BREKO Bundesverband
Breitbandkommunikation e.V.

BREKO | Invalidenstraße 91 | 10115 Berlin

Per Mail: NIS2@bmi.bund.de
Bundesministerium des Innern und für Heimat
Referat CI 1
11014 Berlin

BREKO Bundesverband
Breitbandkommunikation e.V.
Invalidenstraße 91
10115 Berlin

Tel.: +49 30 58580 418
kind@brekoverband.de

27. Mai 2024

Stellungnahme zum Referentenentwurf des BMI für ein Gesetz zur Umsetzung der NIS-2-Richtlinie (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG)

Sehr geehrte Damen und Herren,

das Bundesministerium des Inneren und für Heimat (BMI) hat am 07.05.2024 einen „Referentenentwurf zur Umsetzung der NIS-2-Richtlinie“ in Deutschland zur Kommentierung versandt. Wir begrüßen sehr, dass das BMI den Dialog sucht und bedanken uns als Verband für die Möglichkeit zur Abgabe einer Stellungnahme.

Zusammenfassung der wichtigsten Punkte:

II. 2. c) Bereichsausnahme für § 30 BSIG-E

Aufgrund des Konkurrenzverhältnisses mit dem Sicherheitskatalogs der BNetzA nach § 167 TKG, ist die **Bereichsausnahme der Telekommunikationswirtschaft für den § 30 BSIG-E im Rahmen des § 28 Abs. IV BSIG-E erneut aufzunehmen**. Spätestens mit der Übertragung des Inhalts von § 30 Abs. II BSIG-E in einen neuen § 165 Abs. IIa TKG im Rahmen des Art. 23 des Referentenentwurfs ist die Bereichsausnahme zur Vermeidung einer Doppelregulierung dringend geboten.

II.3. Ausnahmeregelung, § 28 Abs. IX BSIG-E

Es scheint zielführender die Verpflichtungen möglichst einheitlich zu halten und einen großen Flickenteppich an Normen zu vermeiden. Diese Ausnahmeregelung verfehlt hier den Zweck der Entlastung der betroffenen IT-Dienstleister. Darüber hinaus ist **§ 28 Abs. IX BSIG-E unbestimmt und sollte daher gestrichen werden**.

III. Geschäftsführerhaftung, § 38 BSIG-E

Die Geschäftsleitung wird durch § 38 BSIG-E einem außerordentlich hohem und nicht verhältnismäßigen Risiko ausgesetzt. Wir regen daher an, **§ 38 Abs. II BSIG-E zu streichen**. Zumindest sollte aber auf Gesetzesebene (nicht nur in der Gesetzesbegründung) klargestellt werden, dass die Inanspruchnahme einer entsprechenden Versicherung (D&O-Versicherung) zur Absicherung der Geschäftsleitung durch § 38 Abs. II BSIG-E nicht ausgeschlossen werden soll.

IV. Einsatz kritischer Komponenten, § 41 BSIG-E

Die Ausweitung der bereits nach dem TKG für 5G-Netze bestehenden Verpflichtungen auf Betreiber aller kritsichen Anlagen hält der BREKO für unangemessen und unverhältnismäßig. Die Regelung des § 41 BSIG-E sollte in die **Bereichsausnahme des § 28 Abs. IV BSIG-E aufgenommen** und damit der BNetzA überlassen werden, welche Netze sie als „Netze mit erhöhter Kritikalität“ einstuft und den Verpflichtungen im Anlage 2 des Anforerungskataloges unterwirft. Alternativ sollte **§ 41 BSIG-E mit vergleichbaren Anforderungen an den möglichen Adressatenkreis versehen werden, wie es in Ziffer 5.1.3 des Anforderungskataloges der BNetzA geschieht**.

