Gesellschaft für Datenschutz
und Datensicherheit e.V.

An das Bundesministerium des Innern
Referat CI 1 (per E-Mail: NIS2@bmi.bund.de)

Stellungnahme der GDD e.V. zum Referentenentwurf des Bundesministeriums des Innern vom 23.06.2025 für ein Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)

GDD e.V.
Heinrich-Böll-Ring 10
53119 Bonn
T +49 228 969675-00
F +49 228 969675-25
info@gdd.de
www.gdd.de

Vorstand
Prof. Dr. Rolf Schwartmann (Vorsitzender)
Kristin Benedikt
Dr. Stefan Brink
Ulrike Egle
Prof. Dr. Rainer W. Gerling
Bettina Herman
Gabriela Krader
Prof. Dr. Michael Meier
Thomas Müthlein
Steve Ritter
Prof. Dr. Gregor Thüsing

Prof. Peter Gola (Ehrenvorsitzender)

Geschäftsführer
Andreas Jaspers, Rechtsanwalt

Informationen zum Datenschutz unter www.gdd.de/datenschutzerklaerung

Sehr geehrter Herr Dr. Meltzian,
sehr geehrte Damen und Herren,

die Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. tritt als gemeinnütziger Verein für einen sinnvollen, vertretbaren und technisch realisierbaren Datenschutz ein. Sie hat zum Ziel, die Daten verarbeitenden Stellen bei der Lösung und Umsetzung der vielfältigen mit Datenschutz und Datensicherheit verbundenen rechtlichen, technischen und organisatorischen **Anforderungen zu unterstützen. Dabei steht die Umsetzung der NIS-2-Richtlinie** (NIS2) derzeit auch für unsere über 3500 Mitglieder im Fokus. Angesichts der fortwährenden Bedrohungslage für die IT-Sicherheit und die bereits abgelaufene Umsetzungsfrist, begrüßen wir, dass die neue Bundesregierung dieses Vorhaben nun mit Priorität wiederaufgreift und zügig vorantreibt. Als Fachgesellschaft erlauben wir uns die nachfolgende Stellungnahme zum Entwurf zu übermitteln, da wir hoffen, so zu einer angemessenen Lösung beitragen zu können, die der Cybersicherheit ebenso Rechnung trägt wie der Reduzierung der Umsetzungsbelastung auf das dafür notwendige Maß.

1. Art. 1, § 2 BSIG-E (Begriffsdefinitionen)

Im Gesetz werden wesentliche neue Begriffe eingeführt, ohne sie zu definieren.

a. Risiko

Der Begriff „Risiko“ ist bislang in den geltenden deutschen Gesetzen nicht definiert! In Art. 6 Nr. 9 der NIS-2-Richtline, in Art. 2 Nr. 6 der CER-Richtlinie sowie in § 2 Abs. 2 Nr. 7 des Referentenentwurfs des KRITIS-Dachgesetzes aus

dem April 2024 wird der Begriff dann jedoch definiert. Entweder sollte der Begriff in den jeweiligen Umsetzungsgesetzen konsequent nicht legaldefiniert werden oder in allen neuen Gesetzen, die ihn verwenden. Es wird daher empfohlen eine entsprechende Definition in den BSIG-E aufzunehmen:

> *„Risiko" das Potenzial für Verluste oder Störungen, die durch einen Sicherheitsvorfall verursacht werden, das als eine Kombination des Ausmaßes eines Verlusts oder einer Störung und der Wahrscheinlichkeit des Eintretens des Sicherheitsvorfalls zum Ausdruck gebracht wird;*

Entsprechend sollte der Begriff „Risikoanalyse" analog dem Entwurf für § 2 Nr. 7 KRITIS-Dachgesetz vom April 2024 definiert werden:

