BUGLAS
Bundesverband Glasfaseranschluss e.V.

Stellungnahme zum

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung

Berlin, 04. Juli 2025

Bundesverband Glasfaseranschluss e.V. | Geschäftsstelle | Eduard-Pflüger-Str. 58 | 53113 Bonn
Ansprechpartner: Nicolas Goß | Leiter Recht und Regulierung | goss@buglas.de

Vorbemerkung

Wir bedanken uns für die Möglichkeit zur Kommentierung des Gesetzes-Entwurfs (mit Stand vom 23.06.2025, 17:12Uhr).

Diese Stellungnahme enthält **keine Betriebs- und Geschäftsgeheimnisse.**

Der BUGLAS und seine Mitgliedsunternehmen setzen sich sehr für die Stärkung der Cybersicherheit ein. Unsere Mitglieder haben ein intrinsisches Interesse, ihre Netz-Dienste für die Kunden höchstzuverlässig und integer erbringen zu wollen. Außerdem wissen unsere Mitglieder um ihre gesellschaftliche Verantwortung in einer zunehmend vernetzten und digitalisierten Welt.

Der BUGLAS stellt einige Verbesserungen an diesem Entwurf gegenüber dem letzten Regierungs-Entwurf fest. Diese begrüßt der BUGLAS.

Der BUGLAS unterstützt das Ziel des Gesetzes, die Cybersicherheit zu erhöhen. Nach unserer Auffassung müssen Sicherheitsvorgaben und Maßnahmen faktisch umsetzbar sein, um ihren Zweck zu erfüllen. Anforderungen, die sowohl technischen als auch organisatorischen Aufwand (vor allem personell) nach sich ziehen, führen für KMU zu einer erheblichen Belastung. Deswegen ist hinsichtlich der KMU ein erhöhter Differenzierungsgrad bei den konkreten Umsetzungsmaßnahmen geboten und Rücksicht auf die Leistungsfähigkeit von KMU zu nehmen. Dies kann durch Bagatellgrenzen, Schwellenwerte oder mittels geeigneter Alternativen zur Umsetzung von Maßnahmen erfolgen.

Grundsätzlich hält der BUGLAS an der Position fest, dass die Resilienz von (digitalen) KRITIS eine gesamtgesellschaftliche Aufgabe darstellt und der Bund in der Verantwortung ist, hier entsprechenden Aufwendungsersatz zu leisten.

Der BUGLAS kritisiert, dass es dem federführenden Bundesministerium des Inneren erneut nicht gelungen ist, einen Gesamt-Entwurf für das gegenständliche NIS2-UmsuCG und das KRITIS-Dachgesetz vorzulegen. Zumindest wäre auch hier wieder eine parallel laufende Verbändeanhörung beider Entwürfe dringend angezeigt gewesen, da beide Gesetze einen engen Sachzusammenhang aufweisen.

Im Einzelnen nehmen wir wie folgt Stellung.

I. Zum BSIG-E – Artikel 1

1. Zu § 16 BSIG-E – Anordnungsbefugnis des BSI für Eingriff in Nutzersysteme und Beseitigung von Schadsoftware

   Der BUGLAS ist weiterhin der Auffassung, dass das BSI von dieser Anordnungsbefugnis i. V. m. § 169 Absätze 6 und 7 TKG nur in engster Abstimmung mit den betroffenen Telekommunikationsunternehmen (TKU) Gebrauch machen sollte. Ohne exakte Koordinierung in engster Absprache drohen erhebliche Schäden an IT-Systemen und womöglich Ausfälle der Interzugangsdienste. Des Weitern könnte die Kommunikation der jeweiligen Kunden im betroffenen Netz massiv eingeschränkt werden. Eine Rückwirkung der seitens des BSI angeordneten Maßnahmen auf das das System des TK-Anbieters sollte so weitgehend wie möglich ausgeschlossen und das Restrisiko dafür so gering wie möglich sein. Der BUGLAS sieht zudem auch keine regulatorische

oder technische Notwendigkeit, entsprechende Anordnungen über das betroffene Unternehmen hinweg zu treffen, ohne diesem vorab Gelegenheit zur Analyse und Stellungnahme zu geben. Die in § 16 genannten Schutzgüter können auch mit Hilfe kurzer Antwortfristen beachtet werden.

Zu bedenken sind auch Entschädigungsansprüche von Verbrauchern gemäß § 58 TKG, welche sich bei Betroffenheit von mehreren Verbrauchern und je nach Dauer des Ausfalls zu erheblichen Summen addieren können. Im Falle, dass das Unternehmen unverschuldet einem einschlägigen Fall nach § 16 BSIG ausgesetzt ist, hat das BSI nach Ansicht des BUGLAS eine entsprechende Bestätigung zu erteilen, sodass sich das Unternehmen gegenüber den Verbrauchern nach § 58 Abs. 3 Satz 1 Hs. 2 TKG exkulpieren und außerdem der vermutlich ohnehin entstehende Imageschaden möglichst geringgehalten werden kann.