V. Übergangsregelung, Art. 29 des Referentenentwurfs

Angesichts der Tatsache, dass die Verpflichtungen aus dem neuem BSIG durch die erhebliche Ausweitung des Adressatenkreises viele - und gerade kleinere - Unternehmen mit überschaubaren Ressourcen erstmals trifft, bedarf es einer angemessenen Übergangszeit. Erst nach Ende des Gesetzgebungsverfahrens können Unternehmen mit der gezielten Planung der geforderten Sicherheitsmaßnahmen beginnen. Vor diesem Hintergrund halten wir einen **Umsetzungszeitraum von mindestens 12 Monaten nach Inkrafttreten des vollständigen Regelungswerks, einschließlich der Verordnung nach § 58 BSIG-E**, für erforderlich.

Inhaltliche Ausführung:

I. Einleitung

Der im Jahr 1999 gegründete Bundesverband Breitbandkomunikation (BREKO e.V.) vertritt die Interessen von knapp 480 Mitgliedsunternehmen, darunter über 240 Netzbetreibern, die vor allem lokal und regional echte Glasfasernetze (FttB/H) ausbauen. Dafür investieren die Mitgliedsunternehmen des BREKO in jedem Jahr weit über 3 Mrd. Euro.

Für die BREKO-Mitgliedsunternehmen haben die Netz- und IT-Sicherheit ebenso wie die Sicherheit der Daten ihrer Kunden einen hohen Stellenwert. Den im BREKO organiserten Netzbetreibern und Diensteanbietern ist bewusst, dass die IT- und Datensicherheit ein ganz wesentliches Qualitätsmerkmal iher hochwertigen glasfaserbasierten Produkte ist. Entsprechend ernst nehmen die Unternehmen die gesetzlichen Anforderungen.

Dies vorausgeschickt kommentieren wir den vom BMI veröffentlichten Referentenentwurf wie folgt.

II. Vermeidung einer Doppelregulierung

1. Erhebliche Ausdehnung des Adressatenkreises

Durch die NIS-2-Richtlinie und ihre Umsetzung wird der Adressatenkreis des BSI-Gesetzes erheblich erweitert und ist nicht mehr auf die klassischen KRITIS-Betreiber beschränkt. Neben den „Betreibern kritischer Anlagen“ sind – in abgestufter Intensität – nunmehr auch *„besonders wichtige Einrichtungen“* (in der Terminologie der Richtlinie „wesentliche Einrichtungen“) und *„wichtige Einrichtungen“* zur Einhaltung bestimmter Sicherheitsstandards und der Umsetzung der entsprechenden Maßnahmen verpflichtet. Dabei wird der Telekommunikationssektor sehr weitgehend den „besonders wichtigen Einrichtungen“ zugeordnet. Bereits ab 50 Mitarbeitenden bzw. einem Jahresumsatz bzw. einer Jahresbilanzsumme ab € 10 Mio. gelten Telekommunikationsnetzbetreiber und Telekommmunikationsdiensteanbieter als *„besonders wichtige Einrichtungen“* mit den entsprechenden gesetzlichen Verpflichtungen. Telekommunikationsnetzbetreiber und -Dienstanbieter unterhalb dieser Schwellwerte sind als Angehörige eines *„Sektors mit hoher Kritikalität“* (Anlage1, Ziffer 6) den für *„wichtige Einrichtungen“* geltenden Verpflichtungen unterworfen. Die Telekommunikationswirtschaft ist damit praktisch vollständig – und zum großen Teil erstmals – im Zuge der NIS-2-Umsetzung durch das im Zuge der Richtlinienumsetzung zur Neufassung anstehende BSI-Gesetz betroffen.

Die sich hieraus ergebenden Verpflichtungen können gerade von kleineren Telekommunikationsunternehmen überhaupt nur dann bewältigt werden, wenn eine Doppelregulierung konsequent vermieden wird. Dies ist im aktuellen Referentenentwurf gerade nicht der Fall. Zudem kann der Umstand, dass viele TK-Netzbetreiber und -Diensteanbieter erstmals durch das BSI-Gesetz verpflichtet werden nicht ohne Rückwirkungen auf die Umsetzungsfristen bleiben.