> *„Risikoanalyse" ein systematisches Verfahren zur Bestimmung eines Risikos;*

b. Cyberhygiene

Die NIS-2-Richtlinie nutzt an mehreren Stellen den Begriff „Cyberhygiene" (z.B. Art. 7 Abs. 1 lit. f) und i), Art. 21 Abs. 2 lit. g)) ohne ihn zu definieren. In Art. 17, § 5c Abs. 4 Nr. 7 EnWG-E wird der neue Begriff „Cyberhygiene" ebenfalls verwendet, allerdings auch ohne Definition. Im Art. 26, § 165 Abs. 2a Nr. 7 TKG-E wird in der Formulierung der Anforderungen darauf verzichtet. Stattdessen ist von „Grundlegenden Verfahren und Schulungen im Bereich der Sicherheit von Netzen und Diensten" die Rede. Im Art. 1, § 30 Abs. 2 S.2 Nr. 7 BSIG-E wird die Formulierung „grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit der Informationstechnik" verwendet. Der RegE (BT-Drs. 20/13184) enthielt ebenfalls noch den Begriff der Cyberhygiene. Es ist nicht nachvollziehbar, warum ein und dieselbe Vorgabe der NIS-2-Richtlinie in drei Gesetzen jeweils unterschiedlich umgesetzt wird. Im Interesse einer Einheitlichkeit sollte an allen drei Stellen des Gesetzentwurfs eine einheitliche Formulierung benutzt werden. Falls dabei der Begriff „Cyberhygiene" verwendet wird, sollte er legaldefiniert werden. Dabei sollte beachtet werden, dass der Begriff, wie er in der NIS-2-Richtlinie beschrieben wird, eher unterhalb des Standes der Technik angesiedelt zu sein scheint. Dafür spricht neben den Maßnahmen, die in ErwG 89 genannt werden, auch seine Verwendung im Kontext des Art. 18 Abs. 1 lit. c) NIS-2-Richtlinie. Denn Maßnahmen, die für die Bürger gedacht sind, werden regelmäßig eher den allgemein „anerkannten Regeln der Technik" entsprechen als dem „Stand der Technik", der auch fortschrittliche und neuere Maßnahmen umfasst. Da es in den Regelungen des BSIG, EnWG und TKG um Absicherungsmaßnahmen für wichtige und besonders wichtige Unternehmen geht, die den Stand der Technik einhalten sollen, und nicht bloß um solche für Bürgerinnen und Bürger, dürfte sich eine Definition des Begriffs Cyberhygiene also nicht in der bloßen Aufzählung der Maßnahmen aus ErwG 89 der NIS-2-Richtlinie erschöpfen.

c. Uneinheitliche Verwendung der „Sicherheitsbegriffe“

An dieser Stelle sei noch angemerkt, dass der Entwurf die Begriffe Informationssicherheit (Definition § 2 Nr. 17 BSIG-E), Datensicherheit (§ 20 Abs. 3 Nr. 1 BSIG-E), Netzsicherheit (§ 20 Abs. 3 Nr. 1 BSIG-E), Netz- und Informationssicherheit (z.B. § 23 Abs. 2 lit. a), IT-Sicherheit (z.B. § 55 BSIG-E oder Art 17, § 5c EnWG-E), Cybersicherheit (im Kontext von Zertifizierung, z.B. § 3 Nr. 9 BSIG-E) oder Sicherheit in der Informationstechnik (Definition § 2 Nr. 39 BSIG-E) verwendet, ohne dass immer der Unterschied der Bedeutung erkennbar wird. Der Entwurf sollte auf eine einheitliche, stringente Verwendung der Begriffe geprüft werden. Einheitliche Begriffe tragen zur Verständlichkeit und Rechtssicherheit bei den Umsetzungsverpflichteten aber auch bei den Behörden und Gerichten bei.

d. Festlegung der Erheblichkeitsschwelle

Die Meldepflicht wird durch „erhebliche Sicherheitsvorfälle“ ausgelöst. Der Begriff wird zwar in § 2 Nr. 11 BSIG-E definiert, diese Definition wird jedoch praktische Folgefragen auf. Denn ein Sicherheitsvorfall soll auch dann erheblich sein, wenn er andere Personen „durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann“. Es bleibt unscharf, was erhebliche immaterielle Schäden sein sollen. Die nähere gesetzliche Vorkonturierung ist insbesondere deswegen nötig, da bereits die Möglichkeit solcher Schäden die Meldepflicht auslösen sollen und Verstöße gegen die Meldepflicht bußgeldbewehrt sind. Für die verpflichteten Einrichtungen muss hier Rechtsklarheit geschaffen werden. Es wird begrüßt, dass dem BMI in Art. 1, § 56 Abs. 5 BSIG-E die Ermächtigung zum Erlass einer entsprechenden Rechtsverordnung eingeräumt wird. Von dieser sollte schnell Gebrauch gemacht werden. Idealerweise sollte eine entsprechende Frist für das BMI bereits in die Verordnungsermächtigung aufgenommen werden, wie Art. 23 Abs. 11 UAbs. 2 S. 1 NIS-2-Richtline dies für die Durchführungsakte der Kommission in Bezug auf bestimmte Einrichtungen vorsieht.

