Bundesrat **Drucksache** **323/1/26**

26.06.26

Empfehlungen
der Ausschüsse

In - DS - R - Wi

zu **Punkt ...** der 1067. Sitzung des Bundesrates am 10. Juli 2026

Entwurf eines Gesetzes zur Stärkung der Cybersicherheit

A

Der **Rechtsausschuss** (R) und

der **Wirtschaftsausschuss** (Wi)

empfehlen dem Bundesrat, zu dem Gesetzentwurf gemäß Artikel 76 Absatz 2 des Grundgesetzes wie folgt Stellung zu nehmen:

Wi 1. Zum Gesetzentwurf allgemein

a) Der Bundesrat erkennt das mit dem Entwurf eines Gesetzes zur Stärkung der Cybersicherheit verfolgte Anliegen ausdrücklich an. Die Bedrohungslage im digitalen Raum hat sich in den vergangenen Jahren nicht nur quantitativ, sondern auch qualitativ grundlegend gewandelt. Professionell organisierte Ransomware-Kampagnen, staatlich gesteuerte Angriffe und hybride Bedrohungsformen stellen sowohl die Widerstandsfähigkeit kritischer Infrastrukturen als auch das überkommene Instrumentarium des Gefahrenabwehrrechts vor neue Herausforderungen. Die Schaffung gesetzlicher Grundlagen für eine handlungsfähige, auch aktive Cyberabwehr ist im Grundsatz nicht nur akzeptabel, sondern angesichts der sich verschärfenden Bedrohungslage dringend sachlich geboten. Andere EU-Staaten wie beispielsweise Frankreich und die Niederlande verfügen bereits über vergleichbare Befugnisse oder arbeiten derzeit an entsprechenden Regelungen. Deutschland sollte bei dieser Entwicklung den Anschluss wahren.

...

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 0720-2946

b) Zugleich gilt: Das Gebot wirksamer Gefahrenabwehr im digitalen Raum rechtfertigt es nicht, rechtsstaatliche Sicherungen zu lockern, deren Schutzwirkung sich gerade unter den Bedingungen einer verschärften Bedrohungslage bewähren muss. Ein Zuwachs an staatlicher Handlungsfähigkeit im Cyberraum und die Wahrung rechtsstaatlicher Prinzipien stehen nicht in einem Gegensatz. Im Gegenteil sichert erst eine rechtsstaatlich saubere, verhältnismäßige und für die betroffenen Wirtschaftszweige berechenbare Ausgestaltung die dauerhafte Akzeptanz und damit die praktische Wirksamkeit der neuen Befugnisse. Mehr digitale Sicherheit erfordert daher mehr, nicht weniger Sorgfalt und Abwägungsbereitschaft bei den begleitenden Verfahrens- und Kontrollmechanismen.

c) Der Bundesrat stellt fest, dass der vorliegende Gesetzentwurf die notwendige Balance zwischen staatlicher Handlungsfähigkeit im Cyberraum und einer angemessenen rechtsstaatlichen Eingrenzung der neu geschaffenen, besonders eingriffsintensiven Befugnisse noch nicht in vollem Umfang erreicht hat. Der Bundesrat hält es daher für erforderlich, den Entwurf im weiteren Gesetzgebungsverfahren in den nachfolgend bezeichneten Punkten anzupassen. Er verfolgt damit das Ziel, die mit dem geplanten Gesetz angestrebten Sicherheitsgewinne zu erhalten und sie zugleich auf ein rechtsstaatlich tragfähiges, grundrechtsschonendes und für die betroffenen Wirtschaftszweige verlässliches Fundament zu stellen. Hierzu bedarf es insbesondere der folgenden Anpassungen:

aa) Schutz unbeteiligter Dritter, Vermeidung von Kollateralschäden, Mehrwerte für Betreiber kritischer Infrastruktur

