21. Wahlperiode

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache 21(4)068
vom 10. Oktober 2025

Schriftliche Stellungnahme

der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Bonn vom 10. Oktober 2025

Gesetzentwurf der Bundesregierung

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

BT-Drucksache 21/1501

Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

BfDI | Postfach 1468 | 53004 Bonn

Deutscher Bundestag
Innenausschuss
Platz der Republik 1

Per E-Mail an:
innenausschuss@bundestag.de

Prof. Dr. Louisa
Specht-Riemenschneider
Die Bundesbeauftragte

Telefon: +49 228 997799 5000
E-Mail: bfdi@bfdi.bund.de

Aktenz.:
Anlage:

Bonn, 10. Oktober 2025

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie (BT-Drs. 21/1501)

Sehr geehrte Damen und Herren,

der vom Bundesminister des Innern vorgelegte Entwurf für ein Gesetz zur Umsetzung der NIS-2-Richtlinie und Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz) wurde von der Bundesregierung beschlossen und ist Ihnen zur Beratung überwiesen worden.

Anliegend übersende ich Ihnen meine Stellungnahme zum Entwurf mit der Bitte um freundliche Berücksichtigung.

Mit freundlichen Grüßen
In Vertretung

Andreas Hartl

Leitender Beamter

Stellungnahme

der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zur öffentlichen Anhörung des Innenausschusses

am 13.10.2025

zum Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz), BT-Drs. 21/1501

Einleitung

1.1 Datenschutz und Datensicherheit gehen Hand in Hand

IT-Sicherheit und Datenschutz sind stark miteinander verzahnt. Zu den Zielen der IT-Sicherheit gehört u.a., den Missbrauch, unberechtigten Zugang und die unberechtigte Nutzung auch von personenbezogenen Daten ausschließen. IT-Sicherheitsrisiken sind damit regelmäßig auch Datenschutzrisiken. Insoweit ist auch der Zuständigkeitsbereich der Datenschutzaufsichtsbehörden im Rahmen des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes betroffen. Da die RL (EU) 2022/2555 (NIS-2-RL) deutlich mehr Unternehmen erfasst als die erste NIS-Richtlinie, erhöht das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz die Anzahl an verpflichteten Unternehmen in Deutschland und wird die enge Zusammenarbeit des Bundesamts für Sicherheit in der Informationstechnik (BSI) und der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) künftig noch weiter an Bedeutung gewinnen.

1.2 Grundrechte schützen

Mit der Sicherstellung der Cyber- und Informationssicherheit sind zahlreiche Eingriffsrechte verknüpft. Nicht nur das Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz (GG) ist hier regelmäßig betroffen, auch in die Grundrechte aus Art. 10 Abs. 1 GG wird im Rahmen von Maßnahmen der IT-Sicherheit eingegriffen. Um Grundrechte zu schützen, ist es essentiell, dass solche Eingriffe stets nur im Rahmen der Verhältnismäßigkeit stattfinden dürfen und einer steten Kontrolle unterstehen. Besonders wichtig ist in diesem Zusammenhang auch, dass betroffene Personen ihre Rechte effektiv geltend machen können.

2. Stellungnahme zu einzelnen Vorschriften

2.1 Zu Artikel 1, Umgang mit Schwachstellen

Bereits im Rahmen der Ressortabstimmungen des Gesetzentwurfes und in früheren öffentlichen Anhörungen des Bundestages[1] hat meine Behörde mehrfach darauf hingewiesen, dass das Vertrauen der Bürgerinnen und Bürger in digitale Infrastrukturen und Dienste gestärkt und aufrechterhalten werden muss und dafür ein klarer und transparenter Prozess für den Umgang des BSI mit Schwachstellen im Gesetz vorgesehen werden sollte.

[1] Vgl. die Stellungnahme vom 24. Januar 2023 gegenüber dem Ausschuss Digitales des Deutschen Bundestages: https://www.bundestag.de/resource/blob/930968/a87d1422fcd9184d4978590092ebdde9/Stellungnahme-BfDI.pdf.

Die Schließung von Schwachstellen ist auch deshalb geboten, da es sonst zu gesetzgeberischen Widersprüchen kommt. Denn einerseits werden die Anwender von IT in einer zunehmenden Zahl von Regelungen zur Absicherung verpflichtet, weil die Auswirkungen unsicherer IT für Gesellschaft und Wirtschaft immer gravierender werden. Andererseits werden die Anwender von IT nicht konsequent in die Lage versetzt, bestehende Lücken in ihrer IT zu schließen, wenn Schwachstellen von staatlichen Stellen bewusst offengehalten werden.

Trotzdem bleibt im RegE ungeklärt, wie das BSI mit Informationen zu Schwachstellen weiter verfahren soll. Es ist jedoch fundamental, dass sämtliche Schwachstellen unverzüglich geschlossen werden, um die Rechte und Freiheiten der Bürgerinnen und Bürger zu schützen und die Funktionsfähigkeit unserer digitalen Wirtschaft und Gesellschaft zu bewahren. Diese Position findet auch unter Expertinnen und Experten weiten Zuspruch, wie sich unter anderem in der 27. Sitzung des Ausschusses für Digitales am 25. Januar 2023 und der Anhörung zum NIS2UmsuCG im Innenausschuss am 04.11.2024 gezeigt hat. Aus technischer Sicht besteht keine Erforderlichkeit, Schwachstellen aufrechtzuerhalten, um Sicherheits- und Strafverfolgungsbehörden Zugriff zu ermöglichen. Ein unregulierter Zugriff über Schwachstellen hat stets Kollateralschäden zur Folge und schadet dem Vertrauen der Bürgerinnen und Bürger in digitale Infrastrukturen und Dienste. Zudem wird die Sicherheit der Produkte für alle Nutzenden geschwächt und nicht nur für diejenigen, gegen die ein solcher Eingriff sich richtet.

Auch wenn das BSI nach eigener Aussage keine Schwachstellen gezielt offenhält, sorgt allein die Unwissenheit darüber, ob gemeldete Schwachstellen geschlossen werden, für sogenannte Chilling Effects, beispielsweise bei Sicherheitsforschenden, die unter Umständen auf eine Meldung nach § 5 BSIG-E verzichten, wenn sie befürchten, dass die von ihnen entdeckte Schwachstelle von Strafverfolgungs- und Sicherheitsbehörden genutzt werden könnte. Um dies zu verhindern, sollte im BSIG klargestellt werden, dass das BSI gemeldete Schwachstellen niemals zurückhält, sondern sie stets der Schließung zuführt. Dafür kann auf den Regelungsvorschlag zurückgegriffen werden, der dem Ausschuss in der 20. Legislaturperiode bereits in der Formulierungshilfe unterbreitet wurde.