Zudem möchten wir darauf hinweisen, dass das Rangverhältnis in § 2 Nr. 11 BSIG-E bisher unglücklich geregelt ist. Zwar ist vorgesehen, dass die Rechtsverordnung des BMI zur Festlegung der Erheblichkeitsschwelle der allgemeinen Beschreibung in § 2 Abs. 11 Buchst. a und b BSIG-E vorgeht. Es wird dort aber nicht definiert, dass mögliche Durchführungsrechtsakte der EU-Kommission nach Art. 23 Abs. 11 UAbs. 2 S. 2 NIS-2-Richtlinie sowohl den § 2 Nr. 11 Buchst. a und b BSIG-E als auch der Verordnung des BMI nach § 56 Abs. 5 BSIG-E vorgehen. Diese Feststellung findet sich erst im letzten Satz der Verordnungsermächtigung in § 56 Abs. 5 BSIG-E. Als Teil der Begriffsbestimmung gehört sie jedoch nicht dorthin, sondern in die Definition des § 2 Nr. 11 BSIG-E selbst.

2. Art. 1, § 1 BSIG-E (Aufgabenmaßstab)

Im Rahmen des 2. IT-Sicherheitsgesetzes (IT-SiG 2.0) wurde in § 1 die Regelung eingeführt, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) seine Aufgaben *gegenüber den Bundesministerien* auf Grundlage wissenschaftlich-technischer Erkenntnisse durchführt. Die entsprechende Formulierung findet sich nun auch in § 1 BSIG-E wieder. Sie wirft jedoch die Frage auf, was der erkenntnisleitende Maßstab der Arbeit des BSI gegenüber seinen übrigen Zielgruppen (Bundesbehörden, Verbraucher, Hersteller, Anwender etc.) sein soll. Sollen die diese Zielgruppen betreffenden Aufgaben nach politischen, wirtschaftlichen oder sonstigen Maßgaben durchgeführt werden? An dieser Stelle wäre eine Klarstellung sinnvoll.

3. Art. 1, § 3 Abs. 1 S. 2 Nr. 18 c BSIG-E (Unterstützung der Sicherheitsbehörden)

Bereits seit vielen Jahren ist in der Aufgabennorm des BSI die Unterstützung verschiedenster Sicherheitsbehörden vorgesehen. Dazu findet sich die Einschränkung: *„die Unterstützung darf nur gewährt werden, soweit sie erforderlich ist, um Tätigkeiten zu verhindern oder zu erforschen, die gegen die Sicherheit in der Informationstechnik gerichtet sind oder unter Nutzung der Informationstechnik erfolgen.“*. Insbesondere der hintere Satzteil vermag jedoch Zweifel zu schüren, ob das BSI zweifelsfrei der IT-Sicherheit verpflichtet ist oder es nicht doch auch zu seinem Aufgabenprofil gehört, den übrigen Sicherheitsbehörden bei der Ausnutzung von IT-Unsicherheit zu helfen. Während diese Unklarheit früher noch dadurch gerechtfertigt werden konnte, dass das BSI die vorrangige und kompetente Stelle des Bundes in Fragen der Informationstechnik war, hat sich die Lage inzwischen verändert. Genau für diese Beratungsaufgaben gegenüber den Sicherheitsbehörden wurde 2017 die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) als Bundesüberbehörde gegründet. Damit besteht kein Grund mehr, dass das BSI anderen Interessen gegenüber verpflichtet bleibt, als denen der IT-Sicherheit.

Der Satzteil *„oder unter Nutzung der Informationstechnik erfolgen“* sollte daher gestrichen werden.

4. Art. 1, § 5 BSIG-E (Schwachstelleninformationen)

Wie bisher soll das BSI als zentrale Meldestelle Informationen über Sicherheitsrisiken, zu denen auch Informationen über Sicherheitslücken in Hard- und Software gehören, entgegennehmen (Abs. 1 und 2). Diese Informationen sollen unter anderem genutzt werden, um Dritte über die Schwachstellen zu informieren (Abs. 3). Das BSI soll also als Informationsdrehscheibe für IT-Sicherheitslücken dienen.

Wir begrüßen grundsätzlich, dass mit dem BSI ein zentraler Ansprechpartner für entdeckte IT-Sicherheitslücken festgelegt wird. Allerdings befindet sich das BSI ebenso wie die Polizeien und das Bundesamt für Verfassungsschutz im Geschäftsbereich des Bundesministeriums des Innern und für Heimat (BMI). Diese anderen Sicherheitsbehörden haben ein Interesse daran, dass Sicherheitslücken zwar ihnen bekannt aber nicht geschlossen werden, damit sie diese etwa für Remote Forensic Software ausnutzen können. Da das BSI auch nach Gründung des Bundesministeriums für Digitalisierung und Staatsmodernisierung auch weiterhin gegenüber dem BMI weisungsgebunden ist, kann auf Basis des aktuellen Gesetzestextes nicht ausgeschlossen werden, dass das BSI angewiesen wird, eine ihm gemeldete Sicherheitslücke zurückzuhalten, statt den Hersteller zu informieren und die Anwender zu warnen. Angesichts der Bedeutung, den eine verlässlich sichere Informationstechnik für die digitalisierte Gesellschaft hat, ist dieses Risiko nicht akzeptabel. Wenn dem BSI Sicherheitslücken bekannt werden, müssen diese dem Hersteller gemeldet werden, damit dieser sie schließen kann. Nur so können die Anwender in die Lage versetzt werden, ihre IT sicher zu betreiben und damit die Ziele der NIS-2-Richtlinie zu erreichen.

