Referentenentwurf

des Bundesministeriums des Innern und Heimat

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz - NIS2UmsuCG)

A. Problem und Ziel

Am 13. Januar 2023 trat die Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (ABl. L 333 vom 27. Dezember 2022, S. 80, im Folgenden NIS-2-Richtlinie) in Kraft.

Mit der NIS-2-Richtlinie wurden Maßnahmen festgelegt, mit denen in der gesamten Union ein hohes gemeinsames Cybersicherheitsniveau sichergestellt werden soll, um so das Funktionieren des Binnenmarkts zu verbessern. Zu diesem Zweck wird in der NIS-2-Richtlinie die Pflicht für alle Mitgliedstaaten festgelegt, nationale Cybersicherheitsstrategien zu verabschieden sowie zuständige nationale Behörden, Behörden für das Cyberkrisenmanagement, zentrale Anlaufstellen für Cybersicherheit (zentrale Anlaufstellen) und Computer-Notfallteams (CSIRT) zu benennen oder einzurichten. Ferner werden Pflichten in Bezug auf das Cybersicherheitsrisikomanagement sowie Berichtspflichten für Einrichtungen der in den Anhang I oder II der NIS-2-Richtlinie aufgeführten Arten sowie für Einrichtungen, die nach Richtlinie (EU) 2022/2557 als kritische Einrichtungen eingestuft wurden festgelegt. Des Weiteren sieht die NIS-2-Richtlinie Vorschriften und Pflichten zum Austausch von Cybersicherheitsinformationen sowie Aufsichts- und Durchsetzungspflichten für die Mitgliedstaaten vor.

Für das Informationssicherheitsmanagement in der Bundesverwaltung haben sich die bisherigen Steuerungsinstrumente auf überwiegend untergesetzlicher Basis als nicht ausreichend effektiv erwiesen, um eine flächendeckende wirksame Steigerung des Sicherheitsniveaus zu erreichen. Dies haben insbesondere Sachstandserhebungen zum Umsetzungsplan Bund sowie Prüfungen des BRH bestätigt. Vor dem Hintergrund der durch aktuelle geopolitische Entwicklungen („Zeitenwende“) abermals verschärften Bedrohungslage hat sich das Risiko für staatliche Einrichtungen zudem weiter erhöht, durch Gefährdungen aus dem Cyberraum in ihrer Handlungsfähigkeit eingeschränkt zu werden.

B. Lösung

Entsprechend der unionsrechtlichen Vorgaben wird der mit dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 (BGBl. I 2015 S. 1324) und dem Zweiten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) vom 18. Mai 2021 (BGBl. I 2021, S. 1122) geschaffene Ordnungsrahmen durch das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) erweitert. Schwerpunktmäßig werden folgende Änderungen vorgenommen:

- Einführung der durch die NIS-2-Richtlinie vorgegebenen Einrichtungskategorien der mit einer signifikanten Ausweitung des bisher auf Betreiber Kritischer Infrastrukturen, Anbieter digitaler Dienste und Unternehmen im besonderen öffentlichen Interesse beschränkten Anwendungsbereichs einhergeht.

- Der Katalog der Mindestsicherheitsanforderungen des Art. 21 Abs. 2 NIS-2-Richtlinie wird in das BSIG übernommen, wobei in der Intensität der jeweiligen Maßnahme aus Gründen der Verhältnismäßigkeit zwischen den Kategorien ausdifferenziert wird.
- Die bislang einstufige Meldepflicht bei Vorfällen wird durch das dreistufige Melderegime der NIS-2-Richtlinie ersetzt. Dabei soll der bürokratischen Aufwand für die Einrichtungen im Rahmen des Umsetzungsspielraums minimiert werden.
- Ausweitung des BSI Instrumentariums im Hinblick auf von der NIS-2-Richtlinie vorgegebenen Aufsichtsmaßnahmen.
- Gesetzliche Verankerung wesentlicher nationaler Anforderungen an das Informationssicherheitsmanagement des Bundes und Abbildung der zugehörigen Rollen und Verantwortlichkeiten.
- Harmonisierung der Anforderungen an Einrichtungen der Bundesverwaltung aus nationalen und unionsrechtlichen Vorgaben, um ein insgesamt kohärentes und handhabbares Regelungsregime zu gewährleisten.
- Etablierung eines CISO Bund als zentralem Koordinator für Maßnahmen zur Informationssicherheit in Einrichtungen der Bundesverwaltung und zur Unterstützung der Ressorts bei der Umsetzung der Vorgaben für das Informationssicherheitsmanagement.
- Überarbeitung des Bußgeldregimes und entsprechende Differenzierung anhand der Einrichtungskategorien.
- Schaffung einer übersichtlicheren Struktur des BSIG mit neuer Gliederung.