2. Bereichsausnahmen, § 28 Abs. IV BSIG-E

In § 28 Abs. IV BSIG-E wird die Telekommunikationsbranche teilweise durch Bereichsausnahmen von den Verpflichtungen des BSIG-E befreit.

a) Doppelregulierung

Im Sinne der Rechtssicherheit ist bei jedem Schritt der Regulierung zu beachten, dass für betroffene Unternehmen das Maß und der Umfang ihrer Verpflichtungen klar zu erkennen ist. Es darf daher nicht zu Unsicherheiten durch die Kollision verschiedener regulatorischer Verpflichtungen kommen. Es sollte das Ziel einer jeden Regulierung sein, eine Doppelregulierung zu vermeiden.

Eine Doppelregulierung liegt immer dann vor, wenn ein Betroffener durch zwei verschiedene Normen in gleichem Umfang verpflichtet wird. Unabhängig von einer gänzlichen Übereinstimmung, kann der mit dem Gesetz einer Norm verbundene Umfang, sowie beispielsweise die Rechtfolgen, unterschiedlich sein. Es besteht für einen Betroffenen damit eine Rechtsunsicherheit, aus welcher Norm heraus eine Verpflichtung folgt und mit welchen Umfang diese einhergeht.

Eine solche Doppelregulierung kann nur dadurch verhindert werden, dass der sektorspezifischen Regulierung Vorrang zukommt und die nachgestellte Norm durch eine Bereichausnahme für den bereits sektorspezifisch regulierten Bereich für die Betroffenen ausgenommen wird.

Um eine solche Doppelregulierung zu verhindern, sah das Diskussionspapier von September 2023 in § 28 Abs.IV Nr.1 BSIG-E weitgehende Bereichsausnahmen für die Telekommunikationswirtschaft vor. Danach sollten *„wichtige Einrichtungen“* und *„besonders wichtige Einrichtungen“* soweit sie ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen von den Verpflichtungen nach §§ 30 und 31 BSIG-E befreit sein.
Im aktuellen Referentenentwurf ist eine solche Bereichsausnahme in § 28 Abs. IV Nr. 1 BSIG-E nun lediglich für die §§ 31, 32, 35 und 39 BSIG-E vorgesehen.

b) Bereichsausnahme für die §§ 31, 32, 35 und 39 BSIG-E

Die Entscheidung eine Bereichsausnahem für diese Normen aufgrund der sektorspezifischen Verpflichtungen aus dem TKG im Bereich der besonderen Anforderungen an die Risikomanagementmaßnahmen sowie Melde-, Unterrichtungs- und Nachweispflichten zu treffen, wird begrüßt.

Die Bereichsausnahme für § 31 BSIG-E betrifft u.a. den Einsatz von Systemen der Angriffserkennung. Diese Bereichsausnahme ist schlüssig, da der Einsatz von Systemen der Angriffserkennung für die Telekommunikationsbranche bereits in § 165 Abs. III TKG geregelt wird.

Bezüglich der Meldepflichten und Unterrichtungspflichten bei Sicherheitsvorfällen nach §§ 32 und 35 TKG ist eine Bereichsausnahme sinnvoll und notwendig, da § 168 TKG bei Vorliegen eines Sicherheitsvorfalls mit beträchtlichen Auswirkungen TK-Netzbetreibern und -Diensteanietern bereits umfangreiche Mitteilungspflichten an die BNetzA und das BSI sowie darüber hianusgehende Unterrichtungspflichten auferlegt und somit ein vergleichbares Schutzniveau schafft. Eine zusätzliche Verpflichtung nach §§ 32 und 35 BSIG-E würde damit zu einer unzulässigen Doppelregulierung führen.

c) Bereichsausnahme für § 30 BSIG-E

Der Grund für eine notwendige Ausweitung der aktuell geplanten Bereichsausnahme für die Telekommunikationswirtschaft liegt in den erheblichen Überschneidungen des Sicherheitskatalogs der BNetzA mit den Verpflichtungen aus dem aktuellen § 30 BSIG-E. Betroffene Unternehmen müssen bei der Erstellung ihres Sicherheitskonzepts die Anforderungen des **Pflichtenkatalogs nach § 165 TKG** in Verbindung mit dem **Sicherheitskatalog der BNetzA nach § 167 TKG** beachten, wodurch ein adäquat hohes Schutzniveau sichergestellt ist. Hier gilt der Vorrang der spezielleren sektorspezifischen Regulierung.
Die entsprechenden Überschneidungen wurden im Rahmen des vorherigen Diskussionspapier von September 2023 erkannt und dem durch eine entsprechende Bereichsausnahmen Rechnung getragen. Der BREKO hält das **Widereinfügen einer Bereichsausnahme für die Telekommunikationswirtschaft für den § 30 BSIG-E für unausweichlich** um eine Doppelregulierung zu vermeiden.