Daher sollte im Gesetz klargestellt werden, dass das BSI die ihm bekannt gewordenen Sicherheitslücken stets dem Hersteller legitimer Software zu melden hat und entgegenstehende Weisungen nicht zu befolgen braucht. Wie bereits in unserer Stellungnahme an den Innenausschuss des Bundestages zum letzten RegE vorgeschlagen, könnten dafür nach Abs. 3 S. 1 Nr. 5 eine neue Nr. 6 und ein Abs. 3 S. 2 und S. 3 ergänzt werden:

„6. Hersteller von Hard- und Software über Schwachstellen in ihren Produkten zu informieren.

Weisungen, die von S. 1 Nr. 6 abweichen, nimmt das BSI nicht entgegen. Eine Abweichung von S. 1 Nr. 6 ist nur zulässig, wenn es sich bei dem Produkt selbst um Schadsoftware handelt.“

Damit wird ausgeschlossen, dass dem BSI Weisungen erteilt werden können, die einer Schwachstellenschließung und damit einer sicheren IT-Infrastruktur in Deutschland entgegenstehen. Der neue Abs. 3 S. 3 stellt klar, dass Hersteller von Schadsoftware selbstverständlich nicht über Lücken in ihrer Software nicht informiert werden müssen.

5. Art. 1, § 7 Abs. 6 und 7 BSIG, § 29 Abs. 3 BSIG-E, § 43 Abs. 5 S. 4 BSIG, § 44 Abs. 1 S. 7 und Abs. 5 S. 3 BSIG-E

Der vorgelegte Gesetzentwurf sieht eine ganze Reihe von Ausnahmen für bestimmte Behörden vor. Dazu zählen etwa die Ausnahmen für die Auslands-IT des Auswärtigen Amtes sowie den Geschäftsbereich des Bundesministeriums der Verteidigung im Zusammenhang mit Kontrollbefugnissen des BSI.

Auch im Zusammenhang mit den Absicherungs- und Meldepflichten finden sich Ausnahmen für beide Ressorts und zusätzlich für den BND und das BfV.

Das ist insofern unverständlich, da die IT der Bundesverwaltung vernetzt ist und jedes Netz nur so sicher ist, wie sein schwächstes Glied. Zudem erscheint es vor dem Hintergrund der aktuellen geopolitischen Lage sowie den verstärkten Aufklärungs-Aktivitäten und Cyberoperationen fremder Staaten kaum nachvollziehbar, dass gerade die IT-Sicherheit dieser wichtigen Bereiche von gesetzlichen Pflichten ausgenommen und der Eigenverantwortung der jeweiligen Einrichtung überlassen werden sollen. Gerade im Hinblick auf die erfolgreichen und öffentlich gewordenen Angriffe auf das Auswärtige Amt vor einigen Jahren haben gezeigt, dass in diesem Bereich Handlungsbedarf besteht. Daher sollten sämtliche Ausnahmen für einzelne Teile der Bundesverwaltung gänzlich gestrichen werden. Es ist nicht konsequent, einerseits der Wirtschaft mit Verweis auf die gewachsene Gefährdungslage und die Folgen eines Ausfalls von Unternehmen immer mehr Pflichten in Bezug auf die Informationssicherheit aufzuerlegen und andererseits wichtige Teile der öffentlichen Verwaltung von entsprechend engen Verpflichtungen auszunehmen.

6. Art. 1, § 28 Abs. 3 BSIG-E

Nach § 28 Abs. 3 BSIG-E sollen für die Zuordnung einer Einrichtung zu den Sektoren nach den Anlagen 1 und 2 künftig solche Geschäftstätigkeiten außen vor bleiben, die im Hinblick auf die Gesamttätigkeit einer Einrichtung „vernachlässigbar“ sind. Die Zielrichtung dieser Regelung begrüßen wir, da ansonsten etwa Tätigkeiten, die zwar nicht als Geschäftszweck verfolgt werden, die aber formal gewerbliche Tätigkeiten darstellen, wie die Eigenerzeugung von Solarstrom, zur Zuordnung zum Sektor Stromerzeugung führen könnten.

