die neuen Auskunfts- und Mitwirkungspflichten zu bestehenden spezialgesetzlichen Auskunfts- und Übermittlungsregelungen, insbesondere §§ 22, 23 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes (TDDDG) und § 174 des Telekommunikationsgesetzes (TKG), verhalten. Unternehmen benötigen eindeutige Vorgaben, welche Rechtsgrundlage in welchen Fallkonstellationen einschlägig ist und welche Datenschutz-, Geheimhaltungs- und Dokumentationspflichten jeweils gelten.

§ 12 Abs. 7 BVerfSchG-E verweist für die Entschädigung auf § 11 Abs. 7 BVerfSchG-E. Danach gelten grundsätzlich die Regelungen des Justizvergütungs- und -entschädigungsgesetzes; besondere Entschädigungsvereinbarungen sind möglich, wenn diese wegen besonderer Umstände keine angemessene Vergütung gewährleisten. Die praktische Tragfähigkeit dieser Regelung bleibt daher im weiteren Verfahren zu überprüfen, insbesondere mit Blick auf technisch aufwendige Erhebungs-, Aufbereitungs-, Sicherungs- und Übermittlungsleistungen. Staatlich veranlasste Unterstützungsleistungen dürfen nicht zu strukturellen Kostenbelastungen einzelner Unternehmen oder Branchen führen.

Die Unterstützungspflicht bei der Umleitung von Telekommunikation in § 13 Abs. 5 BVerfSchG-E ist bislang nicht hinreichend klar ausgestaltet und bedarf weiterer Präzisierung. Der Entwurf sieht in § 13 Abs. 6 BVerfSchG-E vor, dass verpflichtete Unternehmen Verschlusssachen des Grades VS-NfD (VERSCHLUSSSACHE – NUR FÜR DEN DIENSTGEBRAUCH) nach Maßgabe der gemäß § 35 Abs. 1 SÜG zu erlassenden allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz behandeln. Diesen pauschalen Rückgriff auf die Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung – VSA) halten wir für prüfungsbedürftig. Bei der VSA handelt es sich um eine Verwaltungsvorschrift des Bundes, die ihrem originären Anwendungsbereich nach an Bundesbehörden und bundesunmittelbare öffentlich-rechtliche Einrichtungen gerichtet ist. Abgesehen davon adressiert die VSA einen Nutzerkreis in der Sphäre der Bundesverwaltung und enthält Regelungen, die auf private Unternehmen in Teilen nicht ohne Weiteres anwendbar sind. So wirft insbesondere die Anwendung des Abschnitts VIII VSA auf verpflichtete Unternehmen Abgrenzungs- und Zuständigkeitsfragen auf, etwa mit Blick auf die IT-gestützte Verarbeitung von VS-NfD, die Freigabe des Betriebs von VS-IT, Nachweispflichten und Kontrollen. Des Weiteren ist zu prüfen, ob und inwieweit Einstufungs- und Kumulationslogiken der VSA auf private Unternehmen praxistauglich übertragbar sind. Schließlich sollte der Entwurf konkreter regeln, welche Anforderungen für den Umgang mit VS-NfD in IT-Systemen verpflichteter Unternehmen gelten.

Den Besonderheiten der Behandlung von VS-NfD in der Wirtschaft sollte auch im Kontext des BND-Gesetzes Rechnung getragen werden. Anstelle einer pauschalen Verweisung auf die VSA sollte geprüft werden, ob auf Anlage 4 des Handbuchs für den Geheimschutz in der Wirtschaft beziehungsweise auf das VS-NfD-Merkblatt des Bundesministeriums für Wirtschaft und Energie (BMWE) verwiesen werden kann. 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.

Zudem sollte der Entwurf redaktionell bereinigt werden: Gemäß Art. 22 soll das Artikel 10-Gesetz aufgehoben werden. Grundsätzlich wird die Konsolidierung der Gesetze begrüßt. Allerdings wird an mehreren Stellen weiterhin auf das Artikel 10-Gesetz verwiesen, etwa in Art. 19 Nr. 1 Buchst. a Doppelbuchst. aa oder in Art. 20 Nr. 4 Buchst. a.

