Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)529

BfDI | Postfach 1468 | 53004 Bonn

Deutscher Bundestag
Ausschuss für Inneres und Heimat
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.: **25-170/024#1249**
Dok.: 100056/2024

Anlage:

Bonn, 04. November 2024

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie (BT-Drs. 20/13184)

Sehr geehrte Damen und Herren,

der von der Bundesministerin des Innern und für Heimat 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

Prof. Dr. Louisa Specht-Riemenschneider

Stellungnahme

der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

zur öffentlichen Anhörung des Ausschusses für Inneres und Heimat

am 04.11.2024

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. 20/13184

Einleitung

1.1 Datenschutz und Datensicherheit gehen Hand in Hand

IT-Sicherheit und Datenschutz sind unmittelbar miteinander verzahnt. Ziele der IT-Sicherheit sind dabei 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. Durch die durch die NIS 2-Richtlinie erfasste, deutlich erhöhte Anzahl an verpflichteten Unternehmen, wird die enge Zusammenarbeit des Bundesamts für Sicherheit in der Informationstechnik (BSI) und der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) in Zukunft noch weiter an Bedeutung gewinnen.

1.2 Grundrechte schützen

Mit der Sicherstellung der Cyber- und Informationssicherheit sind zahlreiche Eingriffsrechte verknüpft. Nicht nur das Recht 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, BSI-Gesetz-E, Umgang mit Schwachstellen

Bereits im Rahmen der Ressortabstimmungen dieses Gesetzentwurfes und in früheren öffentlichen Anhörungen des Bundestages[1] hat mein Haus 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. Leider findet sich dazu im vorliegenden Entwurf nichts, obwohl die Bundesregierung sich im Koalitionsvertrag für diese Legislaturperiode diesbezüglich klare Ziele gesetzt hatte. Insbesondere die Schließung von Schwachstellen ist 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.

[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.

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.
Dennoch bleibt im Entwurf 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. 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 gezeigt hat.
Aus technischer Sicht besteht keine Erforderlichkeit, Schwachstellen aufrechtzuerhalten, um Sicherheits- und Strafverfolgungsbehörden Zugriff zu ermöglichen. Ein unregulierter Zugriff über Schwachstellen kann stets Kollateralschäden nach sich ziehen und schadet dem Vertrauen der Bürgerinnen und Bürger in digitale Infrastrukturen und Dienste. Zudem wird das Produkt 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.
In einer digitalen Gesellschaft muss das Vertrauen der Bürgerinnen und Bürger sowie der Unternehmen in die Sicherheit der verwendeten Informationstechnik gestärkt werden. Hat das BMI sowohl die Aufsicht über das BSI, das Sicherheitslücken schließen soll, als auch über weitere Geschäftsbereichsbehörden mit Sicherheitsaufgaben, die ein Interesse am Offenhalten von Schwachstellen haben können, erwächst für die Aufsicht ein Zielkonflikt, der das öffentliche Vertrauen erschüttern kann. Dieser Zielkonflikt ist meines Erachtens – im Interesse des öffentlichen Vertrauens in die IT-Sicherheit der genutzten Geräte und Dienste – durch den parlamentarischen Gesetzgeber durch eine klare gesetzliche Regelung aufzulösen. Durch Parlamentsgesetz ist daher dem BSI ein zweifelsfreies Mandat zur Sicherung und erforderlichenfalls Herstellung von IT-Sicherheit zu erteilen. Dafür muss im BSIG klargestellt werden, dass das BSI Schwachstellen niemals zurückhält, sondern stets auf ihre Schließung hinwirkt und nicht durch anderslautende Weisungen davon abgehalten werden darf. Eine entsprechende Regelung könnte etwa im Zusammenhang mit den Aufgaben des BSI als allgemeine Meldestelle in § 5 BSIG-E verortet werden. Die bisher enthaltenen pauschalen Hinweise auf „Dritte“ in § 5 Abs. 3 Nr. 1 BSIG-E sind nicht ausreichend, um eine Information des Herstellers sicherzustellen. Zudem ist auch in dieser Norm die Information nicht verpflichtend, sondern unzureichend als nur als Soll-Vorschrift formuliert.

2.2. Zu Artikel 1, § 7 Abs. 8 und § 61 Abs. 11 BSIG-E und Art. 26 (Unterrichtungspflichten bei Datenschutzverstößen)

Das BSI soll auch künftig die Sicherheit der Kommunikationstechnik des Bundes bei anderen Einrichtungen kontrollieren können. Wenn es bei diesen Kontrollen Verstöße gegen die Pflichten nach dem BSIG feststellt, soll es gemäß § 7 Abs. 8 BSIG-E auch die zuständige Datenschutzaufsichtsbehörde informieren, sofern damit eine *offensichtliche* Verletzung des Schutzes personenbezogener Daten verbunden ist. Damit bleibt die Regelung hinter den Vorgaben des Artikel 35 der NIS-2-Richtlinie zurück, die eine Unterrichtung der Datenschutzaufsichtsbehörden bereits dann vorschreiben, wenn Verstöße eine Verletzung des Schutzes personenbezogener Daten haben *können*.
Auch bei der allgemeinen Aufsichtsregelung für besonders wichtige Einrichtung in § 61 BSIG-E sieht deren Abs. 11 die Unterrichtung der Datenschutzaufsichtsbehörde nur für offensichtliche Fälle vor, obwohl die NIS-2-Richtlinie dies schon bei der Möglichkeit der Verletzung des Schutzes personenbezogener Daten vorsieht.
In beiden Fällen muss daher die Unterrichtungspflicht richtlinienkonform angepasst werden, um eine europarechtswidrige Umsetzung der Regelungen des Art. 35 NIS-2-Richtlinie zu vermeiden.

