Deutscher Bundestag **Drucksache 21/7406**

21. Wahlperiode

(zu Drucksache 21/6585)
29.07.2026

Unterrichtung

durch die Bundesregierung

Entwurf eines Gesetzes zur Stärkung der Cybersicherheit
– Drucksache 21/6585 –

Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung

Stellungnahme des Bundesrates

Der Bundesrat hat in seiner 1067. Sitzung am 10. Juli 2026 beschlossen, zu dem Gesetzentwurf gemäß Artikel 76 Absatz 2 des Grundgesetzes wie folgt Stellung zu nehmen:

1. Zum Gesetzentwurf allgemein
   a) Der Bundesrat bittet, zu prüfen, ob die aus dem Gesetzentwurf resultierenden Belastungen für die betroffenen Unternehmen in ihrer Gesamtheit angemessen sind.
   b) Er bittet auch darum, zu prüfen, ob den betroffenen Unternehmen ein entsprechendes Unterstützungsangebot gemacht und wie sichergestellt werden kann, dass Maßnahmen im Zuge der Gefahrenabwehr und Strafverfolgung bei dadurch eventuell verursachten Nachteilen bei Dritten nicht zu Haftungsansprüchen gegenüber dem betroffenen Unternehmen führen.
   c) In diesem Zusammenhang bittet der Bundesrat zudem, im weiteren Gesetzgebungsverfahren sicherzustellen, dass die im Gesetzentwurf vorgesehenen Regelungen zur Weitergabe teils hochsensibler Daten den für die Strafverfolgung und Strafvereitelung zwingend notwendigen Umfang nicht überschreiten.
   d) Der Bundesrat fordert, notwendige Sanktionen für Verstöße gegen Mitwirkungs- und Informationspflichten sowie gegen Offenbarungsverbote verhältnismäßig auszugestalten und die entsprechenden Anforderungen an die Unternehmen klar zu definieren. Bei der Festlegung der entsprechenden Bußgelder ist die hohe finanzielle Belastung, welche für die betroffenen Unternehmen im Falle eines Cyberangriffs ohnehin bereits entsteht, zu berücksichtigen.
   e) Der Bundesrat bittet, die Harmonisierung des Gesetzentwurfs mit bereits bestehenden Regulierungen sicherzustellen. Mehrfachregulierungen wie etwa durch parallele Melde- und Reportingpflichten sowie übermäßige bürokratische Aufwände für die Unternehmen sind in jedem Fall zu vermeiden.
   f) Der Bundesrat weist zudem darauf hin, dass bereits bestehende kooperative Ansätze zwischen Behörden und Unternehmen im Bereich der Cybersicherheit, die beispielsweise das gegenseitige Teilen von Informationen umfassen, adäquat im geplanten Gesetz berücksichtigt werden sollten.

   Begründung:
   Die weiterhin angespannte Cybersicherheitslage sowie eine Vielzahl neuer Regulierungen im Bereich Cybersicherheit resultieren in hohen bürokratischen und finanziellen Belastungen für Unternehmen. Vor diesem Hintergrund sollte eine zusätzliche übermäßige Belastung von Unternehmen durch hohe Bußgelder, unan-

gemessene bürokratische Mehraufwände oder Doppelregulierungen wie beispielsweise durch Überschneidungen mit den in der NIS-2-Richtlinie definierten Melde- und Reportingpflichten in jedem Fall vermieden werden. Gleichzeitig ist die Möglichkeit für Unternehmen, ihre sensiblen Daten und Geschäftsgeheimnisse vor unerlaubten Zugriffen zu schützen, Grundvoraussetzung für einen funktionierenden und innovativen Wettbewerb. Deshalb sollte die Verpflichtung der Unternehmen zur Weitergabe entsprechender Daten, auch im Sinne der Gefahrenabwehr, nach möglichst engen und klar definierten Maßgaben erfolgen. Ebenso müssen hohe Cybersicherheits- und Datenschutzstandards bei der Übertragung, weiteren Verarbeitung und Speicherung der Daten durch alle beteiligten Stellen sichergestellt werden.