Vor § 5 Abs. 3 S. 1 BSIG-E sollte daher folgender neuer S. 1 eingefügt werden:

> *„Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 1 gibt das Bundesamt die Informationen zu den nach Absatz 2 gemeldeten Schwachstellen unverzüglich an den Hersteller oder Produktverantwortlichen zum Zwecke der Schließung der*

Schwachstelle weiter, sofern diese nicht bereits öffentlich bekannt sind.“

2.2 Zu Artikel 1, § 12 BSIG-E (Bestandsdatenauskunft)

§ 12 BSIG-E räumt dem BSI die Befugnis ein, Bestandsdatenauskünfte einzuholen. Die Norm ähnelt dem bisherigen § 5c BSIG und wurde lediglich dahingehend angepasst, dass sich die Befugnis nun auf den Schutz von besonders wichtigen und wichtigen Einrichtungen ausgerichtet ist. Es ist jedoch nicht erkennbar, warum eine solche Eingriffsbefugnis überhaupt noch notwendig ist. Die Vorgängernorm wurde geschaffen, um die IT entsprechender Einrichtungen identifizieren und die Einrichtungen warnen zu können, wenn dem BSI lediglich die IP-Adresse bekannt war und der Verdacht bestand, es könnte eine beaufsichtigte Einrichtung gefährdet sein.[2] Mit der Pflicht zur Registrierung der Einrichtungen inkl. ihrer IP-Adressen in § 33 Abs. 1 Nr. 2 BSIG-E entfällt die Notwendigkeit einer Zuordnung über die Bestandsdatenabfrage jedoch vollständig. Aufgrund der klaren Zweckbindung der Auskunftsbefugnis, hat § 12 BSIG-E damit keinen erkennbaren Anwendungsbereich und sollte daher gestrichen werden.

2.3 Zu Art. 1, § 10 BSIG-E (Anordnungsbefugnis)

§ 10 S. 1 BSIG-E sieht die Befugnis des BSI vor, gegenüber Einrichtungen der Bundesverwaltung im Einzelfall Maßnahmen zu Abwendung oder Behebung eines gegenwärtigen Sicherheitsvorfalles anzuordnen. Mit den IT-Sicherheitsmaßnahmen, deren Umsetzung angeordnet werden kann, gehen regelmäßig Verarbeitungen personenbezogener Daten oder solcher Inhalte einher, die durch das Fernmeldegeheimnis verfassungsrechtlich geschützt sind. Die datenschutzrechtliche Zulässigkeit der Maßnahmen für die Anordnungsempfänger in der Bundesverwaltung wird das BSI aber nicht abschließend prüfen können. In der Folge kann es dazu kommen, dass das BSI gegenüber Einrichtungen der Bundesverwaltung IT-Sicherheitsmaßnahmen anordnet, die datenschutzwidrig sind und der Bundesverwaltung durch mich in der Folge untersagt werden müssten. Die Bundesverwaltung sähe sich dann gegensätzlichen Anordnungen zweier Aufsichtsbehörden ausgesetzt.

Um solche gegensätzlichen Anordnungen zu vermeiden, sieht der derzeit geltende § 8a Abs. 3 S. 5 BSIG auch vor, dass das BSI Anordnungen gegenüber KRITIS-Unternehmen nur im Einvernehmen mit anderen Aufsichtsbehörden des Bundes erlassen darf.[3] Dieses seit fast 10 Jahren bewährte Regelungsvorbild sollte daher auch für Anordnungen gegenüber der Bundesverwaltung zur Anwendung kommen.

---

[2] vgl. Kipker/Reusch/Ritter-*Ritter*, Recht der Informationssicherheit, § 5c BSIG Rn. 9.

[3] Kipker/Reusch/Ritter-*Ritter*, Recht der Informationssicherheit, § 8a BSIG Rn. 35.

Dafür sollte § 10 BSIG-E um folgende Sätze ergänzt werden:

> *„Soweit durch die Maßnahmen nach Satz 1 die Verarbeitung personenbezogener Daten betroffen ist, stellt das Bundesamt vor der Anordnung das Einvernehmen mit der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit her, sofern keine Gefahr im Verzug ist. Bei Gefahr im Verzug unterrichtet das Bundesamt die oder den Bundesbeauftragten unverzüglich über die angeordneten Maßnahmen.“*

2.4 Zu Artikel 1, § 15 BSIG-E (Detektion von Angriffsmethoden und von Sicherheitsrisiken für die Netz- und IT-Sicherheit)

Es ist zu begrüßen, dass das BSI nunmehr umfangreich in die Lage versetzt wird, informationstechnische Systeme der Einrichtungen auf Sicherheitslücken hin zu untersuchen. Die vergangenen Jahre haben gezeigt, dass Schwachstellen trotz zur Verfügung stehender Sicherheitsupdates durch die Betreiber nicht geschlossen wurden. Das Fortbestehen dieser Sicherheitslücken in den Systemen gefährdet den Schutz der darin verarbeiteten personenbezogenen Daten und damit die Rechte der betroffenen Personen. Mit seiner erweiterten Detektionsbefugnis kann das BSI überprüfen, ob solche Sicherheitslücken bestehen, und die Einrichtungen informieren, sofern sie selbst noch keine Kenntnis von den Lücken haben. Zudem kann es durch die Befugnisse die Schließung der Lücken überwachen und aufsichtsrechtlich sicherstellen.

Mit der Befugnis sind jedoch auch grundrechtsrelevante Eingriffe verbunden, da das BSI damit unter Umständen Zugriff auf Daten aus den untersuchten Systemen erlangen kann. Soweit dies durch Art. 10 GG geschützte Daten sind, sieht das Gesetz in § 15 Abs. 1 S. 3 BSIG-E die unverzügliche Löschung vor. Diese gesetzliche Begrenzung der Befugnis ist aus Sicht des Datenschutzes zu begrüßen.
Jedoch sieht das Gesetz nicht mehr die noch in der Vorgängernorm des § 7b BSIG enthaltene verfahrensmäßige Absicherung vor, dass die Befugnis nur nach Anordnung von Bediensteten des BSI mit der Befähigung zum Richteramt genutzt werden dürfen. Das ist in zweierlei Hinsicht verwunderlich und problematisch. Zum einen wird die Befugnis deutlich erweitert. Der Kreis der Einrichtungen, die untersucht werden, wird ebenso vergrößert wie die Menge an technischen Möglichkeiten, auf die das BSI bei den Untersuchungen zurückgreifen darf. Die bisherige gesetzliche Begrenzung auf bloße Portscans fällt weg. Zum anderen konkretisiert die Norm nicht selbst, welche Maßnahmen noch ergriffen werden dürfen und welche nicht. Die einzige Einhegung der Eingriffstiefe erfolgt also durch die Behörde selbst, die die Norm nur im erforderlichen und verhältnismäßigen Rahmen anwenden darf. Dann sollte jedoch wenigstens verfahrensmäßig sichergestellt werden, dass die Nutzung im Rahmen des geltenden Rechts erfolgt, indem eine qualifizierte

Rechtsprüfung explizit vorgesehen wird. Dafür sollte das Anordnungserfordernis wieder in die Norm aufgenommen werden.