Mehrere der vorgesehenen Eingriffsbefugnisse setzen an gemeinsam genutzter digitaler Infrastruktur an und können dadurch über die eigentlich Verantwortlichen hinaus auch rechtstreue Diensteanbieter und nicht beteiligte Nutzerinnen und Nutzer beeinträchtigen. Besonders deutlich wird dies bei Maßnahmen, die pauschal an ganze Domains anknüpfen, ohne zwischen den zugrunde liegenden Sachverhalten zu unterscheiden – etwa zwischen einer gezielt zu schädlichen Zwecken eingerichteten und einer ursprünglich legitimen, erst nachträglich von Dritten missbrauchten Infrastruktur. Lässt sich ein Eingriff technisch nicht auf den schädlichen Teil begrenzen, drohen unverhältnismäßige Kollateralschäden zulasten Unbeteiligter. Die maßgeblichen Begriffe und Anwendungsvoraussetzungen des

Gesetzentwurfs sollten daher klarer gefasst und so ausdifferenziert werden, dass die unterschiedlichen Fallgestaltungen angemessen berücksichtigt werden können. Eingriffe sollten zudem so zielgenau, abgestuft, zeitlich begrenzt und umkehrbar wie möglich ausgestaltet sein; breit wirkende, eine Vielzahl von Nutzerinnen und Nutzer erfassende Maßnahmen sollten nur als letztes Mittel und nur dann in Betracht kommen, wenn der Schutz Unbeteiligter gewahrt bleibt und eine zügige Korrektur fehlerhafter oder überschießender Eingriffe sichergestellt ist. Verpflichtet der Entwurf Betreiber kritischer Infrastrukturen – etwa im Energiesektor – zu einer fortlaufenden Übermittlung sicherheitsrelevanter Daten an das Bundesamt für Sicherheit in der Informationstechnik, sollte zu deren Schutz im Gegenzug ein verbindlicher, strukturierter Informationsrückkanal verankert werden, damit die betroffenen Betreiber die für die eigene Abwehr erforderlichen Erkenntnisse zeitnah zurückerhalten können.

bb) Wahrung rechtsstaatlicher Verfahrensprinzipien
Ein Teil der neuen Eingriffsbefugnisse erreicht das Niveau besonders grundrechtssensibler, verdeckter Maßnahmen, ohne durchgängig mit den hierfür anerkannten rechtsstaatlichen Sicherungen verbunden zu sein. So eröffnet eine generalklauselartige Ermächtigung im Bundeskriminalamtgesetz ein sehr weites Eingriffsfeld. Sie trägt dem Bestimmtheitsgebot nicht hinreichend Rechnung und sollte auf einen klar umgrenzten Katalog zulässiger Maßnahmen zurückgeführt werden. Eine vorherige unabhängige, richterliche Kontrolle ist zudem bislang im Wesentlichen auf heimliche Zugriffe auf private Systeme beschränkt, während andere, ebenfalls grundrechtsrelevante Maßnahmen – etwa das Verbot, einzelne informationstechnische Systeme weiter zu betreiben, oder das Umleiten, Einschränken und Unterbinden von Datenverkehr – ohne eine solche Kontrolle bleiben. Der Richtervorbehalt sollte daher auf diese Maßnahmen erweitert werden. Schließlich sollte für heimliche Eingriffe in private Systeme eine gesetzlich bestimmte Höchstdauer vorgesehen werden. Die im Gefahrenabwehr- und Strafverfahrensrecht etablierten Grundsätze wie eine hinreichende Bestimmtheit der Befugnisse, richterliche Kontrolle eingriffsintensiver Maßnahmen und klare zeitliche Grenzen verdeckten staatlichen Handelns müssen auch bei Verfahren im Cyberraum uneingeschränkt

gewahrt bleiben.

cc) Evaluierung und Befristung
Der Entwurf sieht ausdrücklich weder eine Befristung noch eine Evaluierung der neuen Regelungen vor. Das ist bei Befugnissen, die in ihrer Eingriffstiefe und technischen Neuartigkeit ohne unmittelbares Vorbild sind und sich in einem Feld besonders rascher technologischer Veränderung bewegen, nicht sachgerecht. Der Nationale Normenkontrollrat hat in seiner Stellungnahme ausdrücklich festgestellt, dass das Vorhaben evaluierungspflichtig ist. Seiner Empfehlung der Aufnahme einer Evaluierungsklausel mit definierten Zielen und Erfolgskriterien sollte gefolgt werden. Erst eine Evaluierung macht Wirkung, Verhältnismäßigkeit und etwaige unbeabsichtigte Folgen der Befugnisse auch für die betroffenen Wirtschaftszweige überprüfbar. Für die besonders eingriffsintensiven, neuartigen Befugnisse sollte darüber hinaus eine Befristung mit Verlängerungsvorbehalt geprüft werden, um nach Vorliegen der Evaluierungsergebnisse eine bewusste gesetzgeberische Neubefassung sicherzustellen.

d) Der Bundesrat ist überzeugt, dass die vorgeschlagenen Anpassungen das mit dem Gesetzentwurf verfolgte Ziel einer gestärkten staatlichen Cyberabwehr nicht schwächen, sondern es auf eine rechtsstaatlich tragfähige, verhältnismäßige und für die betroffenen Wirtschaftszweige berechenbare Grundlage stellen.