Dieser Ansatz dürfte auch eher richtlinienkonform sein, als der Weg aus dem letzten RegE, bei dem die Berechnung der Unternehmensgröße modifiziert werden sollte. Der alte Ansatz widersprach eindeutig dem Ziel einer einheitlich festgelegten size-cap-rule für die Einrichtungen. Demgegenüber stellt der neue Ansatz in § 28 Abs. 3 BSIG-E auf die Zuordnung der primären Geschäftstätigkeit zu den in der NIS-2-Richtlinie genannten Wirtschaftssektoren ab und erscheint daher grundsätzlich gangbar.

Problematisch ist indes, dass unklar bleibt, bis zu welchem Umfang eine Tätigkeit noch als „vernachlässigbar“ angesehen werden kann. Da sich an diesem Begriff sämtliche Pflichten für die Einrichtungen knüpfen, muss hier Klarheit geschaffen werden. Dies muss auch gesetzlich erfolgen und darf als ganz wesentliche Grundentscheidung über den Umfang der erfassten Ein-

richtungen nicht der künftigen Aufsichtspraxis überlassen bleiben. Was „vernachlässigbar“ genau bedeutet, muss in § 28 Abs. 3 BSIG-E daher noch verbindlich festgeschrieben werden.

7. Art. 1, § 30 Abs. 2 S. 2 BSIG-E, Art. 17, § 5c Abs. 3 neu EnWG und Art. 25, §165 Abs. 2a neu TKG

In diesen drei Änderungen wird eine Aufzählung von Vorgaben aus Art. 21 Abs. 2 der NIS-2-Richtlinie umgesetzt. Dabei wird nicht auf einheitliche Begrifflichkeiten gesetzt. In der jeweiligen Nr. 1 werden die Termini „*Sicherheit in der Informationstechnik*“ (BSIG-E), „*Sicherheit für Informationstechnik*“ (EnWG) und „*Sicherheit für Informationssysteme*“ (TKG) genutzt. In der jeweiligen Nr. 5 wird „*informationstechnischen Systemen, Komponenten und Prozessen*“ (BSIG-E) und „*Netz- und Informationssystemen*“ (EnWG und TKG) verwendet.

Wenn schon bei der erstmaligen Umsetzung unterschiedliche Formulierungen für identische Sachverhalte genutzt werden, lässt sich absehen, wie die Formulierungen nach einigen Gesetzesnovellen auseinanderlaufen. Die IT-Sicherheitsgesetzgebung benötigt jedoch einheitliche und sauber definierte Begriffe. Daher sollte die Begriffsverwendung vereinheitlicht werden. Alternativ müsste im Sinne der Verständlichkeit der Normen klar dargestellt werden, warum unterschiedliche Begriffe verwendet werden und was das für die verpflichteten Einrichtungen bedeutet.

8. Nachteilsverbot bei Meldungen - Art. 1, § 30 Abs. 7 BSIG-E aus dem letzten RegE

Der RegE des Art. 1, § 30 Abs. 7 BSIG-E enthielt die Regelung, dass der Austausch von Informationen und die Abgaben freiwilliger Meldungen nicht dazu führen dürfen, dass den Einrichtungen Verpflichtungen auferlegt werden, die ohne die Meldung nicht für sie gegolten hätten. Im nun vorgelegten Referentenentwurf wurde diese Regelung ersatzlos gestrichen. Gründe für die Streichung sind nicht erkennbar.

Gerade im Bereich Cybersicherheit ist ein schneller und freier Austausch von Lage- und Gefährdungsinformationen notwendig. Die Schnelligkeit mit der dies geschieht, kann hier den Unterschied zwischen verhinderten oder eingetretenen Vorfällen machen. Daher sollte der Rahmen für den Informationsaustausch so gewählt werden, dass Einrichtungen nicht aus Angst vor Nachteilen, von freiwilligen Meldungen abgeschreckt oder deren Abgabe – z.B. wegen zwischengeschalteter Prüfung evtl. erwachsender Nachteile – ausgebremst werden. Die im letzten RegE vorgesehene Regelung des § 30 Abs. 7 BSIG-E sollte daher dringend wieder aufgenommen werden.