Unklar ist zudem der Regelungsgehalt des § 15 Abs. 2 S. 4 BSIG-E, der impliziert, dass das BSI die für den Betrieb eines Systems Verantwortlichen nicht kennen könnte und daher z.B. auf die Bestanddatenauskunft nach § 12 BSIG-E angewiesen sein könnte. Denn die Befugnis des § 15 BSIG-E erlaubt dem BSI die Untersuchungen nur in Bezug auf einen abschließend geregelten Kreis von Einrichtungen. Das heißt, das BSI muss schon zur Nutzung der Befugnis des § 15 BSIG-E wissen, wem das System zuzuordnen ist. Aufgrund der umfassenden Registrierungspflichten in § 33 BSIG-E ist das normativ auch sichergestellt und der Verweis auf die Bestandsdatenauskunft unnötig. Wie die Befugnis des BSI zur Bestanddatenauskunft selbst, sollte daher auch der Verweis in § 15 Abs. 2 S. 4 BSIG-E gestrichen werden.

Zu begrüßen ist wiederum, dass mit den § 15 Abs. 3 und 4 wieder eine Kontrolle der Tätigkeit durch mich vorgesehen ist. Der jetzt gewählte Weg über Kontrollmöglichkeiten für mich auf Anforderung hin ist eine sinnvolle und ausgeglichene Regelung.

2.5 Zu Artikel 1, §§ 21 ff. BSIG-E (Betroffenenrechte)

In Kapitel 2 BSIG-E werden die Kompetenzen des BSI hinsichtlich personenbezogener Daten geregelt. So leitet § 21 BSIG-E zahlreiche Einschränkungen der Betroffenenrechte ein. Beschränkt werden hier die Informationspflicht bei der Erhebung von personenbezogenen Daten (§ 22), das Auskunftsrecht der betroffenen Person (§ 23), das Recht auf Berichtigung (§ 24), das Recht auf Löschung (§ 25), das Recht auf Einschränkung der Verarbeitung (§ 26) sowie das Widerspruchsrecht der betroffenen Person (§ 27).

Aufgrund der erheblichen Vergrößerung des Kreises der betroffenen Einrichtungen wird auch die Menge an personenbezogenen Daten wachsen, die das BSI im Rahmen seiner vom BSIG-E vorgesehenen Kompetenzen verarbeiten wird. Angesichts der Grundrechtsrelevanz vieler Verarbeitungsvorgänge nach dem BSIG-E halte ich es für erforderlich, dass der Verhältnismäßigkeit bei der Einschränkung von Betroffenenrechten nach §§ 21 ff. BSIG-E besondere Rechnung getragen wird.

Aufgrund des deutlich ausgeweiteten Kreises potentiell betroffener Personen ist die Tragfähigkeit der Gesetzesbegründung, dass lediglich die Normen des bisherigen BSIG fortgeführt werden, nicht allzu hoch. Die aktuelle Einschränkung der Betroffenenrechte wurden im Rahmen der nationalen DSGVO-Umsetzung mit dem Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetz EU im November 2019 eingeführt. Der Abwägung lagen also noch die Aufgaben und Befugnisse des BSI zugrunde, wie sie vor dem zweiten IT-Sicherheitsgesetz (IT-SiG 2) und der nun beabsichtigten NIS-2-Umsetzung bestanden. Daher sollten die

Einschränkungen der Betroffenenrechte aus der DSGVO im Lichte der Erfahrungen seit Einführung der DSGVO, der Umsetzung des IT-SiG 2 und dem deutlich erweiterten Betroffenenkreis evaluiert und ihre Verhältnismäßigkeit im Hinblick auf die neuen Verarbeitungsvorgänge und –mengen neu begründet werden. Da dies im laufenden Gesetzgebungsverfahren aufgrund der abgelaufenen Umsetzungsfrist und angesichts des laufenden Vertragsverletzungsverfahrens der EU-Kommission nicht möglich ist, sollte im Umsetzungsgesetz zumindest eine Evaluierungsklausel für diese Regelungen vorgesehen werden.

2.6 Zu Art. 1, § 40 BSIG-E Bürokratie reduzieren, Meldewege bündeln

Die NIS-2-RL legt den Mitgliedstaaten nahe, die Abgabe von Meldungen zu bündeln. Die Meldepflichtigen müssten dann nur eine Meldung gegenüber der zentralen Anlaufstelle nach Art. 8 Abs. 4 NIS 2 RL abgeben und könnten damit sowohl die Meldepflicht nach NIS-2-RL als auch die nach Art. 33 DSGVO erfüllen.

Mit dieser Bündelung der Meldungen könnten die Aufwände für Meldungen auf das notwendige Maß reduziert und ein wesentlicher Beitrag zum Bürokratieabbau geleistet werden. Daher hatte der Bundesrat zum letzten Regierungsentwurf des NIS2UmsuCG bereits vorgeschlagen, dem BSI als zentraler Anlaufstelle nach § 40 BSIG-E die Aufgabe zur Entgegennahme gebündelter Meldungen und die Weiterleitung der Art. 33 DSGVO-Meldungen an die zuständigen Datenschutzaufsichtsbehörden zu übertragen. Diesen Vorschlag hat die Bundesregierung nicht aufgegriffen, da Art. 33 DSGVO keine Öffnungsklausel beinhaltet, die eine Meldung an andere als die zuständigen Datenschutzaufsichtsbehörden vorsieht.

Das Ziel einer solchen Bündelung sollte unbedingt weiterverfolgt werden. Einem vollintegrierten Meldeprozess, wie er ErwG 106 der NIS-2-RL nahelegt, stehen einige rechtliche Herausforderungen gegenüber. So teile ich die Auffassung der Bundesregierung, dass eine befreiende Meldung nach Art. 33 DSGVO bisher nur direkt gegenüber den zuständigen Datenschutzaufsichtsbehörden ergehen kann. Zum anderen dürfte die organisatorische Einbindung des BSI in den Meldeprozess für die Datenschutzbehörden der Länder auch Fragen des Verbots der Mischverwaltung aufwerfen. Um dennoch das Ziel des Bürokratieabbaus erreichen zu können, schlage ich ein zweigeteiltes Vorgehen vor, dessen erster Schritt bereits im Rahmen des NIS2UmsuCG beschritten werden sollte.