2. Zu § 33 BSIG-E – Registrierungspflicht

Der BUGLAS fordert weiter einen Single-Point-of-Contact, was das NIS2-UmsuCG und eine nationale Umsetzung der CER-Richtlinie (zuvor im KRITIS-DachG geplant gewesen) anbelangt. TKU, welche in deren beider Anwendungsbereiche fallen, sollen nicht durch immer mehr Meldepflichten an verschiedene Behörden belastet und nicht nötiger bürokratischer Aufwand vermieden werden. Es ist das Ziel der Bundesregierung, sowohl auf nationaler und europäischen Ebene Bürokratie abzubauen. Deswegen hält der BUGLAS den Ansatz einer gemeinsamen Meldestelle von BSI und einer anderen Behörde grundsätzlich für sinnvoll, soweit und solange gewährleistet, dass die Meldungen

- unkompliziert sind,
- anerkannte digitale Übermittlungsverfahren verwenden,
- datenschutzkonform sind,
- Betriebs- und Geschäftsgeheimnisse wahren,
- eine Ende-zu-Ende-Verschlüsselung nach dem Stand der Technik verwenden und
- kollaborativ bearbeitet werden können.

Die Integrität der Daten muss in der genutzten Cloud oder den lokalen Speichermedien der Behörden durch gleichwertige Schutzmaßnahmen wie bei den TKU gewährleistet sein.

Hinsichtlich der anderen Behörde: Der BUGLAS hat erhebliche Zweifel, ob im Hinblick auf TKU das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) die geeignete Behörde ist. Wir präferieren deutlich, dass an die Stelle des BBK die Bundesnetzagentur rückt. Zudem ist angesichts des Fachkräftemangels und der kaum konkurrenzfähigen Bezahlung auf den relevanten Besoldungsstufen im öffentlichen Dienst die Besetzung der neu zu schaffenden Stellen wenig realistisch.

3. Zu § 41 BSIG-E (aktuell 9b BSIG) – Untersagung kritischer Komponenten

Der BUGLAS gibt zu bedenken, dass der Ausschluss eines Herstellers Abhängigkeit nur scheinbar reduziert. Ein solcher Ausschluss schafft neue Abhängigkeiten, die sich bei Netzbetreibern preislich sehr erheblich auswirken können. Darüber hinaus sinkt auch das Innovationspotenzial bei den verbliebenen Herstellern. Zu beachten ist aus Sicht des BUGLAS auch die Problematik der Lieferketten. Wie während Corona, dem Schiffsunglück im Suez-Kanal oder anderer Krisen deutlich festzustellen war, können Unterbrechungen der Lieferketten gravierende

Folgen nach sich ziehen. Dies gilt nach Einschätzung des BUGLAS für viele Hersteller in den Kerntechnologien.

Die NIS2-Richtlinie und deren nationale Umsetzung sollten das Cybersicherheitsniveau in Deutschland stärken. Das setzt zwingend voraus, dass gegebenenfalls bei einem erzwungenen Austausch von Komponenten genügend Zeit für Interoperabilitätstests verbleibt. Anderenfalls gefährdet ein solcher Austausch die IT- und Betriebssicherheit und schafft schlimmstenfalls Lücken, auf die nicht getestet werden konnte. Das Gegenteil vom grundsätzlichen Ziel dieser Gesetzgebung wäre dann die Folge.

Unabhängig davon ist es dem BUGLAS ein Anliegen, dass sich bei den zuständigen Akteuren das Bewusstsein für das Maßgebliche beim Thema „Cybersicherheit“ weiterentwickelt. Schließlich stellen sich Haftungsfragen, umso mehr, wenn die gesetzliche Grundlage einen prognostischen Anteil enthält.

4. Zu § 56 BSIG-E – Gesetzliche Grundlage für Rechtsverordnung

Der BUGLAS merkt an, dass in der Norm nach § 56 BSIG-E in keinem Absatz das neugeschaffene Bundesministerium für Digitales und Staatsmodernisierung genannt (BMDS) wird. Danach wäre das vorgenannte Ressort bei der Erarbeitung der Rechtsverordnungen auf Grundlage des § 56 BSIG-E ausgeschlossen. Wir gehen davon aus, dass es sich bei der entsprechenden Formulierung um einen redaktionellen Fehler handelt.