§ 7 Abs. 8 BSIG-E wäre demnach wie folgt zu fassen:

Stellt das Bundesamt im Rahmen seiner Kontrollen fest, dass ein Verstoß gegen die Verpflichtungen dieses Gesetzes eine Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Nummer 12 der Verordnung (EU) 2016/679 zur Folge haben kann, die gemäß Artikel 33 dieser Verordnung zu melden ist, so unterrichtet es unverzüglich die zuständigen Aufsichtsbehörden.

§ 61 Abs. 11 BSIG-E müsste wie folgt gefasst werden:

Stellt das Bundesamt im Zuge der Beaufsichtigung einer Einrichtung oder Durchsetzung einer Maßnahme fest, dass ein Verstoß gegen die Verpflichtungen dieses Gesetzes eine Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Nummer 12 der Verordnung (EU) 2016/679 zur Folge haben kann, die gemäß Artikel 33 dieser Verordnung zu melden ist, unterrichtet es unverzüglich die zuständigen Aufsichtsbehörden.

Da entsprechende Unterrichtungspflichten im Bereich des TKG bisher gar nicht vorgesehen sind, müssten sie dort für eine richtlinienkonforme Umsetzung des Art. 35 NIS-2-Richtlinie ebenfalls vorgesehen werden.

2.3. 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 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.

2.4. 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, das 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,

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

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 aus § 15 BSIG-E wissen, wem das System zuzuordnen ist. Aufgrund der umfassenden Registrierungspflichten 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 meine Behörde vorgesehen ist. Der jetzt gewählte Weg über Kontrollmöglichkeiten für meine Behörde 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 in der Datenschutz-Grundverordnung verankerten 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 nicht möglich ist, sollte im Umsetzungsgesetz zumindest eine Evaluierungsklausel für diese Regelungen vorgesehen werden.

2.6. 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 die BfDI kein Ressort sind, würden zwar der Festlegung 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 das Einvernehmen für die Festlegung herstellen muss. Alternativ könnte sie neben den unabhängigen Gerichten und Verfassungsorganen von der Bindungswirkung des § 44 Abs. 6 S. 1 und 2 BSIG-E ausgenommen werden.

2.7. Zu Artikel 1, § 46 BSIG-E (Ressort-Informationssicherheitsbeauftragte)

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 macht auch 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 des Ressorts, die der Einrichtung zuständig sind.

2.8. 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 jedoch weder in der NIS-2-Richtlinie, noch in § 2 BSIG-E (legal)definiert. Es sollte daher eine Definition mit hinreichend klaren und abschließende Kriterien an einen „berechtigten Zugangsnachfrager“ in § 2 BSIG-E aufgenommen werden. Neben Behörden, die die o.g. Angaben im Rahmen ihres gesetzlichen Tätigwerdens benötigen (beispielsweise im Zusammenhang mit datenschutzrechtliche Beschwerden oder strafrechtlichen Ermittlungen), sollte der Kreis von weiteren berechtigten Zugangsnachfragern möglichst eingeschränkt werden. Denn anderenfalls droht, dass personenbezogene Daten von Domain-Inhabern missbräuchlich angefragt und verwendet werden könnten.

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. Darüber hinaus empfiehlt es sich auch, notwenige 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.

2.9. 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“ von Daten der Sache nach auch datenschutzrechtlicher Natur ist, sollte das Anonymisierungsverfahren im Einvernehmen mit meinem Haus 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.“

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

Im Hinblick darauf, dass Verstöße gegen IT-Sicherheitsvorschriften auch einen Verstoß gegen die Pflicht zum Schutz personenbezogener Daten darstellen können, sieht § 65 Abs. 10 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, jedenfalls des Benehmens mit der zuständigen Datenschutzaufsichtsbehörde zu verpflichten.

2.11. Zu Art. 1, § 3 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 sieht für das KRITIS-Dach-Gesetz[3] eine entsprechende Legaldefinition vor. Da beide Gesetzgebungsvorhaben eng verzahnt sind, sollten beide konsistent dem gleichen Regelungsansatz folgen. Wenn die Legaldefinition im KRITIS-DachG erhalten bleibt, sollte der Begriff des Risikos also auch in § 3 BSIG-E legaldefiniert werden.

---

3 https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/KM4/KRITIS-DachG-2.pdf