Als eine schnelle Lösung bietet es sich an, dem BSI in seiner Rolle als zentraler Anlaufstelle neu die Aufgabe zuzuweisen, Verfahren vorzusehen, mit denen die Einrichtungen bei Erfüllung der NIS-2-Meldepflicht

gleichzeitig auch ihren Verpflichtungen nach Art. 33 DSGVO nachkommen können. Dafür sollte § 40 Abs. 3 BSIG-E um folgende Nummer 5 ergänzt werden:

> *besonders wichtigen und wichtigen Einrichtungen geeignete elektronische Verfahren anzubieten, bei der Erfüllung ihrer Verpflichtungen nach § 32 auch ihren Verpflichtungen nach Art. 33 der Verordnung (EU) 2016/679 nachzukommen. Einzelheiten der Ausgestaltung des gebündelten Meldeverfahrens werden zwischen dem Bundesamt und den zuständigen Datenschutzaufsichtsbehörden geregelt. § 61 Abs. 11 bleibt unberührt.*

Damit würde das BSI im Rahmen seiner Aufgaben als zentrale Meldestelle im Bereich der IT-Sicherheit verpflichtet, den Meldenden die gleichzeitige Abgabe der Meldungen nach Art. 33 DSGVO zu ermöglichen. Dies könnte so ausgestaltet sein, dass die Inhalte aus der NIS-2-Meldung an das BSI in Bezug auf die datenschutzrelevanten Informationen in eine separate E-Mail oder anderweitige elektronische Mitteilung an die zuständige Datenschutzaufsichtsbehörde übernommen werden, die die Meldepflichtigen nur noch absenden müssen. Mit dieser Lösung würden den derzeitigen Vorgaben des Art. 33 DSGVO Rechnung getragen, da die Betroffenen die Meldung noch immer selbst vornehmen würden. Da das BSI die Meldungen nach Art. 33 DSGVO nicht selbst an die Landesdatenschutzbehörden weiterreicht, sondern den Meldenden lediglich die Zweitverwertung der Angaben aus der NIS-2-Meldung erleichtert, sind Probleme mit dem Verbot der Mischverwaltung zwischen Bundes- und Landesbehörden ebenfalls ausgeschlossen.

Durch diese Lösung könnte der bürokratische Aufwand für die Einrichtungen reduziert und die Einhaltung der verschiedenen Meldefristen bereits erleichtert werden. Langfristig sollte jedoch weiter das von ErwG 106 NIS-2-RL postulierte Ziel eines vollintegrierten Meldeprozesses für die NIS-2- und DSGVO-Meldungen verfolgt werden. Hierfür stellen derzeit sowohl die fehlenden Öffnungsklauseln des Art. 33 DSGVO eine Herausforderung dar, als auch das Verbot der Mischverwaltung in Bezug auf die Tätigkeit des BSI für die Landesdatenschutzbehörden. Das Problem der fehlenden Öffnungsklausel, muss auf europäischer Ebene gelöst werden.

2.7 Zu Art. 1, § 11 Abs. 4 S. 2, § 42 und § 56 Abs. 4 BSIG-E; Art. 17, § 5d Abs. 5 EnWG – (Aktenzugang)

Der Gesetzentwurf enthält an vielen Stellen Ausnahmen vom Zugang zu behördlichen Informationen. § 42 BSIG-E basiert auf dem aktuellen § 8e BSIG. Allerdings werden der Umfang des Informationsausschlusses und der Charakter der Regelung fundamental verändert, ohne dass dies notwendig und verhältnismäßig ist. Der geltende § 8e BSIG schränkt den Informationszugang nur in Bezug auf solche Informationen ein, die Kritische

Infrastrukturen, Anbieter digitaler Dienste oder Unternehmen im besonderen öffentlichen Interesse betreffen. Diese Einschränkungen lassen sich damit rechtfertigen, dass es u.a. um sicherheitsrelevante Meldungen bei Einrichtungen geht, die für die Sicherheit und Versorgung in Deutschland von elementarer Bedeutung sind und deren Zahl vor allem auch überschaubar ist. Die Transparenzeinschränkung ist daher bisher begrenzt.

Zudem stellt der bisherige § 8e Abs. 1 keinen bloßen Ausschluss vom Informationszugang dar, sondern ist eine Informationszugangsregelung, die auch eine positive Komponente enthält („kann […] Auskunft […] erteilen“).[4]

Mit beidem bricht die Regelung des § 42 BSIG-E ohne tragfähige Begründung. Statt einer zielgerichteten Ausgestaltung des Informationsanspruches, die die Sicherheits- und Vertraulichkeitsinteressen unserer Gesellschaft und der Betreiber einerseits und das Transparenzinteresse der Bevölkerung in der demokratischen Gesellschaft andererseits in einen angemessenen Ausgleich bringt, enthält § 42 BSIG-G einen pauschalen Informationsausschluss. Dies erscheint umso problematischer, als mit der NIS-2-Umsetzung auch eine Vielzahl von Einrichtungen neu verpflichtet werden, bei denen in einer Abwägung beider Interessen das Geheimhaltungsinteresse nicht das gleiche Gewicht hätte, wie etwa bei Kritischen Infrastrukturen. Daher erscheint mir ein pauschaler Ausschluss des Informationszugangs als zu weitreichend. Aufgrund der Ausweitung der Tätigkeiten des BSI würde damit ein viel größerer Bereich staatlicher Tätigkeiten einem Auskunftsanspruch und damit dem Informationsinteresse der Bürger unzugänglich.

Dabei ist der Ausschluss des Informationszugangs auch inhaltlich deutlich erweitert worden. Statt zielgerichteter Ausschlüsse von Informationen etwa über Meldungen von Sicherheitsvorfällen, bei denen das Interesse am Ausschluss nachvollziehbar ist, soll nach dem Entwurf die gesamte Tätigkeit des BSI nach Teil 3 des BSIG-E im Bereich Informationssicherheit von Einrichtungen intransparent werden. Dafür ist kein tragfähiger Grund ersichtlich. Es ist nicht erkennbar, warum etwa Informationen der Nationalen Verbindungsstelle (§ 40 BSIG-E) oder zu den Geschäftsleitungspflichten (§ 38 BSIG-E) nicht zugänglich sein sollten. Gerade in diesen Bereichen besteht ein nachvollziehbares Interesse, auch der regulierten Einrichtungen, Informationen über die Hintergründe und Grundlagen der zuständigen Aufsichtsbehörde zu erlangen.

Ähnliches gilt für den Ausschluss des Informationszugangs in Bezug auf Teil 1 §§ 4 bis 10 BSIG-E. Denn auch hier wird durch den aktuellen § 42

[4] Kipker/Reusch/Ritter-*Ritter*, Recht der Informationssicherheit, § 8e BSIG Rn. 3.

BSIG-E ein erheblicher Teil der BSI-Tätigkeit der Kontrolle durch die Öffentlichkeit entzogen. Dabei können etwa die Ergebnisse der Kontrolltätigkeit des BSI nach § 7 BSIG-E in abstrakter Form durchaus relevant für die Öffentlichkeit und den Diskurs über das hinreichende Maß an Cybersicherheit in der Bundesverwaltung sein. Nur in wenigen sensiblen Bereichen, wie etwa der Angriffserkennung (§§ 8 und 9 BSIG-E) dürfte ein legitimes Geheimhaltungsinteresse das Transparenzinteresse praktisch immer überwiegen.

Auch im Bereich der Energiewirtschaft sieht § 5d Abs. 5 EnWG-E eine weitgehende Beschränkung des Zugangs zu Akten der BNetzA im Zusammenhang mit den Absicherungs- und Meldepflichten vor, ohne dass dies sachlich notwendig wäre.