Bei der Gegenübersteltung des Sicherheitskatalogs der BNetzA mit den Verpflichtungen aus dem aktuellen BSIG-E ergibt sich eine erhebliche Überschneidung an Verpflichtungen.
So beinhaltet der Sicherheitskatalog bereits Regelungen zu den Themen:

- Durchführung einer Risikoanalyse (§ 30 II Nr. 1 BSIG-E vs. Pkt. 5.1.3-5 und 7 Sicherheitskatalog)
- Umgang mit Sicherheitsvorfällen (§ 30 II Nr. 2 BSIG-E vs. Pkt. 3.5 Sicherheitskatalog)

- Handeln während und nach einem Sicherheitsvorfall (§ 30 II Nr. 3 BSIG-E vs. Pkt. 3.6 Sicherheitskatalog)
- Sicherheit des Lieferantenmanagements (§ 30 II Nr. 4 BSIG-E vs. Pkt. 3.1.3 Sicherheitskatalog, Pkt. 3 Anlage 2 Sicherheitskatalog)
- Bewertung der Wirksamkeit der Risikomanagementmaßnahmen (§ 30 II Nr. 6 BSIG-E vs. Pkt. 3.7, 3.8 Sicherheitskatalog)
- Schulung des Personals (§ 30 II Nr. 7 BSIG-E vs. Pkt. 3.2 Sicherheitskatalog, Pkt. 6 Anlage 2 Sicherheitskatalog)
- Verschlüsselungstechnologien (§ 30 II Nr. 8 BSIG-E vs. Pkt. 2.1.1, 3.3.1, 3.3.6 Sicherheitskatalog, Pkt. 5.2 Anlage 2 Sicherheitskatalog)
- Physische Sicherheit der Anlagen (§ 30 II Nr. 9 BSIG-E vs. Pkt. 3.3 Sicherheitskatalog)
- Vertraulichkeit der Kommunikation (§ 30 II Nr. 10 BSIG-E vs. Pkt. 3.3.6 Sicherheitskatalog, 3.1 Anlage 1 Sicherheitskatalog)

All diese Verpflichtungen werden in ähnlichem Umfang in dem Sicherheitskatalog der BNetzA aufgeführt (siehe Verweise).

Eine Rechtfertigung, weshalb sich diese Verpflichtungen voneinander in dem Maße unterscheiden sollten, dass in diesem Fall keine Doppelregulierung vorliegt, ist nicht ersichtlich. Der Sicherheitskatalog der BNetzA umfasst einen erheblichen Umfang an Vorgaben und regelt bereits auf sektorspezifischer Ebene die von § 30 Abs. II BSIG-E geforderten Maßnahmen.

Die bereits durch das Nebeneinander von § 30 Abs. II BSIG-E und dem Sicherheitskatalog der BNetzA erzeugte Doppelregulierung wird spätestens durch **Art. 23 des Referentenentwurfs** noch einmal verstärkt. Durch diesen wird der Maßnahmenkatalog aus § 30 Abs. II BSIG-E vollständig in § 165 Abs. IIa TKG-E übernommen. Die in § 30 Abs. II BSIG-E für die Unternehmen festgelegten Verpflichtungen werden damit komplett in § 165 Abs. IIa TKG gespiegelt.

Nur eine Bereichsausnahme zumindest für § 30 Abs. II BSIG-E der Telekommunikationswirtschaft kann eine Rechtsunsicherheit der betroffenen Unternehmen und damit eine Doppelregulierung verhindern.