C. Alternativen

Keine.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Es entsteht kein Erfüllungsaufwand für die Bürgerinnen und Bürger.

E.2 Erfüllungsaufwand für die Wirtschaft

[*Anm. BMI CI1 – Das Statistische Bundesamt (StBA) hatte nach inhaltlicher Finalisierung der NIS-2-Richtlinie eine Folgekostenschätzung erstellt. Diese wird nun unter Zugrundelegung des Referentenentwurfs plausibilisiert und die ausstehenden Angaben werden nachgetragen. Bei den in eckigen Klammern gesetzten Beträgen handelt es sich um die Ergebnisse der damaligen Schätzung.*]

Der Wirtschaft entsteht für die Erfüllung der im Gesetz vorgesehenen zusätzlichen Aufgaben ein laufender Erfüllungsaufwand in Höhe von [1,65 Mrd.] Euro. Davon entfallen [●] Euro auf jährliche Personalkosten und rund [●] Euro auf jährliche Sachkosten. Bürokratiekosten durch Informationspflichten sind davon [●] Euro. Der einmalige Erfüllungsaufwand in Form von eimaligen Personalkosten beläuft sich auf [1,37 Mrd.] Euro.

E.3 Erfüllungsaufwand der Verwaltung

[*Anm. BMI CI1 – Die Erfüllungsaufwände für die Verwaltung sollen hinsichtlich BMI und BMI-Geschäftsbereichsbehörden in der Hausabstimmung und hinsichtlich BKAmt und den Ressorts im Übrigen in der Ressortabstimmung abgefragt werden.*]

Der Verwaltung entsteht für die Erfüllung der im Gesetz vorgesehenen zusätzlichen Aufgaben insgesamt ein Aufwand von insgesamt [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit einem jährlichen Erfüllungsaufwand in Höhe von [●] Euro. Davon entfallen [●] Euro auf jährliche Personalkosten und [●] Euro auf jährliche Sachkosten. Durch die gesetzliche Änderung entstehen einmalige Sachkosten in Höhe von [●] Euro.

Davon entfallen auf:

- das Bundeskanzleramt (BKAmt) einschließlich seines Geschäftsbereichs [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit einem jährlichen Erfüllungsaufwand in Höhe von [●] Euro. Davon entfallen [●] Euro auf jährliche Personalkosten und [●] Euro auf jährliche Sachkosten.
- das Bundesministerium für Wirtschaft und Klimaschutz (BMWK) einschließlich seines Geschäftsbereichs [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit einem jährlichen Erfüllungsaufwand in Höhe von [●] Euro. Davon entfallen [●] Euro auf jährliche Personalkosten und [●] Euro auf jährliche Sachkosten;
- das Bundesministerium der Finanzen (BMF) einschließlich seines Geschäftsbereichs [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit einem jährlichen Erfüllungsaufwand in Höhe von [●] Euro. Davon entfallen [●] Euro auf jährliche Personalkosten und [●] Euro auf jährliche Sachkosten;
- das Bundesministerium des Innern und für Heimat (BMI) einschließlich seines Geschäftsbereichs [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit einem jährlichen Erfüllungsaufwand in Höhe von [●] Euro. Davon entfallen [●] Euro auf jährliche Personalkosten und [●] Euro auf jährliche Sachkosten. Durch die gesetzliche Änderung entstehen einmalige Sachkosten in Höhe von [●] Euro;
- das Auswärtige Amt (AA) einschließlich seines Geschäftsbereichs insgesamt [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit einem jährlichen Erfüllungsaufwand in Höhe von [●] Euro. Davon entfallen [●] Euro auf jährliche Personalkosten und [●] Euro auf jährliche Sachkosten. Zusätzlich entstehen einmalig Sachkosten in Höhe von [●] Euro;
- das Bundesministerium der Justiz (BMJ) einschließlich seines Geschäftsbereichs insgesamt [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit einem jährlichen Erfüllungsaufwand in Höhe von [●] Euro. Davon entfallen [●] Euro auf jährliche Personalkosten und [●] Euro auf jährliche Sachkosten. Zusätzlich entstehen einmalig Sachkosten in Höhe von [●] Euro;
- das Bundesministerium für Arbeit und Soziales (BMAS) einschließlich seines Geschäftsbereichs [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit einem jährlichen Erfüllungsaufwand in Höhe von [●] Euro. Davon entfallen [●] Euro auf jährliche Personalkosten und [●] Euro auf jährliche Sachkosten;
- das Bundesministerium der Verteidigung (BMVg) einschließlich seines Geschäftsbereichs [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit einem jährlichen Erfüllungsaufwand in Höhe von [●] Euro. Davon entfallen [●] Euro auf jährliche Personalkosten und [●] Euro auf jährliche Sachkosten;
- das Bundesministerium für Ernährung und Landwirtschaft (BMEL) einschließlich seines Geschäftsbereichs [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit einem jährlichen Erfüllungsaufwand in Höhe von [●] Euro. Davon entfallen [●] Euro auf jährliche Personalkosten und [●] Euro auf jährliche Sachkosten;
- das Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ) einschließlich seines Geschäftsbereichs [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit einem jährlichen Erfüllungsaufwand in Höhe von [●] Euro. Davon entfallen [●] Euro auf jährliche Personalkosten und [●] Euro auf jährliche Sachkosten;
- das Bundesministerium für Gesundheit (BMG) einschließlich seines Geschäftsbereichs [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit einem jährlichen Erfüllungsaufwand in Höhe von [●] Euro. Davon entfallen [●] Euro auf jährliche Personalkosten und [●] Euro auf jährliche Sachkosten;
- das Bundesministerium für Digitales und Verkehr (BMDV) einschließlich seines Geschäftsbereichs [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit einem jährlichen Erfüllungsaufwand in Höhe von [●] Euro. Davon entfallen [●] Euro auf jährliche Personalkosten und [●] Euro auf jährliche Sachkosten;
- das Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV) einschließlich seines Geschäftsbereichs [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit einem

jährlichen Erfüllungsaufwand in Höhe von [●] Euro. Davon entfallen [●] Euro auf jährliche Personalkosten und [●] Euro auf jährliche Sachkosten;

- das Bundesministerium für Bildung und Forschung (BMBF) einschließlich seines Geschäftsbereichs [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit einem jährlichen Erfüllungsaufwand in Höhe von [●] Euro. Davon entfallen [●] Euro auf jährliche Personalkosten und [●] Euro auf jährliche Sachkosten;
- das Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (BMZ) einschließlich seines Geschäftsbereichs [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit einem jährlichen Erfüllungsaufwand in Höhe von [●] Euro. Davon entfallen [●] Euro auf jährliche Personalkosten und [●] Euro auf jährliche Sachkosten;
- das Bundesministerium für Wohnen, Stadtentwicklung und Bauwesen (BMWSB) einschließlich seines Geschäftsbereichs [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit einem jährlichen Erfüllungsaufwand in Höhe von [●] Euro. Davon entfallen [●] Euro auf jährliche Personalkosten und [●] Euro auf jährliche Sachkosten; und
- den Bundesbeauftragten für den Datenschutz und für die Informationsfreiheit (BfDI) [●] Planstellen/Stellen ([●] hD; [●] gD) mit einem jährlichen Erfüllungsaufwand in Höhe von [●] Euro. Davon entfallen [●] Euro auf jährliche Personalkosten und [●] Euro auf jährliche Sachkosten.

Der Bedarf an Sach- und Personalmitteln sowie Planstellen und Stellen wird finanziell und stellenmäßig in den jeweiligen Einzelplänen ausgeglichen.

F. Weitere Kosten

Keine

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG)[1]

Vom ...