Wi 2. <u>Zum Gesetzentwurf allgemein</u>

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, unangemessene 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.

Wi 3. Zu Artikel 1 Nummer 2 (§ 41a Absatz 1 BPolG), Artikel 3 Nummer 9 (§§ 68b bis 68d BKAG)

Der Bundesrat bittet, § 41a Absatz 1 BPolG-E und die §§ 68b bis 68d BKAG-E zu prüfen. Die Normen sehen offensive Eingriffsbefugnisse für Bundesbehörden vor. Diese sind mit Risiken und Eingriffen in die Rechte der Betroffenen verbunden. Daher sollte geprüft werden, die Cyberabwehr auf defensive Maßnahmen wie zum Beispiel Anordnungsbefugnisse an die Betreiber für konkrete defensive Maßnahmen zu beschränken.

Begründung:

Der Gesetzentwurf enthält weitgehende Eingriffsbefugnisse für die Bundespolizei und das BKA. Deren Erforderlichkeit sollte geprüft werden. Denn statt eines aktiven Eingreifens sind mildere Maßnahmen wie zum Beispiel das Einräumen von Anordnungsbefugnissen gegenüber den Betreibern zur Vornahme konkreter defensiver Maßnahmen denkbar und womöglich auch zielführender. Diese könnten punktgenau und zielgerichtet angewendet werden und ebenfalls die schnelle Ausschaltung eines Sicherheitsrisikos bewirken. Dieses Vorgehen ist effektiv, ohne die Integrität der Netze unnötig zu gefährden. Bei aktiven Maßnahmen wird die Sicherheitslücke hingegen unnötig lange offengehalten und sorgt damit für eine weitere Gefährdung. Die vorgesehenen offensiven Maßnahmen sind zudem mit erheblichen Risiken behaftet. Es ist üblich, dass Angreifer bei der Durchführung von Cyberattacken Zwischensysteme nutzen oder fremde Domains kapern. Durch IP-Adressen und Netzwerkmerkmale kann lediglich das Zwischensystem identifiziert werden, von dem der Angriff ausgeht, nicht aber der tatsächliche Angreifer. Es besteht daher die Gefahr, dass nur gekaperte Drittsysteme getroffen werden. Dies führt zu erheblichen Kollateralschäden. Ein besonderes Gefahrenpotenzial ergibt sich ferner, wenn die Betroffenen nicht über die Maßnahmen in Kenntnis gesetzt werden. Maßgebliche Informationen über die Systeme liegen typischerweise nur bei den betroffenen Betreibern vor, sodass verdeckte Eingriffe ohne deren Wissen kaum verlässlich durchführbar sind. Gerade bei Eingriffen in die Systeme von Betreibern kritischer Infrastruktur drohen erhebliche Risiken, von Betriebsstörungen bis hin zu Versorgungsausfällen. Mit unverhältnismäßigem Overblocking ist ebenfalls zu rechnen, da die Maßnahmen meist nicht auf einzelne Inhalte begrenzt werden und daher auch rechtmäßige Inhalte betreffen können.

Darüber hinaus stellt sich die Frage nach der Vereinbarkeit der geplanten Maßnahmen mit deutschen und europäischen Grundrechten, wenn eine Information der Betroffenen dauerhaft unterbleibt, da so kaum eine gerichtliche Rechtmäßigkeitskontrolle stattfinden kann, und eine Rückgängigmachung durch die Behörden nur dann vorzunehmen ist, soweit dies technisch möglich ist und dem Zweck der Maßnahme nicht entgegensteht.