Sollte es sich hingegen nicht um einen Fehler handeln, muss nach Auffassung des BUGLAS das BMDS dringend mitwirkungsbefugt sein. Denn bei den festzulegenden IT-Sicherheitsvorgaben, Cybersicherheitszertifizierung, Festlegung des Versorgungsgrades bzgl. kritischer Dienstleistungen sowie erheblicher Sicherheitsvorfälle (in unserem Sektor) sind sachliche Zuständigkeiten des BMDS in erheblichem Umfang berührt.

Hinzu kommt, dass in vielen Regelungen des BSIG-E auf dessen § 56 und somit auf Rechtsverordnungen verwiesen wird. Hier würde die Nicht-Nennung bzw. das Ausklammern des BMDS abzulehnende Folgewirkungen nach sich ziehen.

II. TKG-E - Artikel 25

1. Zu § 168 Abs. 1 Nr. 1 TKG – Meldung eines Sicherheitsvorfalls

Der BUGLAS ist weiterhin der Auffassung, dass eine Ausnahme von der 24h-Frist erforderlich und geboten ist. Uns ist bewusst, dass der ministerielle Gesetzgeber mit dieser Norm den Art. 23 Abs. 4 NIS2-RL umsetzen will. Diese Regelung der Richtlinie sowie deren deutsche Umsetzung müssen der EU-Grundrechte-Charta Rechnung tragen.

Daran bestehen erhebliche Zweifel im Hinblick auf Art. 52 Abs. 1 S. 2, 1. Hs. der vorgenannten Charta. Dieser fordert die Wahrung der Verhältnismäßigkeit. Bisher sorgte unter anderem das Tatbestandsmerkmal „unverzüglich“ hinsichtlich der Meldung von Sicherheitsvorfällen für Beachtung der Verhältnismäßigkeit. Entsprechend § 121 Abs. 1 S. 1 BGB wird unverzüglich als ohne schuldhaftes Zögern verstanden. Auch im Hinblick auf KMU, deren Personalressourcen und Leistungsfähigkeit gewährleistete dies eine verhältnismäßige Anwendung. Nach § 168 Abs. 1 Nr. 1, 2. Hs. TKG wird nun allerdings eine frühe Erstmeldung eines erheblichen Sicherheitsvorfalls

innerhalb von spätestens 24 Stunden nach Kenntniserlangung verlangt. Der bisher möglichen Auslegung, durch wen eine Meldung ohne schuldhaftes Zögern erfolgt, mit Rücksicht auf Personal und Leistungsfähigkeit, insbesondere bei KMU, steht nun der Wortlaut entgegen. Andere verhältnismäßigkeitswahrende und gleich wirksame Schranken enthalten die weiteren Regelungen des § 168 nicht.

Deshalb regt der BUGLAS folgende Anpassung (rot gedruckt und kursiv) von § 168 Abs. 1 Nr. 1 TKG an:

„…unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, eine frühe Erstmeldung, in der angegeben wird, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte*; abweichend hiervon genügt eine frühe Erstmeldung jedoch spätestens innerhalb von 48 Stunden, wenn die Voraussetzungen nach § 28 Abs. 2 S. 1 Nr. 2 BSI-Gesetzes vorliegen.“*

Eine solche Anpassungspflicht zu Gunsten von KMU ergibt sich nach Auffassung des BUGLAS nicht nur aus der EU-Grundrechte-Charta, sondern aus dem Verhältnismäßigkeitsprinzip abgeleitet aus Art. 20 Absatz 3 GG. Diese Anpassung wäre auch sachgerecht, da erhebliche Sicherheitsvorfälle hinsichtlich KMU eher selten sein dürften als auch die Anzahl der betroffenen Nutzer nicht hoch sein dürfte.

Wir würden uns über eine Berücksichtigung der von uns angesprochenen Punkte sehr freuen und stehen Ihnen für Rückfragen und einen weiteren Austausch jederzeit sehr gerne zur Verfügung.

Mit freundlichen Grüßen

Bundesverband Glasfaseranschluss e. V.

Wolfgang Heer	Nicolas Goß
Geschäftsführung	Recht & Regulierung

Über den BUGLAS

Der BUGLAS vertritt mehr als 170 Unternehmen, die in Deutschland den Ausbau von Glasfasernetzen (Fiber to the Building/Home, FttB/H) vorantreiben. Dazu zählen ausbauende Unternehmen, Netzbetreiber und Ausrüster. Unsere Mitgliedsunternehmen versorgen über 70 Prozent aller Glasfaserkunden in Deutschland mit nachhaltiger digitaler Infrastruktur. Der BUGLAS setzt sich für

einen flächendeckenden Ausbau von Glasfasernetzen ein und spricht sich für investitionsfreundliche Rahmenbedingungen aus, in denen FttB/H-Geschäftsmodelle erfolgreich realisiert werden können.