9. Art. 1, § 31 Abs. 2 BSIG-E, Art. 17, § 5c Abs. 4 EnWG-E (Systeme zur Angriffserkennung)

Die Regelung des Art. 1, § 31 Abs. 2 BSIG-E und Art. 17, § 5c Abs. 4 EnWG-E heben eine bestimmte Risikomanagementmaßnahme, nämlich die Angriffserkennungssysteme, heraus, ohne dass ersichtlich ist, warum. Welche Risikomanagementmaßnahmen zu ergreifen sind, muss sich immer aus einer vorausgehenden Risikoanalyse ergeben. Erst aus dieser lässt sich ableiten, welche Maßnahmen das Risiko am effektivsten adressieren. Angriffserkennungssysteme können und werden oft eine dieser Maßnahmen sein. Ob sie jedoch die sind, die in einer Auswahl verschiedener Maßnahmen und unter Berücksichtigung des Aufwandes insgesamt den besten Schutz versprechen, lässt sich nicht a priori und für alle Fälle gleichförmig beantworten. Es ist denkbar, dass die Aufwände für den Aufbau und Betrieb eines Angriffserkennungssystems in anderen Maßnahmen besser investiert wären und zu einem höheren Schutzniveau führen. Auf dieses grundsätzliche Problem wurde bereits bei Einführung der Vorgängerregelung durch IT-Sicherheitsexperten hingewiesen. Leider wurde dem kein Gehör geschenkt. Wenn Ziel des Gesetzes ist, die IT-Sicherheit bestmöglich zu fördern, sollte dieser Fehler nicht fortgeschrieben, sondern § 31 Abs. 2 BSIG-E und § 5c Abs. 4 S. 3 Nr. 11 EnWG-E gestrichen werden.

10. Art. 1, § 39 Abs. 1 BSIG-E – Begrenzung der Nachweispflicht

Wir begrüßen ausdrücklich, dass in § 39 Abs. 1 BSIG-E klargestellt wird, dass sich die Nachweispflicht für KRITIS-Betreiber auch künftig nicht auf deren gesamte IT bezieht, sondern nur auf diejenige, die für den Betrieb der kritischen Anlagen relevant ist. Dies war im RegE der letzten Legislaturperiode noch nicht vorgesehen. Durch die Klarstellung werden unnötige Zusatzaufwände für Betreiber deutlich reduziert, die nicht nur kritische Anlagen betreiben und die Nachweise nach der letzten Fassung für sämtliche IT hätten erbringen müssen. Mit der aktuellen Fassung wird der Aufwand auf das notwendige Maß begrenzt und gleichzeitig ein hinreichendes Maß an erhöhter Sicherheit für Kritische Infrastrukturen beibehalten, so dass die Regelung jetzt als gut ausgewogen bezeichnet werden kann.

11. Art. 1, 32, 40 BSIG-E (Meldepflichten) - Vermeidung der Pflicht zu doppelten Meldungen

Mit § 32 BSIG-E wird eine große Zahl von Einrichtungen einer neuen Meldepflicht unterworfen. Dabei unterliegen bereits heute viele Unternehmen verschiedensten Meldepflichten aufgrund verschiedenster Regelungen. Dazu zählt u.a. die Meldepflicht für Datenschutzverletzungen nach Art. 33 DS-GVO. Die Vielzahl unterschiedlicher Meldeverpflichtungen führt zu einem kontinuierlichen Anstieg der Bürokratie für die verpflichteten Einrichtungen, ohne

dass dem im gleichen Maß Vorteile gegenüberstehen. Daher sollte bereits auf gesetzgeberischer Ebene versucht werden, die Meldepflichten zu vereinfachen und zu vereinheitlichen. Hier gilt es die Möglichkeiten, die die Digitalisierung der Verwaltung bietet, zu nutzen.

Gerade im Fall von IT-Sicherheitsvorfällen ist die Wahrscheinlichkeit hoch, dass auch personenbezogene Daten betroffen sein können und neben der Meldepflicht nach NIS2 auch eine nach Art. 33 DS-GVO ausgelöst wird. Statt zweimal an unterschiedliche Stellen melden zu müssen, wäre es sinnvoll, ein zentrales Meldeportal zu etablieren, auf dem die Meldepflichtigen ihre Informationen einmal zentral eingeben und das dann automatisch die jeweils benötigten Eingaben an die jeweils zuständige NIS-2- und Datenschutzaufsichtsbehörde weiterleitet.

Der Bundesrat hatte bereits einen entsprechenden Vorschlag zum letzten RegE unterbreitet (BR-Drs. 380/24, S. 11). Auch wenn dieser Vorschlag noch nicht ausgereift war, begrüßen wir das dahinterstehende Ziel, den Meldeaufwand für die Einrichtungen zu reduzieren. Da die Realisierung weder rechtlich noch in der technischen Umsetzung trivial ist und die gesetzgeberische Lösung sicherlich einige Zeit benötigt, ist es aus Sicht der GDD nachvollziehbar, diesen Vorschlag noch nicht im laufenden NIS-2-Umsetzungsgesetzgebungsverfahren aufzugreifen. Dies würde die ohnehin verspätete Richtlinienumsetzung nur noch weiter verzögern. Gleichwohl bitten wir darum, diese vereinheitlichte Meldemöglichkeit weiter zu verfolgen, ausarbeiten zu lassen und bei passender Gelegenheit in ein Gesetzgebungsverfahren einzubringen, um den Erfüllungsaufwand in der Wirtschaft jedenfalls mittelfristig wieder zu reduzieren.