Über die Einbindung und Stärkung freiwilliger, kooperativer Ansätze parallel zu den im Gesetzentwurf vorgesehenen weitgehenden Befugnissen der Behörden, soll zudem sichergestellt werden, dass die Cybersicherheit im Zusammenschluss von staatlichen und wirtschaftlichen Akteuren gemeinsam gestärkt wird. Nur so kann durch die Einbindung aller relevanter Akteure eine vertrauensvolle Zusammenarbeit gelingen.

2. Zu Artikel 2 Nummer 5 (§ 15 Absatz 6 BSIG)

Der Bundesrat bittet, die geplante Regelung in § 15 Absatz 6 BSIG-E, wonach das BSI bestimmte Auskünfte über sicherheitsrelevante technische Informationen verlangen kann, weiter zu konkretisieren und zudem Anforderungen an die Sicherheit der Übertragungswege festzulegen.

Begründung:

Die vorgesehene Begrenzung der Informationsbereitstellung auf technische Durchführbarkeit und wirtschaftliche Zumutbarkeit sollte konkretisiert werden, damit Unternehmen Rechtssicherheit haben, wann eine Ausnahme greift. Zudem ist eine weitere Präzisierung der verlangten Informationen notwendig, da zahlreiche unbestimmte Begriffe verwendet werden. Die Unternehmen müssen Klarheit über die zu liefernden Daten haben. Da es um die Übertragung hochsensibler Daten geht, sind ausreichende Vorkehrungen zu treffen, um den Schutz und die Vertraulichkeit der übermittelten Daten zu gewährleisten. Ein sicherer und praxistauglicher Austausch von Informationen ist sicherzustellen. Hierzu kommen zum Beispiel standardisierte Schnittstellen mit Ende-zu-Ende-Verschlüsselung in Betracht. Anforderungen an die Sicherheit der Übertragungswege sollten bereits gesetzlich festgelegt werden.

3. Zu Artikel 3 Nummer 9 (§ 68d Absatz 1 BKAG)

Der Bundesrat spricht sich dafür aus, dass Maßnahmen nach § 68d Absatz 1 BKAG-E nur durch das Gericht angeordnet werden dürfen.

Begründung:

Es gibt keine hinreichende Begründung, warum Maßnahmen in nicht private informationstechnische Systeme gemäß 68d Absatz 1 BKAG-E keiner richterlichen Anordnung bedürfen sollten. Häufig ist eine Abgrenzung zwischen privaten und kommerziellen Systemen erst im Nachhinein möglich. Informationstechnische Systeme werden heutzutage oft gleichzeitig sowohl zu privaten als auch gewerblichen Zwecken genutzt. Vor diesem Hintergrund ist nicht nachvollziehbar, warum für einen Eingriff in Systeme von Unternehmen kein Richtervorbehalt als nötig erachtet wird. Unternehmen sind durch aktive Eingriffe in ihre IT-Infrastruktur ohne Kenntnis ebenso in ihren Grundrechten beeinträchtigt. Entsprechende Maßnahmen sollten daher generell, unabhängig von der Nutzungsart des betroffenen Systems, einer richterlichen Anordnung bedürfen.

4. Zu Artikel 3 Nummer 9 (§ 68e Absatz 3, § 68f Absatz 2 BKAG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren die Bestimmung der konkreten gerichtlichen Zuständigkeit einschließlich der diesbezüglichen Verfahrensregelungen für § 68e Absatz 3 und § 68f Absatz 2 BKAG-E zu prüfen.

Begründung:

In der derzeitigen Fassung sehen § 68e Absatz 3 und § 68f Absatz 2 BKAG-E zwar einen Richtervorbehalt bzw. ein gerichtliches Zustimmungserfordernis vor, enthalten jedoch keine entsprechende Bestimmung der konkreten gerichtlichen Zuständigkeit sowie der diesbezüglichen Verfahrensregelungen wie dies etwa § 41a

Absatz 6 bzw. Absatz 11 Satz 2 und 3 BPolG-E vorsehen. Auch einen alternativ in Betracht kommenden Verweis in § 90 BKAG auf den neu einzuführenden Abschnitt 8a enthält der Gesetzentwurf nicht.