Darüber hinaus ist darauf hinzuweisen, dass durch die Einführung des § 165 Abs. IIa TKG die oben aufgeführte „Dopplung“ der Verpflichtungen, im Vergleich zum Sicherheitskatalog der BNetzA, nun innerhalb des TKG vorliegen würde. Um die Rechtssicherheit der Betroffenen zu wahren, wäre auch hier die Klärung des Verhältnisses zwischen den Verpflichtungen des § 165 Abs. IIa TKG und dem Sicherheitskatalog der BNetzA sinnvoll.
Systemkonform wäre es, die Vorgaben zur Umsetzung der im TKG enthaltenden Regelungen nicht im TKG selbst, sondern in einer zentrale Übersicht, wie dem Sicherheitskatalog der BNetzA, zu implimentieren. Diese Vorgehensweise scheint auch aus verfahrensökonomischer Sicht sinnvoll, da die Änderung bzw. Ergänzung eines Gesetzes erheblich mehr Zeit in Anspruch nimmt und ein weitreichenderes Verfahren bedarf, als die Anpassung bzw. Ergänzung einer zentralen Übersicht. Gerade vor dem Hintergrund der schnellen Weiterentwicklung des Themas Cybersicherheit und den damit einhergehenden sich schnell verändernden Anforderungen an den Stand der Technik von Sicherheitskonzepten, erscheint eine solche Lösung vorzugswürdig.

3. Ausnahmeregelung, § 28 Abs. IX BSIG-E

Mit § 28 Abs. IX BSIG-E des Referentenentwurfs wird eine Ausnahmeregelung für Unternehmen geschaffen, die im Eigentum einer Gebietskörperschaft stehen und bereits durch Landesrecht reguliert werden.

Fraglich ist hierbei zu nächst, was mit „im (…)unmittelbaren Eigentum von Gebietskörperschaften“ stehend gemeint sein soll. Da das „unmittelbare“ Eigentum innerhalb des Sachenrechts nicht vorgesehen ist, wird um Klärung und ggf. Anpassung dieser Bezeichnung gebeten. Sollte es sich dabei um Unternehmen handeln, an welchen entsprechende Gebietskörperschaften Beteiligungsstrukturen inne haben, so würde eine dahingehend klarere Bezeichnung auftretende Verwirrungen vermeiden.

Fraglich ist grundsätzlich, welche Unternehmen von der Regelung umfasst sind. Gerade im Bereich der Stadtwerke würden mit diesen verbundene Tochterunternehmen als IT-Dienstleistern, jeweils nach unterschiedlichen Rechtsgrundlagen (BSIG-E vs. Länderregeln) verpflichtet. Dies würde bei der Zusammenarbeit der einzelnen Instanzen und insbesondere bei Dienstleistungen des IT-

Dienstleisters für die Stadtwerke, zu erheblichen Unterschieden und damit vermeidbaren Hürden führen.

Es scheint zielführender die Verpflichtungen möglichst einheitlich zu halten und einen großen Flickenteppich an Normen zu vermeiden. Diese Ausnahmeregelung verfehlt damit ihren Zweck, die IT-Dienstleister eines solchen Falls zu entlasten und sollte daher gestrichen werden.

III. Geschäftsführerhaftung, § 38 BSIG-E

Der Referentenentwurf sieht in § 38 BSIG-E eine umfangreiche Haftung der Geschäftsleiter *„besonders wichtiger Einrichtungen“* und „*wichtiger Einrichtungen“* im Hinblick auf die Umsetzung und Überwachung der gebotenen Risikomanagementmaßnahmen vor. Die Verantwortlichkeit kann weder horizontal z.B. im Vorstand, noch vertikal auf einzelne Mitarbeitende komplett abdelegiert werden. Darüber hinaus besteht eine Verpflichtung der Geschäftsleiter zur Teilnahme an Schulungen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung von Risiken sowie Risikomanagementmaßnahmen im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.

Über diese bereits strengen Anforderungen aus Art. 20 der NIS-2-Richtlinie hinaus, sieht die geplante nationale Regelung in § 38 BSIG-E vor, dass ein Verzicht der Einrichtung auf Ersatzansprüche gegen die Geschäftsleitung oder ein in einem groben Missverhältnis zu einer bestehenden Ungewissheit über das Rechtsverhältnis stehender Vergleich der Einrichtung aufgrund einer Pflichtverletzung der Umsetzungs- und Überwachungspflicht zu Risikomanagementmaßnahmen oder ein Vergleich unwirksam sein sollen. Dies gilt jedenfalls bis zur Grenze der Abwendung eines Insolvenzverfahrens des Ersatzpflichtigen.