Um sowohl den berechtigten Geheimhaltungsinteressen als auch dem Informationsinteresse der Wirtschaft und der Bürger gerecht zu werden, bietet es sich an, die Informationszugangsregelungen in den verschiedenen Gesetzen dem derzeit geltenden § 8e BSIG nachzuahmen. Hierfür biete ich als Bundesbeauftragte für die Informationsfreiheit gerne Unterstützung an.

2.8 Zu Art. 1, §§ 29 Abs. 2, 30, 48 BSIG-E (Vorgaben für die Einrichtung der Bundesverwaltung)

Der Regierungsentwurf sieht vor, dass für die Einrichtungen der Bundesverwaltung die Regelungen für die besonders wichtigen Einrichtungen anwendbar sind. Von den Risikomanagementmaßnahmen des § 30 BSIG-E sind jedoch die meisten Einrichtungen ausgenommen. Daran wurde öffentlich bereits viel Kritik geübt und die Rückkehr zur Regelung aus der Länder- und Verbändebeteiligung gefordert. Diese sah vor, dass die Einrichtungen der Bundesverwaltung „Mindestanforderungen“ an den Schutz der in der Bundesverwaltung verarbeiteten Informationen erfüllen. Die Mindestanforderungen wiederum sollten sich aus den BSI-Standards, dem IT-Grundschutzkompendium sowie den Mindeststandards für die Sicherheit in der Informationstechnik des Bundes (Mindeststandards) ergeben.

Sofern im parlamentarischen Verfahren über eine strengere Verpflichtung für die Bundesverwaltung diskutiert werden sollte, empfehle ich folgende Punkte zu beachten:

Es sollten nicht 1:1 die Regelungen aus der Fassung der Länder- und Verbändebeteiligung übernommen. Das dort in § 44 Abs. 1 BSIG-E enthaltene Anforderungs-Trias ist gesetzessystematisch nicht sinnvoll. Denn Sinn der „Mindeststandards“ ist es bereits, die Mindestanforderungen an die Bundesverwaltung zu formulieren. In diesen sollten die Anforderungen aus den allgemeinen BSI-Standards sowie dem IT-Grundschutzkompendium also bereits durch das BSI in einer Form konsolidiert worden

sein, die von der Bundesverwaltung nur noch umgesetzt werden muss. Denn gerade für die Formulierung einheitlicher Anforderungen an die Bundesverwaltung zur Sicherstellung eines einheitlich hohen Schutzniveaus wurde das Instrument der Mindeststandards gesetzlich geschaffen.[5] Diesem Verständnis folgend sind die Mindeststandards des BSI aber deckungsgleich mit den Mindestanforderungen an die Bundesverwaltung und nicht nur ein untergeordneter Bestandteil derselben.

Zudem warf der Entwurf der Länder- und Verbändebeteiligung weitere Fragen im Zusammenspiel mit der Fiktion aus § 44 Abs. 3 BSIG-E auf. Dies sah vor, dass die Anforderungen aus § 30 BSIG-E für alle Einrichtungen der Bundesverwaltung als erfüllt gelten sollten, soweit die Mindestanforderungen aus § 44 Abs. 1 eingehalten wurden und die Durchführungsrechtsakte der EU-Kommission keine weitergehenden Anforderungen stellen. Offen blieb dabei aber, was die Einrichtungen zu beachten haben, wenn sich widersprüchliche Anforderungen aus den diversen Vorgabe-Formaten des BSI einerseits und den Vorgaben aus den Durchführungsrechtsakten der Kommission andererseits ergeben.

Beide skizzierten Probleme ließen sich lösen, wenn sämtliche Mindestanforderungen, die die Bundesverwaltung in Bezug auf die IT-Sicherheit erfüllen muss, in den BSI-Mindeststandards ihren Niederschlag finden. Eventuelle Widersprüche zwischen BSI-Standards, IT-Grundschutzkompendium oder Durchführungsrechtsakten wären dann nicht durch alle verpflichteten Einrichtungen jeweils für sich in einem konsolidierten Anforderungskatalog aufzulösen, sondern durch das BSI als zentrale und kompetente Stelle für Informationssicherheit des Bundes. Zugleich würden die Mindeststandards dann auch praktisch zu dem zentralen Element, als das sie rechtlich bisher gedacht waren. Die Einrichtungen der Bundesverwaltungen müssten diesen zentralen Anforderungskatalog dann nur noch – ggf. unter Rückgriff auf die Hilfestellungen nach § 44 Abs. 3 BSIG-E – umsetzen. Die daraus resultierende Klarheit wäre ein entscheidender Treiber für eine zügige Umsetzung und die schnelle Etablierung eines hohen IT-Sicherheitsniveaus in der Bundesverwaltung.

Wenn die Idee des § 44 Abs. 1 BSIG-E aus der Verbändebeteiligung wieder aufgegriffen werden sollte, sollte die Regelung dafür wie folgt gefasst werden:

> *„Die Einrichtungen der Bundesverwaltung müssen Mindestanforderungen zum Schutz der in der Bundesverwaltung verarbeiteten Informationen erfüllen. Die Mindestanforderungen ergeben sich aus den Mindeststandards für die Sicherheit in der Informationstechnik*

[5] Vgl. BT.-Drs. 16/11967, S. 15 f.; Kipker/Reusch/Ritter-*Brandenburg*, Recht der Informationssicherheit, § 8 BSIG Rn. 3.

des Bundes (Mindeststandards) in den jeweils geltenden Fassungen. Die jeweils geltenden Fassungen werden auf der Internetseite des Bundesamtes veröffentlicht. Die Mindeststandards legt das Bundesamt im Benehmen mit den Ressorts und weiteren obersten Bundesbehörden fest. Es konsolidiert darin auch die Anforderungen an die Bundesverwaltung, die sich aus den BSI-Standards, dem IT-Grundschutz Kompendium (IT-Grundschutz) oder Durchführungsrechtsakten der Europäischen Kommission gemäß Artikel 21 Absatz 5 Unterabsatz 2 der NIS-2-Richtlinie ergeben. Der IT-Grundschutz und die Mindeststandards werden durch das Bundesamt regelmäßig evaluiert und entsprechend dem Stand der Technik sowie unter Berücksichtigung der Erfahrungen aus der Praxis und aus der Beratung und Unterstützung nach Absatz 3 fortentwickelt; dabei wird der Umsetzungsaufwand soweit möglich minimiert. Das Bundesamt wird den IT-Grundschutz bis zum [sechs Monate nach Inkrafttreten] modernisieren und fortentwickeln. Für die Verpflichtung nach Satz 1 gelten die Ausnahmen nach § 7 Absatz 6 und 7 entsprechend.“

Sofern die Bundesverwaltung zur Umsetzung entsprechender Standards verpflichtet wird, ist aber auch unbedingt darauf zu achten, die nötigen Ressourcen dafür zur Verfügung zu stellen. Denn Informationssicherheit wird nicht schon mit der Verabschiedung von Gesetzen geschaffen, sondern erst in der Umsetzung entsprechender Informationssicherheitsmaßnahmen. Fachgesetzgeber und Haushaltsgesetzgeber müssen hier Hand in Hand gehen und dürfen sich nicht in Widerspruch zueinander setzen.