12. Art. 1, § 50 Abs. 1 BSIG-E (Auskünfte Domainnamen)

§ 50 Abs. 1 BSIG-E verpflichtet Top-Level-Domain Name Registries und Domain-Name-Registry-Dienstleister zur Herausgabe der bei ihnen gespeicherten Informationen auf berechtigtes Verlangen. Die Informationen sollen binnen 72 Stunden herausgegeben werden und das Nichtvorliegen der Informationen soll sogar binnen 24 Stunden nach Antragseingang mitgeteilt werden. Damit wirft die Regelung zwei Probleme auf.

a. Fehlende Definition des berechtigten Verlangens

Das erste ist die Frage, wann ein Informationsverlangen berechtigt ist. Dazu geben weder der Wortlaut der Richtlinie noch der vorliegende Umsetzungsgesetzestext einen Hinweis. Im Hinblick darauf, dass es sich bei den herauszugebenden Informationen um personenbezogene Daten handeln kann, erscheint eine Herausgabepflicht ohne klar umrissenen Verarbeitungszweck

und Berechtigungsumfang problematisch. Hier ist eine klarere Konturierung der Pflicht im Gesetzestext selbst notwendig.

b. Überumsetzung der Richtlinie bei der Frist zur Negativmitteilung

Das zweite Problem ergibt sich aus der Frist für Negativmitteilungen von 24 Stunden. Es ist ohnehin problematisch, wenn zu Negativmitteilungen verpflichtet wird, da diese für die Unternehmen stets unnötige Aufwände erzeugen. Warum dann die Pflicht auch noch binnen 24 Stunden – für die Unternehmen also prioritär – erfüllt werden soll, ist nicht nachvollziehbar. Die Richtlinie selbst schreibt für die Auskunft selbst vor, dass diese zwar unverzüglich aber spätestens binnen 72 Stunden zu beantworten sind. Damit erfasst sie sowohl die Positiv- wie die Negativantwort in einer einheitlichen Frist. Daran sollte sich auch die deutsche Umsetzung orientieren, statt ohne Not über die Richtlinienvorgaben hinauszugehen.

13. Art. 1, § 65 BSIG-E; Art. 17, § 95 EnWG-E; Art. 25, § 228 TKG-E (Bußgeldvorschriften)

Die Regelungen zu den Bußgeldern in BSIG-E, EnWG-E und TKG-E sind verbesserungsbedürftig und teilweise richtlinienwidrig.

a. Keine sichere Vermeidung doppelter Bußgelder im Bereich des BSIG-E

In § 65 Abs. 10 BSIG-E wird – ganz der Richtlinie folgend – geregelt, dass das BSI als NIS-2-Aufsichtsbehörde dann keine Bußgelder verhängen darf, wenn die Datenschutzaufsichtsbehörden für das gleiche Verhalten bereits eine nach Art. 58 DS-GVO verhängt haben.

Wir begrüßen, dass der europäische und der deutsche Gesetzgeber eine Doppelsanktionierung von Verstößen gegen die Datensicherheit im Cybersicherheits- und Datenschutzrecht vermeiden wollen. Leider ist die Regelung weder auf europäischer noch auf nationaler Ebene gelungen, da sie lediglich der NIS-2-Behörde verbietet, ein Bußgeld zu verhängen, wenn die Datenschutzbehörde dies bereits getan hat. Umgekehrt ist die Verhängung eines Bußgeldes durch die Datenschutzaufsichtsbehörden aber weiterhin möglich, wenn die NIS-2-Behörde bereits eines für das gleiche Verhalten verhängt hat. Es ist nach der derzeitigen Regelung also vom Zufall bzw. der Geschwindigkeit der jeweiligen Behörden abhängig, ob einer Einrichtung eine Doppelbestrafung droht oder nicht. Stattdessen sollte aber das Bußgeldverfahren gesetzlich so strukturiert werden, dass Doppelsanktionen sicher ausgeschlossen sind. Da eine Einschränkung der Bußgeldkompetenz der Datenschutzbehörden europarechtlich ausgeschlossen ist, wäre es etwa denkbar, dass das BSI als

NIS-2-Bußgeldbehörde vor Einleitung eines Bußgeldverfahrens das Einvernehmen der zuständigen Datenschutzaufsichtsbehörde einholen muss. Diese könnte mit dem Einvernehmen erklären, selbst nicht wegen des gleichen Verhaltens ein Bußgeld nach der DS-GVO verhängen zu wollen. Die jeweils zuständige Datenschutzaufsichtsbehörde ist dem BSI aufgrund der Angaben aus der Registrierung der Einrichtungen auch bereits bekannt.