Der BREKO hält diese durch die umzusetzende Richtlinie nicht vorgebene Haftungsverschärfung für nicht angemessen. Die Geschäftsleitung würde dadurch einem **außerordentlich hohem und nicht verhältnismäßigen Risiko** ausgesetzt. Die strenge Haftungsregelung in Art.20 der NIS-2-Richtlinie ist unseres Erachtens vollkommen ausreichend, um den hohen Stellenwert der Cybersicherheitsanforderungen auch gegenüber der Geschäftsleitung abzusichern. Dazu kommt die intrinsische Motivation, den Kundinnen und Kunden auch in Bezug auf die IT- und Datensicherheit ein hochqualitatives Produkt anzubieten.

Wir regen daher an, **§ 38 Abs. II BSIG-E zu streichen**.

Zumindest sollte aber auch auf Gesetzesebene (nicht lediglich in der Gesetzesbegründung) klargestellt werden, dass die Inanspruchnahme einer entsprechenden Versicherung (D&O-Versicherung) zur Absicherung der Geschäftsleitung durch § 38 Abs. II BSIG-E nicht ausgeschlossen werden soll. Zur Gewährleistung der Rechtssicherheit und Planungssicherheit für die Geschäftsleitung, wäre eine Klarstellung zur Versicherbarkeit dieser Haftungsverpflichtung auf Gesetzesebene sinnvoll, um auch im Versicherungsfall eine klare und wirkungsvolle Einordnung des Gesetzgebers als Argument gegenüber den Versicherern zu haben. Insbesonder vor dem Hintergrund, dass eine entsprechend weitreichende Haftung der Geschäftsleitung von der Richtlinie nicht gefordert wird, ist die Versicherbarkeit dieser Haftungserweiterung des BSIG-E geboten.

IV. Einsatz kritischer Komponenten, § 41 BSIG-E

Nach der Regelung in § 41 BSIG-E muss der Betreiber einer kritischen Anlage den Einsatz kritischer Komponenten gegenüber dem BMI anzeigen und eine Garantieerklärung des Herstellers beibringen. In der Folge kann das BMI den Einsatz von geplanten oder bereits in Betrieb befindlichen Komponenten untersagen. Wesentlicher Anknüpfungspunkt ist dabei die Garantiererklärung.

Die Untersagung des Einsatzes einer kritischen Komponente – insbesondere, wenn diese bereits in Betrieb genommen worden ist – stellt einen erheblichen Eingriff in das Eigentum der Unternehmen dar und erhöht deren Investitionsrisiko erheblich. Eine Ausweitung dieser sehr weitgehenden Rechtsfolgen auf alle Betreiber einer kritsichen Anlage hält der BREKO für unangemessen und unverhältnismäßig. Im Telekommunikationssektor findet sich eine entsprechende Verpflichtung in Anlage 2 zum Katalog von Sicherheitanforderungen ausschließlich für Netze mit „erhöhter Kritikalität“.

Zur Einstufung als TK-Netz mit erhöhter Kritikalität finden sich in Ziffer 5.1.3 des BNetzA-Anforderungskatalog verschiedene Kriterien:

Neben der Teilnehmerzahl sind dies die besondere Bedeutung des Netzes für das Gemeinwohl z.B. durch die „querschnittliche Verwendiung in allen Bereichen des öffentlichen Lebens“, wodurch die

„Verfügbarkeit des Netzes mit hoher Wahrscheinlichkeit nicht nur den Einzelnen, sondern auch Staat, Wirtschaft und die Gesellschaft gleichermaßen“ betrifft (S.37 Anforderungskatalog).