2.9 Zu Art. 1, § 48 BSIG-E (Koordinator für Informationssicherheit)

Der Gesetzentwurf sieht in § 48 BSIG-E erstmals das Amt der Koordinatorin oder des Koordinators für Informationssicherheit vor. Das ist grundsätzlich zu begrüßen, da die Informationssicherheit für die Gewährleistung eines hohen technischen Datenschutzniveaus unerlässlich ist. Leider erschöpft sich die Regelung darin, die Benennung durch die Bundesregierung vorzusehen.

Eine klare Beschreibung der Aufgaben fehlt indes. Diese ist aus mehreren Gründen erforderlich. Zum einen ist eine klare gesetzliche Aufgabenbeschreibung nötig, um eine Grundlage für die mit den Tätigkeiten der Stelle verbundene Verarbeitung personenbezogener Daten zu schaffen. Nur wenn klar ist, welche Tätigkeiten zur Erreichung welcher Ziele wahrgenommen werden sollen, lassen sich die Erforderlichkeit bestimmen und die Zweckbindung der Daten sicherstellen. Zum anderen ist die klare Beschreibung der Aufgaben und Befugnisse aber auch notwendige Vorbedingung dafür, dass das Ziel einer zentralen Koordinierung erreicht werden kann. Ohne klare Beschreibung der Koordinatoren-Rolle wird diese im komplexen Gefüge der Bundesverwaltung nur sehr schwer Wirkung

entfalten können. Im Konzert der Informationssicherheitsakteure in der Bundesverwaltung muss für jeden Akteur klar geregelt sein, wer welche Rolle zur Erreichung der Informationssicherheit zu spielen hat.
Für die Einrichtungen und ihre Leitungen ist das in §§ 43 f. BSIG-E geregelt. Die Rolle der Informationssicherheitsbeauftragten der Einrichtungen und Ressorts werden in §§ 45 f. BSIG-E konturiert. Alleine für die Koordinierungsrolle fehlt es an der Beschreibung ihrer Stellung im System der Informationssicherheit der Bundesverwaltung und damit auch an der klaren Festlegung ihres Verhältnisses zu den übrigen Akteuren. Diese klare Festlegung der Aufgaben und damit der genauen Rolle im Gesamtsystem der Informationssicherheit der Bundesverwaltung sollte daher unbedingt im Gesetzestext ergänzt werden. Nur mit klaren Strukturen und Zuständigkeiten ist gewährleistet, dass die Informationssicherheit der Bundesverwaltung gewährleistet und kontinuierlich verbessert wird.

2.10 Zu Artikel 1, § 50 BSIG-E (Verpflichtung zur Zugangsgewährung)

§ 50 Absatz 1 BSIG-E verpflichtet Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister, auf rechtmäßige und hinreichend begründete Anträge berechtigten Zugangsnachfragern im Einklang mit dem Datenschutzrecht Zugang zu bestimmten Domain-Namen-Registrierungsdaten zu gewähren.

Der Begriff „berechtigter Zugangsnachfrager“ wird in § 2 Nr. 2 BSIG-E sehr weit legaldefiniert. Neben dem Bundesamt und den zuständigen NIS-2-Landesbehörden sollen auch Strafverfolgungsbehörden, Polizeien des Bundes und der Länder sowie die Verfassungsschutzbehörden Zugangsanfragen stellen können. Die Pflicht zur Zugangsgewährung folgt aus Art. 28 NIS 2-Richtlinie. Ausweislich des Art. 28 Abs. 1 NIS-2-Richtlinie ist das Ziel die Sicherheit, Stabilität und Resilienz des Domänennamensystems. Vor diesem Hintergrund ist unklar, warum außer bei den NIS-2-Aufsichtsbehörden von Bund und Ländern auch bei den übrigen aufgezählten Behörden die Notwendigkeit eines Zugriffs auf diese Informationen besteht, um die Anforderungen der NIS-2–Richtlinie umzusetzen. Zudem sollte gesetzlich konturiert werden, in welchen Fällen ein berechtigtes Interesse vorliegt. Dies ist sowohl im Hinblick auf die Rechtsklarheit für die Verpflichteten als auch im Hinblick auf den Schutz der informationellen Selbstbestimmung derjenigen geboten, deren Daten im Rahmen des Zugangs betroffen sind.

Zudem steht durch die kurze Frist von 72 Stunden nach Eingang einer Anfrage gemäß § 50 Absatz 1 BSIG-E zu befürchten, dass Dienstleister Anträge nur flüchtig prüfen und im Zweifel die angefragten Daten – unter Verstoß gegen die DSGVO – einmal zu viel als einmal zu wenig

herausgeben, um nicht gegen die Vorgaben der o.g. Vorschrift zu verstoßen.
Ich rege daher an, ein Mindestmaß an Verifikationsschritten in § 50 BSIG-E festzuschreiben. Insbesondere sollten nicht nur die in der Gesetzesbegründung aufgeführten Minimalkriterien aufgenommen werden, sondern auch die Voraussetzungen zur Erfüllung einer hinreichenden Begründung weiter unmittelbar im Gesetz konkretisiert werden. Diese Konkretisierung und Aufnahme in den Gesetzestext empfiehlt sich insbesondere im Hinblick auf das offensichtliche Über- und Unterordnungsverhältnis zwischen den Registries und den Zugangsnachfragern. Die in der Gesetzesbegründung aufgelisteten Kriterien zur Feststellung eines als ausreichend begründet gestellten Antrages sind nicht ausreichend, da die Registries regelmäßig nicht über die Geeignetheit, Erforderlichkeit und Angemessenheit der Registry-Daten zur Aufgabenerfüllung des Antragsstellers werden urteilen können. Effektiv reduziert sich damit die Prüfung auf eine Verifikation, ob der Antrag von einem nach § 2 Abs. 2 BSIG-E gestellten „berechtigten Zugangsnachfrager“ gestellt wurde.
Darüber hinaus empfiehlt es sich auch, notwendige Nachweispunkte für eine Überprüfung von „berechtigten Zugangsnachfrager“ in der Vorschrift zu ergänzen. Neben dem dadurch verbesserten Schutz gegen Missbrauch der Zugangsmöglichkeit erhöht dies auch die Rechtssicherheit für die Dienstleister und vermindert dadurch die dortigen Umsetzungsaufwände.