Unter diesen Umständen ist nach der derzeit vorgesehenen gesetzlichen Regelung weder klar, welches Gericht entscheidet, noch nach welcher Verfahrensordnung eine Entscheidung zu treffen ist.

Der in § 68f Absatz 2 BKAG-E enthaltene Verweis auf § 74 Absatz 3 Satz 5 und 6 BKAG erscheint unzureichend. Zwar fällt § 74 BKAG als solcher in den Anwendungsbereich von § 90 Absatz 1 BKAG, allerdings verweist § 68f Absatz 2 BKAG-E hinsichtlich der grundsätzlichen Erforderlichkeit einer gerichtlichen Entscheidung für eine über zwölf Monate hinausgehende Zurückstellung gerade nicht auf § 74 (Absatz 3 Satz 1) BKAG.

Gegenäußerung der Bundesregierung

Die Bundesregierung äußert sich zur Stellungnahme des Bundesrates vom 10. Juli 2026 wie folgt:

Zu Nummer 1 (zum Gesetzentwurf allgemein)

Die Bundesregierung lehnt die Vorschläge des Bundesrats insgesamt ab.

Zu a)

Aus Sicht der Bundesregierung sind die Belastungen angemessen. Sie sind ins Verhältnis zu setzen zu einem deutlichen Gewinn an Sicherheit. Bei der Übermittlung von Informationen nach § 31 Absatz 3 Nummer 2 des BSI-Gesetzes in der Entwurfsfassung (BSIG-E) und § 5c Absatz 7 Nummer 2 des Energiewirtschaftsgesetzes in der Entwurfsfassung (EnWG-E) ist zu beachten, dass nur die Informationen weiterzuleiten sind, die in den bereits gegenwärtig obligatorischen Systemen zur Angriffserkennung anfallen. Zudem entfallen bestimmte Nachweispflichten für Betreiber kritischer Anlagen infolge der Anpassung in § 39 Absatz 1 BSIG-E.

Zu b)

Maßnahmen im Zuge der Gefahrenabwehr führen aus Sicht der Bundesregierung grundsätzlich nicht zu Haftungsansprüchen gegen Unternehmen, wenn diese aufgrund einer sicherheitsbehördlichen Anordnung handeln.

Zu c)

Die Weitergabe von Daten durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterliegt in den Fällen der Datenverarbeitung nach § 8 BSIG (Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes) sowie künftig auch für die Verarbeitung der durch Umleitungen erhobenen Daten (§§ 16 ff. BSIG-E) engen Grenzen und ist auf den erforderlichen Umfang beschränkt. Der insoweit einschlägige § 8 Absatz 6 und 7 BSIG-E ist wie bisher nicht auf Zwecke der Strafverfolgung begrenzt, sondern schließt auch notwendige Zwecke der Gefahrenabwehr und Gefahrenaufklärung mit ein.

Soweit personenbezogene oder dem Fernmeldegeheimnis unterliegende Daten verarbeitet werden, haben die beteiligten Stellen – wie in anderen Fällen auch – grundsätzlich angemessene Vorkehrungen zum Vertraulichkeitsschutz zu treffen. Für die automatisierte Übermittlung von Daten nach § 31 BSIG-E bzw. § 5c Absatz 7 EnWG-E sind entsprechende Vorgaben im Rahmen des von dem BSI bzw. der Bundesnetzagentur (BNetzA) im Einvernehmen mit BSI nach Anhörung der Betreiber und Wirtschafts- bzw. Branchenverbände zu erstellenden Übermittlungsstandards zu berücksichtigen.

Zu d)

Aus Sicht der Bundesregierung sind die vorgesehenen Sanktionsrahmen angemessen und die Tatbestände hinreichend konkret ausgestaltet.