Diese überragende Funktion für das Gemeinwohl sieht die BNetzA im Anforderungskatalog nicht einmal beim flächendeckenden Festnetz der Telekom Deutschland als gegeben an, sondern nur bei den Betreibern von 5G-Netzen:

„Eine enorme Sonderstellung kommt dem Betrieb von 5G-Netzen im Sinne der EUEmpfehlung 2019/534 vom 26. März 2019 zu. 5G-Netze sind in diesem Sinn das künftige Rückgrat unserer zunehmend digitalisierten Volkswirtschaften und Gesellschaften. Sie werden Milliarden von Objekten und Systemen mit einander und auch in den Kritischen Infrastrukturen der Sektoren Energie, Wasser, Ernährung, Gesundheit, Finanz- und Versicherungswesen, Transport und Verkehr sowie dem Sektor Informationstechnik und Telekommunikation sensible Informationen verarbeiten und Sicherheitssysteme unterstützen. Werden daher öffentlich zugängliche 5G- Mobilfunknetze mit einer Teilnehmerzahl von mehr als 100.000 Teilnehmern betrieben, so kann eine herausragende Bedeutung dieser Telekommunikationsnetze für das Gemeinwohl indiziert sein.“(Anforderungskatalog S.37)

Mit Blick auf die erheblichen Eingriffe, die Anlage 2 des Sicherheitskataloges gegenüber den Betreibern von Netzen mit erhöhter Kritikalität ermöglicht, formuliert die BNetzA also restriktive Kriterien für die entsprechende Einstufung der Netze. An einer entsprechenden Beschränkung des Adressatenkreises mit Blick auf die überragende Bedeutung des Netzes für das Gemeinwohl, die die Regelung überhaupt erst verhältnismäßig machen würde, fehlt es aber in § 41 BSIG-E. Es wäre aber nicht verhältnismäßig die Kritikalität z.B. eines regional begrenzten Glasfasernetzes mit vielleicht gerade 100.000 Teilnehmern (Schwellenwert) mit einem 5G-Netz mit vielen Millionen Teilnehmern und einer viel stärkeren Querschnittsfunktion gleichzusetzen und die Betreiber gleich tiefen Eingriffen zu unterwerfen.

Wir fordern das BMI daher auf, die Regelung des § 41 BSIG-E entweder in die Bereichsausnahme des § 28 Abs. IV BSIG-E aufzunehmen und damit der BNetzA zu überlassen, welche Netze sie als „Netze mit erhöhter Kritikalität“ einstuft und den Verpflichtungen im Anlage 2 des Anforerungskataloges unterwirft oder § 41 BSIG-E mit vergleichbaren Anforderungen an den möglichen Adressatenkreis zu versehen, wie es in Ziffer 5.1.3 des Anforderungskataloges der BNetzA geschieht.

Die Regelung ist jedenfalls unter Verhältnismäßigkeitsgesichtspunkten in ihrem Anwendungsbereich erheblichzu begrenzen.

V. Übergangsregelung, Art. 29 des Referentenentwurfs

Artikel 29 des Referentenentwurfs sieht ein Inkrafttreten des neuen BSIG zum 01.10.2024 vor. Im Rahmen des vorherigen Diskussionspapier von September 2023 wurde in der Begründung zu Artikel 29 dazu ausgeführt, dass bei einem erwarteten Abschluss des Gesetzgebungsverfahrens im März 2024 den Unternehmen noch 6 Monate zur Verfügung stünden, um die notwenigen Maßnahmen zur Umetzung zu treffen.

Diesen zeitlichen Rahmen hat der BREKO in seiner Stellungnahme vorherigen Diskussionspapier von September 2023 angezweifelt. Ein Umsetzungszeitraum von 6 Monaten ist bereits grundlegend erheblich zu kurz, angesichts der Tatsache, dass die Verpflichtungen aus dem neuem BSIG durch die erhebliche Ausweitung des Adressatenkreises viele - und gerade kleinere - Unternehmen mit überschaubaren Ressourcen erstmals trifft.