Die entsprechende Vorgabe könnte durch eine Ergänzung des § 65 Abs. 10 BSIG-E um folgenden Satz erreicht werden:

„Um eine doppelte Verhängung von Bußgeldern zu vermeiden, hat das Bundesamt vor Verhängung eines Bußgeldes das Einvernehmen der zuständigen Aufsichtsbehörde nach der Verordnung (EU) 2016/679 einzuholen.“

b. Fehlende Kollisionsregelungen in EnWG und TKG

Soweit der vorliegende RefE die Bußgeldregelungen in Art. 17, § 95 EnWG-E und Art. 25, § 228 TKG-E anpasst, lässt er die Vorgaben des Art. 35 Abs. 2 NIS-2-Richtlinie völlig außer Acht. Danach dürfen die NIS-2-Aufsichtsbehörden keine Bußgelder für Sachverhalte verhängen, wenn die zuständige Datenschutzaufsichtsbehörde bereits in gleicher Sache eines verhängt hat. In § 65 Abs. 10 BSIG-E wurde dies vom vorliegenden RefE abgebildet, in § 95 EnWG-E und § 228 TKG-E fehlen entsprechende Regelungen. Da Art. 35 Abs. 2 NIS-2-Richtlinie damit nicht vollständig umgesetzt wurde, könnte dies zur Verlängerung des bereits laufenden Vertragsverletzungsverfahrens führen. Um das zu vermeiden, sollte bei den Bußgeldregelungen in § 95 EnWG und § 228 TKG-E aufgenommen werden, dass § 65 Abs. 10 BSIG-E entsprechend gilt.

14. Art. 6 (Änderung des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme)

Mit Art. 7 NIS2UmsuCG soll die in Art. 6 des zweiten IT-Sicherheitsgesetzes (IT-SiG 2.0) enthaltene Evaluierungsklausel aufgehoben werden. Diese verpflichtet das BMI dazu, die mit dem IT-SiG 2.0 eingeführten Regelungen, u.a. im BSIG, bis zum Mai 2025 zu evaluieren. Die Streichung wird damit begründet, dass sich viele der damals enthaltenen Vorschriften durch die NIS-2-Umsetzung ändern und die unveränderten Regelungen durch das NIS2UmsuCG bestätigt würden. Das überzeugt jedoch nicht. Denn eine Evaluierung dient nicht der bloßen Bestätigung existierender Regelungen. Vielmehr dient sie der Überprüfung, ob die mit einem Gesetz verfolgten Ziele durch die Regelungen auch in der Praxis erreicht werden oder Anpassungen notwendig sind. Eine Evaluierung ist die erforderliche Grundlage dafür, gesetzliche Regelungen entweder zu bestätigen oder anzupassen. An einer solchen Grundlage fehlt es für die im BSIG enthaltenen Grundlagen weiterhin. Denn bereits mit

Art. 6 IT-SiG 2.0 wurde die zuvor im IT-Sicherheitsgesetz von 2015 vorgesehen Evaluierungspflicht aufgehoben. Es drängt sich daher der Eindruck auf, dass zwar entsprechende Klauseln immer wieder vorgesehen, die Evaluierungen dann aber nicht durchgeführt, sondern die Klauseln bei nächster Gelegenheit lieber wieder gestrichen werden.

Das ist nicht akzeptabel, da die eingeführten Verpflichtungen für die Unternehmen massive Aufwände erzeugen und deren Wirksamkeit daher regelmäßig überprüft werden sollte, um ein angemessenes Verhältnis von Aufwand und Wirkung sicherzustellen. Zudem kann nur so sichergestellt werden, dass die Maßnahmen ihr **Ziel, die Cybersicherheit zu erhöhen**, auch in der Praxis wirklich erreichen. Wo dies nicht der Fall ist, sollten diese Regelungen gestrichen oder durch neue, wirksamere Regelungen ersetzt werden. Auch im Hinblick auf die dem BSI seit 2015 eingeräumten Eingriffsbefugnisse und deren grundrechtseinschränkende Wirkung ist eine Evaluierung inzwischen dringend geboten.

Bonn, den 01.07.2025.