Sicherheitsüberprüfungen mit Beschäftigtendatenschutz und Mitbestimmungsrecht harmonisieren

Der Entwurf enthält mit § 13 Abs. 6 BVerfSchG-E sowie § 12 Abs. 3 und § 13 Abs. 6 BNDG-E neue Vorgaben zum Einsatz geeigneten Personals bei verpflichteten Unternehmen. Danach können Unternehmen verpflichtet sein, Personen auszuwählen, einer einfachen Sicherheitsüberprüfung nach dem Sicherheitsüberprüfungsgesetz unterziehen zu lassen und über Mitteilungsverbote sowie die Strafbarkeit eines Verstoßes zu belehren. Die Einbeziehung von Unternehmensbeschäftigten in solche Verfahren ist dem Grunde nach nachvollziehbar. Verhältnismäßigkeit erfordert jedoch, dass Eingriffe in Persönlichkeitsrechte klar begrenzt und vorhersehbar sind. Zugleich müssen entsprechende Verfahren für Unternehmen planbar und zügig durchführbar sein, damit sicherheitsrelevante Tätigkeiten und industrielle Hochlaufprozesse nicht unverhältnismäßig verzögert werden.

Die Neuregelungen lassen aktuell noch keine hinreichende Harmonisierung mit den Vorgaben der DSGVO zum Beschäftigtendatenschutz und dem Mitbestimmungsrecht nach dem Betriebsverfassungsgesetz erkennen. Es fehlen eine Begrenzung der Mitwirkungspflicht auf rechtmäßig erhobene Daten, Klarstellungen zu besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO, Verfahrensregelungen für Mitarbeiter mit mehrfacher Staatsangehörigkeit sowie zeitliche Grenzen für laufende Überprüfungen. Für deutsche Unternehmen im internationalen Wettbewerb um qualifizierte Fachkräfte begründet diese Rechtsunsicherheit einen strukturellen Rekrutierungsnachteil.

Die Mitwirkungspflicht des Arbeitgebers ist daher auf rechtmäßig erhobene Daten zu beschränken. Die Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 DSGVO sollte ausdrücklich gesetzlich geregelt, auf das Erforderliche beschränkt und mit besonderen Schutzvorkehrungen versehen werden. Für internationale Sachverhalte sollte eine Rechtsverordnung des Bundesministeriums des Innern Verfahren und Zuständigkeiten regeln. Laufende Überprüfungen dürfen nur auf der Grundlage konkreter tatsächlicher Anhaltspunkte angeordnet werden; anlasslose Dauerüberwachung von Beschäftigten ist mit dem Verhältnismäßigkeitsgrundsatz unvereinbar.

Normkonflikte mit europäischem Recht geordnet auflösen

Die Auskunftspflichten (§§ 11 ff. BVerfSchG-E), die Geheimhaltungspflichten (§ 13 BVerfSchG-E) und die Vorgaben zum Einsatz sicherheitsüberprüf-

ten Personals bei verpflichteten Unternehmen (§ 13 Abs. 6 BVerfSchG-E sowie § 12 Abs. 3 und § 13 Abs. 6 BNDG-E) berühren Bereiche, die durch europäisches Primär- und Sekundärrecht überlagert werden. Dies betrifft insbesondere die DSGVO, die Grundrechte der Charta der Grundrechte der Europäischen Union (Art. 7, 8 und 47 GRC), die NIS-2-Richtlinie sowie die CER-Richtlinie. Der Entwurf enthält hierfür keinen ausdrücklichen Klärungsmechanismus. Unternehmen müssen solche Konflikte im Einzelfall selbst auflösen, mit dem Risiko widersprüchlicher Rechtspflichten.

Konkret kann ein Spannungsverhältnis zwischen Geheimhaltungspflichten nach § 13 BVerfSchG-E in Verbindung mit § 9 Abs. 3 BVerfSchG-E, Informationspflichten nach Art. 13 und 14 DSGVO sowie vertraglichen Informations- oder Offenlegungspflichten in grenzüberschreitenden Dienstleistungs-, Plattform-, Managed-Service- und Cloud-Strukturen entstehen. Für inländische Verpflichtete in internationalen Vertrags- und Konzernstrukturen bleibt unklar, wie sie mit kollidierenden Geheimhaltungs-, Datenschutz- und Offenlegungspflichten umgehen sollen. Der Entwurf sieht hierfür keinen geordneten Klärungsmechanismus vor.

Vor diesem Hintergrund sollte in den Regelungen zu Auskunfts-, Mitwirkungs- und Geheimhaltungspflichten ausdrücklich klargestellt werden, dass diese unionsrechtskonform anzuwenden sind und zwingende Vorgaben des europäischen Datenschutzrechts unberührt bleiben. Zudem sollte insbesondere § 13 BVerfSchG-E um ein Verfahren für Kollisionsfälle ergänzt werden. Bestehen nachvollziehbare Anhaltspunkte für einen Konflikt zwischen Geheimhaltungspflichten nach dem Nachrichtendienstrecht und zwingenden gesetzlichen oder vertraglichen Pflichten, sollte das verpflichtete Unternehmen eine behördliche Klärung verlangen und den Unabhängigen Kontrollrat über den Konflikt unterrichten können. In eilbedürftigen oder streitigen Fällen sollte eine unabhängige Kontrolle oder gerichtlicher Eilrechtsschutz vorgesehen werden.