2.11 Zu Artikel 1, § 58 Absatz 4 BSIG-E (Berichtspflicht gegenüber ENISA)

Das BSI wird durch die Regelung verpflichtet, der ENISA alle drei Monate einen Bericht mit anonymisierten und aggregierten Daten zu erheblichen Sicherheitsvorfällen vorzulegen. Da der Begriff der „Anonymität“ der Sache nach zum Datenschutz gehört, sollte das Anonymisierungsverfahren im Einvernehmen mit mir erfolgen, soweit hier keine zentrale Festlegung auf europäischer Ebene erfolgt. Dazu könnte Absatz 4 um einen neuen Satz 2 ergänzt werden, der lautet:

> *„Das Anonymisierungsverfahren legt das Bundesamt im Einvernehmen mit der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit fest.“*

2.12 Zu Artikel 1, § 65 Abs. 10 BSIG-E (Bußgeldvorschriften)

Im Hinblick darauf, dass Verstöße gegen den IT-Sicherheitsvorschriften auch einen Verstoß gegen die Pflicht zum Schutz personenbezogener Daten darstellen können, sieht § 65 Abs. 11 BSIG-E vor, dass das BSI für entsprechende Sachverhalte dann kein Bußgeld verhängen darf, wenn eine Datenschutzaufsichtsbehörde bereits eines verhängt hat. Das entspricht der Regelung des Art. 35 Abs. 2 NIS-2-Richtlinie. So sollen Doppel-Bußgelder vermieden werden.

Das stellt die bisher vorgeschlagene Regelung jedoch nur unzureichend sicher, da die Datenschutzaufsichtsbehörden ihrerseits nicht daran gehindert sind, Bußgelder für Sachverhalte zu verhängen, für die das BSI dies bereits getan hat. Da eine Beschränkung der Bußgeldzuständigkeit der Datenschutzaufsichtsbehörden aufgrund der vorrangigen Geltung der DSGVO nicht möglich ist, sollte durch eine entsprechende Ausgestaltung des Bußgeldverfahrens im BSIG sichergestellt werden, dass das BSI kein Bußgeld in Fällen verhängt, in denen eine Datenschutzaufsichtsbehörde gegebenenfalls später eines verhängen möchte. Hier würde es sich etwa anbieten, das BSI in solchen Fällen zur Herstellung des Einvernehmens mit der zuständigen Datenschutzaufsichtsbehörde zu verpflichten.

Dafür könnte § 65 Abs. 11 BSIG-E um folgenden neuen Satz ergänzt werden:

> *„Das Bundesamt stellt vor Verhängung eines Bußgeldes das Einvernehmen mit der zuständigen Aufsichtsbehörde nach der Verordnung (EU) 2016/679 her.“*

2.13 Zu Art. 17, EnWG (Unterrichtung der Datenschutzaufsichtsbehörden; Verbot doppelter Bußgelder)

Die Regelungen des Art. 35 NIS-2-RL scheint der vorgelegte Entwurf im Bereich des EnWG gar nicht umzusetzen. Weder ist eine Unterrichtung der Datenschutzbehörden gem. Art. 35 NIS-2-RL vorgesehen, wie sie etwa § 7 Abs. 8 und § 61 Abs. 11 BSIG-E enthalten, noch findet sich das Verbot doppelter Bußgelder aus Art. 35 Abs. 2 NIS-2-RL im Entwurf wieder. Das führt zu einer **richtlinienwidrigen Umsetzung**. Für eine richtlinienkonforme Umsetzung sollten entsprechende Regelungen ergänzt werden.

Zur Umsetzung von Art. 35 Abs. 1 NIS-2-RL könnte § 5d EnWG-E um eine weiteren Absatz 6 zu ergänzen, der wie folgt lautet:

> *„Die Regelung des § 61 Absatz 11 des BSI-Gesetzes ist entsprechend anzuwenden.“*

Zur Umsetzung von Art. 35 Abs. 2 NIS-2-RL wird eine Ergänzung des § 95 EnWG um folgende Regelung vorgeschlagen:

> *„Die Regelung des § 65 Absatz 11 des BSI-Gesetzes ist entsprechend anzuwenden.“*

2.14 Zu Art. 25, TKG-E (Unterrichtung der Datenschutzaufsichtsbehörden; Verbot doppelter Bußgelder)

Im Bereich des TKG-E sind die zwingenden Vorgaben des Art. 35 der NIS-2-Richtline ebenfalls nicht umgesetzt, was zur **Richtlinienwidrigkeit** führt.

Zur Umsetzung des Art. 35 Abs. 1 NIS 2 könnte folgender Satz 2 in § 165 Abs. 10 TKG ergänzt werden:

> *„Stellt die Bundesnetzagentur im Zuge der Beaufsichtigung einer Einrichtung oder Durchsetzung einer Maßnahme fest, dass ein Verstoß gegen die Verpflichtungen dieses Gesetzes eine offensichtliche Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Nummer 12 der Verordnung (EU) 2016/679 zur Folge hat, die gemäß Artikel 33 dieser Verordnung zu melden ist, unterrichtet es unverzüglich die zuständige Aufsichtsbehörde.“*

Losgelöst von den europarechtlichen Anforderungen aus Art. 35 Abs. 2 NIS-2-RL stellt sich das Problem doppelter Bußgelder im Bereich des TKG im aktuellen Entwurf nur deswegen nicht, weil die zur Umsetzung des Art. 34 Abs. 2 NIS-2-RL notwendigen Bußgeldtatbestände zwar in § 65 BSIG-E und § 95 EnWG umgesetzt wurden, aber nicht im TKG. Auch die Bußgeldobergrenzen wurden nicht an die Anforderungen des Art. 34 Abs. 4 und 5 NIS-2-RL angepasst. Wenn die notwendigen Bußgeldregelungen ergänzt werden, ist auch an die Übernahme des Doppelbestrafungsverbots aus Art. 35 Abs. 2 NIS-2-RL zu denken.

Um die Konformität mit Art. 35 Abs. 2 NIS-2-RL herzustellen, könnte ein neuer Abs. 8a in § 228 TKG ergänzt werden, der wie folgt gefasst ist:

> *„§ 65 Absatz 11 des BSI-Gesetzes ist entsprechend anzuwenden.“*

2.15 Zu Art. 1, § 2 BSIG-E (Begriffsbestimmung)

Der Gesetzentwurf verwendet in vielen neuen Bestimmungen den Begriff „Risiko“. Der Begriff wird jedoch nur in der Gesetzesbegründung näher konkretisiert aber nicht legaldefiniert. Der veröffentlichte Referentenentwurf für das KRITIS-Dach-Gesetz[6] sieht eine entsprechende Legaldefinition vor. Da beide Gesetzgebungsvorhaben eng verzahnt sind, sollten sie beide dem gleichen Regelungsansatz folgen. Wenn die Legaldefinition im KRITIS-DachG erhalten bleibt, sollte der Begriff des Risikos also auch in § 2 BSIG-E legaldefiniert werden.

2.16 Zu Art. 1, Fehlende Berücksichtigung der besonderen Stellung der BfDI

Der Gesetzentwurf berücksichtigt an einer Reihe von Punkten nicht die besondere Stellung, die der oder dem BfDI aus unionsrechtlichen Gründen und im organisatorischen Gefüge der Bundesverwaltung innehat.