Zwar ist es richtig, dass einige von den Bereichsausnahmen umfassten Verpflichtungen durch das TKG vorgegeben und bereits seit Längerem umgesetzt sind. Der BSIG-E enthält aber auch eine Reihe darüber hinausgehender Verpflichtungen, die von den Unternehmen umgesetzt werden müssen. Erschwerend hinzu kommt, dass erst mit der nach § 58 BSIG-E ebenfalls zu erlassenden Verordnung hinreichend sicher klargestellt ist, welchem Adressatenkreis das betreffende Unternehmen zuzuordnen ist und welche Verpflichtungen genau umzusetzen sind.

Eine ausbleibende oder „zu kurze“ Übergangszeit führt dazu, dass eine pünktliche Umsetzung der Verpflichtungen – insbesondere für kleinere – Unternehmen zum maßgeblichen Zeitraum kaum zu möglich ist. Dabei ist es keine Unterstützung, dass die Umsetzung der Verpflichtungen erst zu einem späteren Zeitpunkt von der zuständigen Stelle kontrolliert wird. Vielmehr besteht für die Unternehmen in der Zeit **zwischen in Kraft treten des Gesetzes und der tatsächlich erfolgten Umsetzung ihrer Verpflichtungen ein erhebliches Haftungsrisiko im Schadensfall**, insbesondere vor dem Hintergrund der verschärften Geschäftsführerhaftung nach § 38 BSIG-E. Die aufgeschobene Kontrolle der zuständigen Stelle führt nicht zu einer „Haftungssperre“ für die Unternehmen, sollten sie bei einem Schadensfall die Maßnahmen zu denen Sie laut BSIG-E verpflichtet sind, noch nicht umgesetzt haben.

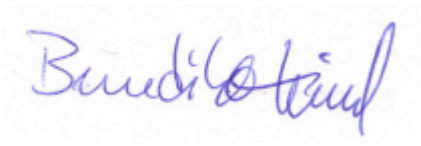
Faktisch müsste ein Unternehmen bereits jetzt und damit vor dem Beschluss eines konkreten Gesetzentwurfs, die entsprechenden Verpflichtungen umsetzen, um sich rechtlich abzusichern. Dies jedoch ohne von dem konkreten Umfang der Betroffenheit sowie der konkreten Ausgestaltung der Verpflichtungen Kenntnis erlangt zu haben. Das dabei ein enormes finanzielles Risiko und ein hohes Maß an Planungsunsicherheit besteht zeigt beispielsweise die erfolgte Änderung der Bereichausnahme zum § 30 BSIG-E für die Telekommunikationswirtschaft. Es ist den Unternehmen daher faktisch nicht möglich nachhaltig und effizient die Verpflichtungen umzusetzen, solange das Gesetzgebungsverfahren nicht abgeschlossen ist. Erst ab diesem Zeitpunkt können Unternehmen mit der gezielten Planung der geforderten Sicherheitsmaßnahmen beginnen.

In unserer ersten Stellungnahme haben wir bereits Zweifel daran geäußert, dass das Gesetzgebungsverfahren bereits im März 2024 abgeschlossen sein könnte. Nun wurde im Mai 2024 der Referentenentwurf veröffentlicht, wobei eine entsprechende Verbändeanhörung erst Anfang Juni 2024 stattfindet. Insbesondere mit Blick auf die künftigen Sommerpausen scheint ein Abschluss des Gesetzgebungsverfahrens weit vor, beziehungsweise zum geplanten Zeitpunkt Oktober 2024 zweifelhaft. Damit würde für die betroffenen Unternehmen eine konkrete Umsetzung der Verpflichtungen erst unmittelbar vor in Kraft treten des Gesetzes beginnen können.

Vor diesem Hintergrund halten wir einen **Umsetzungszeitraum von mindestens 12 Monaten** nach Inkrafttreten des vollständigen Regelungswerks, einschließlich der Verordnung nach § 58 BSIG-E, für erforderlich.

Wir freuen uns auf eine vertiefte Erlörterung im Rahmen der vom BMI angebotenen Verbändeanhörung am 03.06.2024, stehen für Rückfragen aber auch gerne schon vorher zur Verfügung.

Mit freundlichen Grüßen



Benedikt Kind
Leiter Recht & Grundsatzfragen Regulierung

Lisa Müller
Referentin für Recht & Regulierung