Umgang mit IT-Schwachstellen eng einhegen

Besonders sensibel ist der im Entwurf angelegte Informationsfluss vom Bundesamt für Sicherheit in der Informationstechnik (BSI) an den Bundesnachrichtendienst (BND) im Cyberkontext. § 10 Abs. 2 Nr. 2 BNDG-E sieht eine Übermittlungspflicht des BSI an den BND vor. Die Begründung zu § 10 BNDG-E zielt darauf ab, bestehende rechtliche Unsicherheiten bei Datenübermittlungen des BSI an den BND zu beseitigen und einen frühzeitigen

Informationsaustausch im Zusammenhang mit Cybervorfällen zu ermöglichen.

Der BDI erkennt das legitime Interesse staatlicher Stellen an der Gewinnung cyberbezogener Erkenntnisse an. Gleichzeitig ist die Cybersicherheit von Wirtschaft, Staat und Gesellschaft selbst ein sicherheitspolitisches und wirtschaftliches Gut von strategischer Bedeutung. Der Umgang mit Schwachstelleninformationen darf daher nicht dazu führen, dass die Cybersicherheit insgesamt geschwächt wird.

Bekannte Schwachstellen sollten grundsätzlich einer möglichst schnellen Bewertung, verantwortungsvollen Offenlegung und Behebung zugeführt werden. Bei Entscheidungen über die Nutzung oder Zurückhaltung von Schwachstelleninformationen sind mögliche Auswirkungen auf die Cybersicherheit der Wirtschaft sowie potenzielle Folgewirkungen für Wertschöpfungsnetzwerke und Kritische Infrastrukturen zu berücksichtigen.

Regelungen, die eine zeitweise Zurückhaltung oder Nutzung von Schwachstelleninformationen ermöglichen, bedürfen daher einer besonders sorgfältigen Abwägung zwischen den Aufklärungsinteressen der Sicherheitsbehörden einerseits und den Sicherheitsinteressen von Wirtschaft, Staat und Gesellschaft andererseits. Abweichungen vom Grundsatz einer zügigen Bewertung und Behebung von Schwachstellen kommen nur unter engen Voraussetzungen in Betracht und unterliegen klaren Zuständigkeiten, nachvollziehbarer Dokumentation sowie wirksamen Kontrollmechanismen.

Eng verwandt mit dem Umgang mit Schwachstelleninformationen ist die Frage der Verhältnismäßigkeit beim Zugriff auf laufende Netzwerk- und IT-Infrastruktur. Die im Entwurf vorgesehenen Befugnisse zur Verfolgung technischer Angriffsspuren (§§ 12, 24 BVerfSchG-E / § 36 BNDG-E) können Eingriffe in aktive Betriebsinfrastruktur ermöglichen. Zwar enthält der Entwurf bereits Ansätze einer Subsidiaritätslogik; diese sollten jedoch für Eingriffe in laufende Betriebsinfrastruktur ausdrücklich konkretisiert werden. Eingriffe in laufende Systeme können über das eigentliche Zielobjekt hinausgehende Betriebsstörungen auslösen und bei Betreibern Kritischer Infrastruktur kaskadierende Wirkungen entfalten.

Die vorhandene Subsidiaritätslogik bedarf einer ausdrücklichen Konkretisierung. Eingriffe in laufende Betriebsinfrastruktur dürfen nur angeordnet werden, wenn die erforderlichen Erkenntnisse nicht durch Auswertung bereits gespeicherter Protokolldaten oder durch Kooperation mit dem Betreiber auf weniger eingriffsintensive Weise gewonnen werden können. Dies entspricht

der im BSI-Gesetz bereits angelegten Kooperationslogik zwischen Staat und Infrastrukturbetreibern und ist zugleich Ausdruck des verfassungsrechtlich gebotenen Verhältnismäßigkeitsgrundsatzes. Der Betreiber ist grundsätzlich vor einem Eingriff anzuhören; eine nachträgliche Unterrichtung ist in Ausnahmefällen unverzüglich nachzuholen.

Wirtschaft in die Gesamtverteidigung einbinden

Der Entwurf enthält besondere Bestimmungen zur Landes- und Bündnisverteidigung. Für das BNDG-E sind insbesondere §§ 125 bis 127 BNDG-E relevant. Sie betreffen den Verteidigungs-, Spannungs- und Zustimmungsfall, die Unterstützung durch andere Stellen und die Datenerhebung unter Mitwirkung anderer Stellen.