---

[6] https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/KM4/Kritis-Dachgesetz.pdf

2.16.1 Zu Art. 1, § 2 Nr. 21 BSIG-E (Kommunikationstechnik des Bundes) sowie § 44 Abs. 1 S. 4 BSIG-E (Mindeststandards)

So wird in § 2 Nr. 21 BSIG-E der Begriff der Kommunikationstechnik des Bundes definiert. Vom Begriff ausgenommen sind eine Reihe von Einrichtungen, die qua Gesetz eine besondere Unabhängigkeit besitzen. Dazu gehören seit Einführung des Begriffs im BSIG z.B. der Deutsche Bundestag und der Bundesrechnungshof. Im Rahmen der Änderungen durch das 2. IT-Sicherheitsgesetz wurde auch das Bundesverfassungsgericht in die Aufzählung aufgenommen, um seiner Sonderstellung gerecht zu werden.

Die oder der BfDI, deren bzw. dessen Unabhängigkeit aufgrund von europäischem Primärrecht aus Art. 16 Abs. 2 S. 2 AEUV sowie einfachem europäischem Recht nach Art. 52 DSGVO zwingend zu beachten ist, fehlt in der Reihe der vorgenannten Einrichtungen. Wenn die Unabhängigkeit der Einrichtungen für die Definition relevant ist, gebietet es der Grundsatz der effektiven Umsetzung europäischen Rechts, auch die mit europarechtlich fundierter Unabhängigkeit ausgestatteten Einrichtungen in dieser Aufzählung zu ergänzen. Dafür könnte § 2 Nr. 21 letzter Hs. wie folgt gefasst werden:

> *„nicht als „Kommunikationstechnik des Bundes“ gelten die Kommunikationstechnik des Bundesverfassungsgerichts, der Bundesgerichte, soweit sie nicht öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen, des Bundestages, des Bundesrates, des Bundespräsidenten, des Bundesrechnungshofes und der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, soweit sie ausschließlich in deren eigener Zuständigkeit betrieben wird“*

Ähnlich verhält es sich mit der Ausnahmeregelung in § 44 Abs. 1 S. 4 BSIG-E, die auf den § 2 Nr. 21 BSIG-E verweist und Gerichte und Verfassungsorgane aufgrund ihrer unabhängigen Stellung von der Umsetzung der Mindeststandards ausnimmt. Wenn man eine solche Ausnahme für unabhängige Stellen vorsehen möchte, gebietet es die effektive Umsetzung der europarechtlichen Vorgaben zur Unabhängigkeit der Datenschutzaufsichtsbehörden, Maßnahmen zur Absicherung der Unabhängigkeit nicht nur für solche Einrichtungen vorzusehen, die nach nationalem Recht unabhängig zu stellen sind. Sofern die Ausnahme in § 44 Abs. 1 S. 4 BSIG-E also beibehalten werden soll, sollte sie wie folgt gefasst werden:

> *„Für die in § 2 Nummer 21 genannten Gerichte, Verfassungsorgane und die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit haben die Vorschriften nach Satz 1 empfehlenden Charakter.“*

2.16.2 Zu Artikel 1, § 44 Abs. 6 BSIG-E (Festlegungskompetenz des BMI zur Verwendung bestimmter IT-Sicherheitsprodukte)

Nach § 44 Abs. 6 BSIG-E darf das BMI festlegen, dass die Einrichtungen der Bundesverwaltung bestimmte vom BSI bereitgestellte IT-Sicherheitsprodukte abrufen müssen und Eigenbeschaffungen unzulässig sind. Für diese Festlegung ist die Herstellung des Einvernehmens mit den anderen Ressorts vorgesehen.

Oberste Bundesbehörden, die wie meine Behörde kein Ressort sind, würden zwar den Festlegungen des BMI unterworfen, hätten nach dem aktuellen Stand des Entwurfes aber kein Mitspracherecht. Zudem sieht die Regelung für bestimmte Einrichtungen – wie z.B. Gerichte –, die für ihre Aufgabenerfüllung eine gesetzlich garantierte Unabhängigkeit genießen, eine Ausnahme von der Verpflichtung vor. Die BfDI als unabhängige Behörde wird dagegen nicht erwähnt.

Insgesamt wird damit die BfDI sowohl gegenüber den Ressorts als auch den anderen unabhängigen Einrichtungen benachteiligt, ohne dass dies sachlich gerechtfertigt wird. Um dem Status der BfDI als unabhängige Behörde hinreichend Rechnung zu tragen, sind zwei Varianten denkbar. Zum einen könnte vorgesehen werden, dass das BMI auch mit ihr bzw. ihm das Einvernehmen für die Festlegung herstellen muss. Alternativ könnte sie bzw. er wie in den anderen Regelungen neben den unabhängigen Gerichten und Verfassungsorganen von der Bindungswirkung des § 44 Abs. 6 S. 1 und 2 BSIG-E ausgenommen werden. Solange eine Ausnahme für andere unabhängige Einrichtungen vorgesehen ist, erscheint die Ergänzung der oder des BfDI in deren Aufzählung systematisch sinnvoller. § 44 Abs. 6 BSIG-E wäre dann wir folgt zu fassen:

> *„Dies gilt nicht für die in § 2 Nummer 21 genannten Gerichte, Verfassungsorgane, die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sowie die Auslandsinformations- und -kommunikationstechnik gemäß § 7 Absatz 6.“*

2.16.3 Zu Art. 1, § 46 BSIG-E (Ressort-IT-Sicherheitsbeauftragte)

In § 46 Abs. 1 BSIG-E ist die Pflicht zur Benennung von Informationssicherheitsbeauftragten der Ressorts vorgesehen. Diese Pflicht besteht neben der Pflicht zur Benennung von Informationssicherheitsbeauftragten der Einrichtungen der Bundesverwaltung nach § 45 BSIG-E. Ressorts und „weitere“ oberste Bundesbehörden müssen also grundsätzlich zwei unterschiedliche Informationssicherheitsbeauftragten-Rollen schaffen: Die der Einrichtungen und die der Ressorts. Das ergibt dort Sinn, wo es einen behördlichen Unterbau eines Ressorts oder einer obersten

Bundesbehörde gibt, da die Ressort-Informationssicherheitsbeauftragten bestimmte Aufgaben im Hinblick auf die untergeordneten Behörden ausüben. Für oberste Bundesbehörden ohne untergeordnete Behörden ist die Schaffung einer eigenen Rolle des Ressort-Informationssicherheitsbeauftragten nicht sinnvoll. Vielmehr sollten dessen Aufgaben und Befugnisse stattdessen durch den Informationssicherheitsbeauftragten der Einrichtung wahrgenommen werden. Diese Möglichkeit sollte im Gesetz klargestellt werden.
Dazu sollte ein § 46 Abs. 7 BSIG-E mit folgendem Inhalt ergänzt werden:

> *Die Regelungen der Absätze 1 bis 3 und Absatz 6 finden keine Anwendung auf oberste Bundesbehörden ohne Geschäftsbereich. Die Absätze 4 und 5 finden für sie mit der Maßgabe Anwendung, dass statt der Informationssicherheitsbeauftragten oder des Informationssicherheitsbeauftragten des Ressorts, die der Einrichtung zuständig sind.*

****