Wi 4. Zu Artikel 1 Nummer 2 (§ 41a Absatz 6 Satz 1 BPolG)

In Artikel 1 Nummer 2 § 41a Absatz 6 Satz 1 ist die Angabe „in Verbindung mit Absatz 5“ zu streichen.

Begründung:

Es gibt keine hinreichende Begründung, warum Maßnahmen nach § 41a Absatz 1 Satz 1 Nummer 3 BPolG-E nur bei Eingriff in private informationstechnische Systeme einer 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 den 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. Besondere Abwehrmaßnahmen nach § 41a Absatz 1 Satz 1 Nummer 3 BPolG-E sollten daher generell, unabhängig von der Nutzungsart des betroffenen Systems, einer richterlichen Anordnung bedürfen.

Wi 5. Zu Artikel 1 Nummer 2 (§ 41a Absatz 9 BPolG), Artikel 3 Nummer 9 (§ 68c Absatz 2 BKAG)

Der Bundesrat bittet, die nach § 41a Absatz 9 BPolG-E und § 68c Absatz 2 BKAG-E vorgesehenen Mitwirkungspflichten der nach dem Telekommunikationsgesetz Verpflichteten sowie von Anbietern nach dem Digitale-Dienste-Gesetz zu konkretisieren und auf klar begrenzte, technisch umsetzbare und defensive Unterstützungsleistungen zu beschränken.

Begründung:

Die vorgesehenen Mitwirkungspflichten begegnen erheblichen Unsicherheiten hinsichtlich Umfang, Frist und technischer Umsetzung. So sollte der Begriff der „unverzüglichen“ Mitwirkung konkretisiert werden. Zudem ist unklar, wel-

che konkreten Handlungen von den Unternehmen erwartet werden. Mitwirkungspflichten sind präzise und technisch umsetzbar zu regeln, zumal Verstöße dagegen mit Geldbuße bis zu fünfhunderttausend Euro geahndet werden können. Darüber hinaus sollte klargestellt werden, dass sich die Verpflichtung von Unternehmen zur Unterstützung nicht auf offensive Eingriffsbefugnisse erstreckt. Solche Maßnahmen dürfen – wenn überhaupt – nur von staatlichen Stellen unter klar definierten Voraussetzungen durchgeführt werden.

Wi 6. 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.

Wi 7. Zu Artikel 2 Nummer 7 (§ 16a Absatz 1 Satz 2 BSIG)

Artikel 2 Nummer 7 § 16a Absatz 1 Satz 2 ist zu streichen.

Begründung:

Die dem BSI eingeräumte Befugnis, anzuordnen, dass Nameserver-Einträge eines vom BSI benannten Domain-Namens geändert oder neue Einträge hinzufügt werden müssen, stellt einen erheblichen Eingriff mit einschneidenden Auswirkungen sowohl auf Anbieter als auch Nutzer dar, der typischerweise nicht nur einzelne Inhalte, sondern die Erreichbarkeit ganzer Domains betreffen kann. Eine faktische Korrektur möglicher Fehlentscheidungen verursacht

erheblichen Aufwand. In Anbetracht dieser Risiken sollte an dem gesetzlichen Regelfall nach § 80 Absatz 1 VwGO, dass Widerspruch und Anfechtungsklage aufschiebende Wirkung haben, festgehalten werden, zumal es dem BSI wie jeder anderen Behörde zumutbar ist, zu prüfen, ob die Voraussetzungen für eine Anordnung der sofortigen Vollziehbarkeit seiner Maßnahmen nach § 80 Absatz 2 Satz 1 Nummer 4 VwGO vorliegen, und dies dann auch umzusetzen. Es bedarf jedoch einer schnellen und effektiven gerichtlichen Überprüfbarkeit. Nur so lassen sich unverhältnismäßige Eingriffe, unverhältnismäßige Belastungen für Unternehmen sowie nicht abschätzbare Auswirkungen auf Dienste, Nutzervertrauen und internationale Datenflüsse vermeiden.

Wi 8. 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.

R 9. 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 gericht-

lichen 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.

B

10. Der federführende **Ausschuss für Innere Angelegenheiten** und

der **Ausschuss für Digitales und Staatsmodernisierung**

empfehlen dem Bundesrat, gegen den Gesetzentwurf gemäß Artikel 76 Absatz 2 des Grundgesetzes keine Einwendungen zu erheben.