Für solche Lagen braucht es eine frühzeitige Konkretisierung der Anforderungen an Unternehmen. Gesamtverteidigung setzt voraus, dass Staat und Wirtschaft möglichst bereits vor einer Krise wissen, welche Beiträge erforderlich sind, welche Verfahren gelten, welche Kommunikationswege genutzt werden und wie Haftung, Vergütung, Geheimschutz und Priorisierung ausgestaltet sind. Unternehmen bilden mit ihren Kapazitäten, Lieferketten, digitalen Infrastrukturen und logistischen Fähigkeiten zentrale Pfeiler der Resilienz und Verteidigungsfähigkeit.

5. Fazit

Der Entwurf enthält wichtige Ansatzpunkte, um Wirtschaftsschutz und KRITIS-Schutz im Nachrichtendienstrecht konkreter abzubilden. Für den BND betrifft dies die Benennung wirtschafts-, technologie-, versorgungs- und infrastrukturspezifischer Bedrohungsziele in §§ 3 und 4 BNDG-E. Für das BfV betrifft dies die Information über präventiven Wirtschafts- und Wissenschaftsschutz nach § 45 Abs. 1 BVerfSchG-E und die Übermittlung an Unternehmen und andere nichtöffentliche Stellen nach § 51 Abs. 1 Nr. 3 BVerfSchG-E. Für beide Dienste sind die Übermittlungsregelungen an nichtöffentliche Stellen zentrale Schnittstellen zur Wirtschaft, insbesondere § 51 BVerfSchG-E und § 85 BNDG-E.

Gleichzeitig müssen die Auskunfts- und Mitwirkungspflichten so ausgestaltet sein, dass sie mit dem europäischen Datenschutzrecht vereinbar sind und mögliche Kollisionslagen in grenzüberschreitenden Vertrags-, Konzern- und Dienstleistungsstrukturen rechtssicher aufgefangen werden. Dafür braucht es mehrere Klarstellungen: die rechtssichere Bestimmung der Auskunftspflicht

gegenüber Auftragsverarbeitern, die klare Zuordnung des jeweils verpflichteten Rechtsträgers bei internationalen Unternehmensgruppen und die Konkretisierung der Subsidiaritätsvorgaben beim Eingriff in laufende Infrastruktur. Hinzu kommen die Harmonisierung der Sicherheitsüberprüfungen mit dem Beschäftigtendatenschutz, die geordnete Auflösung von Normkonflikten mit europäischem Recht sowie verbindliche Zweckbindungs- und Löschungsregelungen für übermittelte Daten. Aus Sicht des BDI ist entscheidend, dass diese Regelungen zu einer Erhöhung der Sicherheit in der Praxis führen. Maßgeblich sind rechtssichere Austauschverfahren, ein belastbares Lageverständnis von Staat und Wirtschaft, verhältnismäßige Mitwirkungspflichten und ein Umgang mit IT-Schwachstellen, der die Cybersicherheit der Wirtschaft nicht schwächt. Sicherheit im allgemeinen und Wirtschaftsschutz im Besonderen wird nicht allein durch zusätzliche Befugnisse gestärkt. Dies entsteht durch Vertrauen, klare Zuständigkeiten, einen belastbaren Informationsaustausch und handlungsfähige Kooperation zwischen den Sicherheitsbehörden und der Wirtschaft.

Über den BDI

Der BDI transportiert die Interessen der deutschen Industrie an die politisch Verantwortlichen. Damit unterstützt er die Unternehmen im globalen Wettbewerb. Er verfügt über ein weit verzweigtes Netzwerk in Deutschland und Europa, auf allen wichtigen Märkten und in internationalen Organisationen. Der BDI sorgt für die politische Flankierung internationaler Markterschließung. Und er bietet Informationen und wirtschaftspolitische Beratung für alle industrierelevanten Themen. Der BDI ist die Spitzenorganisation der deutschen Industrie und der industrienahen Dienstleister. Er spricht für 38 Branchenverbände und mehr als 100.000 Unternehmen mit rund acht Mio. Beschäftigten. Die Mitgliedschaft ist freiwillig. 15 Landesvertretungen vertreten die Interessen der Wirtschaft auf regionaler Ebene.

Impressum

Bundesverband der Deutschen Industrie e.V. (BDI)
Breite Straße 29, 10178 Berlin
www.bdi.eu
T: +49 30 2028-0

Lobbyregisternummer: R000534

Ansprechpartner

Kerstin Petretto
Senior Referentin Sicherheit und Verteidigung
T: +49 30 2028-1710
k.petretto@bdi.eu

Steven Heckler
Senior Referent Cybersicherheit und Digitale Unternehmensidentitäten
T: +49 30 2028-1523
s.heckler@bdi.eu

BDI Dokumentennummer: D 2337