Zu e)

Die Vereinbarkeit des Entwurfs mit bestehenden Melde- und Registrierungspflichten wurde bei Erstellung des Entwurfs sorgfältig geprüft. Überschneidungen und unnötige bürokratische Aufwände entstehen aus Sicht der Bundesregierung nicht. Insbesondere handelt es sich bei den Übermittlungspflichten nach § 31 Absatz 3 BSIG-E und § 5c Absatz 7 EnWG-E um eine (teil-)automatisierte Bereitstellung von Informationen. Der Entwurf sieht im Gegenzug vor, dass Nachweispflichten nach § 39 Absatz 1 BSIG-E entfallen.

Zu f)

Bestehende kooperative Ansätze werden durch den Gesetzentwurf nicht beeinträchtigt, sondern sind weiterhin zentraler Bestandteil der nationalen Sicherheitsgewährleistung.

Zu Nummer 2 (Artikel 2 Nummer 5 – § 15 Absatz 6 BSIG-E)

Die Bundesregierung lehnt den Vorschlag ab. Der Begriff der technischen und wirtschaftlichen Zumutbarkeit ist hinreichend etabliert – in den einschlägigen Gesetzen (wie zum Beispiel in § 169 Abs 4 und 5 des Telekommunikationsgesetzes, § 19 Absatz 2 und 4 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes) entsprechend konkretisiert. Die Voraussetzungen des Auskunftsverlangens sind damit hinreichend rechtsklar. Sie ermög-

lichen, auf die Verhältnisse der einzelnen Unternehmen einzugehen. Dies wäre nicht möglich, wenn stattdessen auf starre Einzelkriterien abgestellt würde.

Aus Sicht der Bundesregierung sind die zu übermittelnden Informationen hinreichend konkretisiert: Die Übermittlungspflicht ist auf sicherheitsrelevante technische Informationen begrenzt. Der Begriff der technischen Informationen wird bereits in § 21 Absatz 1 des MAD-Gesetzes verwendet und ist daher geltendes Recht. Zusätzlich werden die zu übermittelnden Informationen durch die in § 15 Absatz 6 Satz 1 BSIG-E benannten Voraussetzungen weiter auf gesetzlicher Ebene konkretisiert und auf angriffsbezogene Parameter beschränkt. Welche Informationen im Einzelfall zu übermitteln sind, ergibt sich jeweils eindeutig aus der entsprechenden Anordnung des BSI.

Auf konkrete Anforderungen zur Art der Übermittlung (etwa in elektronischer oder automatisierter Form) wurde verzichtet, um die betroffenen Unternehmen nicht über Gebühr zu belasten. Abhängig von der Art der zu übermittelnden Daten und der gewählten Übermittlungsform, zu denen die gesetzliche Regelung den betroffenen Unternehmen keine Vorgaben macht, können Anforderungen an eine sichere Übermittlung grundsätzlich heterogen ausgestaltet sein. Sollte im Einzelfall eine besondere Art der Übermittlung sachgerecht und erforderlich sein, ist dem im Rahmen der Bewertung der wirtschaftlichen Zumutbarkeit in der Übermittlungsanordnung des BSI Rechnung zu tragen.

Zu Nummer 3 (Artikel 3 Nummer 9 – § 68d Absatz 1 BKAG-E)

Die Bundesregierung lehnt den Vorschlag ab. Die Unterscheidung zwischen privater und nicht privater IT sowie die sich darauf beziehende Regelung eines Richtervorbehalts knüpft an die Betroffenheit des IT-System-Grundrechts als Ausprägung des allgemeinen Persönlichkeitsrechts an (vgl. zum Schutzbereich des IT-System-Grundrechts BVerfG, Beschluss vom 24. Juni 2025 – 1 BvR 2466/19 (Trojaner I), Leitsatz 2a), Rn. 97; BVerfG, Beschluss vom 24. Juni 2025 – 1 BvR 180/23 (Trojaner II).

Zu Nummer 4 (Artikel 3 Nummer 9 – § 68e Absatz 3, § 68f Absatz 2 BKAG-E)

Die Bundesregierung hat die vom Bundesrat erbetene Prüfung vorgenommen und wird im parlamentarischen Verfahren einen Vorschlag für eine entsprechende Ergänzung des § 90 BKAG vorlegen.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.bundesanzeiger-verlag.de
ISSN 0722-8333