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
0		**Artikel 1** **Änderung des BSI-Gesetzes**	
1	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG)[2]	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Betreibern und Einrichtungen (BSI-Gesetz – BSIG)	Berücksichtigung des Umstands, dass es sich nicht mehr um ein reines Errichtungsgesetz einer Bundesbehörde handelt.
2	Nichtamtliches Inhaltsverzeichnis § 1 Bundesamt für Sicherheit in der Informationstechnik § 2 Begriffsbestimmungen § 3 Aufgaben des Bundesamtes § 3a Verarbeitung personenbezogener Daten § 4 Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes	Inhaltsübersicht Teil 1 Allgemeine Vorschriften § 1 Bundesamt für Sicherheit in der Informationstechnik § 2 Begriffsbestimmungen Teil 2 Das Bundesamt	Schaffung einer (amtlichen) Inhaltsübersicht aufgrund des gestiegenen Umfangs des Gesetzes sowie Strukturierung des Gesetzes in Teile (und Kapitel) zur besseren Übersicht für den Rechtsanwender.

[1] Dieses Gesetz dient der Umsetzung der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (ABl. L 333 vom 27.12.2022, S. 80).

[2] BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 12 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982) geändert worden ist.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	§ 4a Kontrolle der Kommunikationstechnik des Bundes, Betretensrechte § 4b Allgemeine Meldestelle für die Sicherheit in der Informationstechnik § 5 Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes § 5a Verarbeitung behördeninterner Protokollierungsdaten § 5b Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen § 5c Bestandsdatenauskunft § 6 Beschränkungen der Rechte der betroffenen Person § 6a Informationspflicht bei Erhebung von personenbezogenen Daten § 6b Auskunftsrecht der betroffenen Person § 6c Recht auf Berichtigung § 6d Recht auf Löschung § 6e Recht auf Einschränkung der Verarbeitung § 6f Widerspruchsrecht § 7 Warnungen § 7a Untersuchung der Sicherheit in der Informationstechnik § 7b Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden § 7c Anordnungen des Bundesamtes gegenüber Diensteanbietern § 7d Anordnungen des Bundesamtes gegenüber Anbietern von Telemediendiensten § 8 Vorgaben des Bundesamtes	Kapitel 1 Aufgaben und Befugnisse § 3 Aufgaben des Bundesamtes § 4 Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes § 5 Allgemeine Meldestelle für die Sicherheit in der Informationstechnik § 6 Informationsaustausch § 7 Kontrolle der Kommunikationstechnik des Bundes, Betretensrechte § 8 Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes § 9 Verarbeitung von Protokollierungsdaten der Kommunikationstechnik des Bundes § 10 Anordnungen von Maßnahmen zur Verhütung oder Behebung von Sicherheitsvorfällen § 11 Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen § 12 Bestandsdatenauskunft § 13 Warnungen § 14 Untersuchung der Sicherheit in der Informationstechnik § 15 Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden § 16 Anordnungen des Bundesamtes gegenüber Diensteanbietern § 17 Anordnungen des Bundesamtes gegenüber Anbietern von Telemediendiensten § 18 Anordnungen des Bundesamtes gegenüber Herstellern von IKT-Produkten	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen § 8b Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen § 8c Besondere Anforderungen an Anbieter digitaler Dienste § 8d Anwendungsbereich § 8e Auskunftsverlangen § 8f Sicherheit in der Informationstechnik bei Unternehmen im besonderen öffentlichen Interesse § 9 Zertifizierung § 9a Nationale Behörde für die Cybersicherheitszertifizierung § 9b Untersagung des Einsatzes kritischer Komponenten § 9c Freiwilliges IT-Sicherheitskennzeichen § 10 Ermächtigung zum Erlass von Rechtsverordnungen § 11 Einschränkung von Grundrechten § 12 Rat der IT-Beauftragten der Bundesregierung § 13 Berichtspflichten § 14 Bußgeldvorschriften § 14a Institutionen der Sozialen Sicherung § 15 Anwendbarkeit der Vorschriften für Anbieter digitaler Dienste	§ 19 Bereitstellung von IT-Sicherheitsprodukten Kapitel 2 Datenverarbeitungen § 20 Verarbeitung personenbezogener Daten § 21 Beschränkungen der Rechte der betroffenen Person § 22 Informationspflicht bei Erhebung von personenbezogenen Daten § 23 Auskunftsrecht der betroffenen Person § 24 Recht auf Berichtigung § 25 Recht auf Löschung § 26 Recht auf Einschränkung der Verarbeitung § 27 Widerspruchsrecht Teil 3 Sicherheit in der Informationstechnik von Betreibern und Einrichtungen Kapitel 1 Anwendungsbereich § 28 Anwendungsbereich, Betreiber kritischer Anlagen, besonders wichtige Einrichtungen und wichtige Einrichtungen § 29 Einrichtungen der Bundesverwaltung Kapitel 2 Risikomanagement, Melde-, Registrierungs-, Nachweis- und Unterrichtungspflichten § 30 Risikomanagementmaßnahmen § 31 Meldepflichten § 32 Registrierungspflicht § 33 Besondere Registrierungspflicht für Anbieter digitaler Dienste	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		§ 34 Nachweispflichten für besonders wichtige Einrichtungen § 35 Unterrichtungspflichten § 36 Rückmeldungen des Bundesamts gegenüber meldenden Einrichtungen; Information der Öffentlichkeit § 37 Ausnahmebescheid § 38 Billigungs- und Überwachungspflicht für Leitungsorgane von Wesentlichen Einrichtungen und Wichtigen Einrichtungen; Schulungen § 39 Zusätzliche Anforderungen an Kritische Einrichtungen § 40 Zentrale Melde- und Anlaufstelle § 41 Untersagung des Einsatzes kritischer Komponenten § 42 Auskunftsverlangen Kapitel 3 Sicherheit in der Informationstechnik von Einrichtungen der Bundesverwaltung § 43 Informationssicherheitsmanagement § 44 Vorgaben des Bundesamtes § 45 Informationssicherheitsbeauftragte der Einrichtungen der Bundesverwaltung § 46 Informationssicherheitsbeauftragte der Ressorts § 47 Wesentliche Digitalisierungsvorhaben des Bundes § 48 Amt des Koordinators für Informationssicherheit § 49 Aufgaben des Koordinators § 50 Befugnisse des Koordinators	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		Teil 4 Datenbank der Domain-Namen-Registrierungsdaten § 51 Pflicht zum Führen einer Datenbank § 52 Verpflichtung zur Zugangsgewährung § 53 Kooperationspflicht Teil 5 Zertifizierung und Kennzeichen § 54 Zertifizierung § 55 Nationale Behörde für die Cybersicherheitszertifizierung § 56 Freiwilliges IT-Sicherheitskennzeichen Teil 6 Verordnungsermächtigungen, Grundrechtseinschränkungen, Rat der IT Beauftragten und Berichtspflichten § 57 Ermächtigung zum Erlass von Rechtsverordnungen § 58 Einschränkung von Grundrechten § 59 Berichtspflichten des Bundesamtes Teil 7 Bußgeldvorschriften und Aufsicht § 60 Sanktionsvorschriften § 61 Institutionen der Sozialen Sicherung § 62 Zuständigkeit des Bundesamtes § 63 Zentrale Zuständigkeit in der Europäischen Union für Anbieter digitaler Dienste § 64 Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtige Einrichtungen	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		§ 65 Aufsichts- und Durchsetzungsmaßnahmen für wichtige Einrichtungen	
3		Teil 1 Allgemeine Vorschriften	Neue Gliederung zur Steigerung der Übersichtlichkeit
4	§ 1 Bundesamt für Sicherheit in der Informationstechnik	§ 1 Bundesamt für Sicherheit in der Informationstechnik	
5	Das Bundesamt für Sicherheit in der Informationstechnik (Bundesamt) ist eine Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern, für Bau und Heimat. Es ist die zentrale Stelle für Informationssicherheit auf nationaler Ebene. Aufgaben gegenüber den Bundesministerien führt das Bundesamt auf Grundlage wissenschaftlich-technischer Erkenntnisse durch.	Das Bundesamt für Sicherheit in der Informationstechnik (Bundesamt) ist eine Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern und für Heimat. Es ist die zentrale Stelle für Informationssicherheit auf nationaler Ebene. Aufgaben gegenüber den Bundesministerien führt das Bundesamt auf Grundlage wissenschaftlich-technischer Erkenntnisse durch.	redaktionelle Änderung
6	§ 2 Begriffsbestimmungen	§ 2 Begriffsbestimmungen	
7	(1) Die Informationstechnik im Sinne dieses Gesetzes umfasst alle technischen Mittel zur Verarbeitung von Informationen.		Verschoben nach § 2 Abs. 2 Nr. 20 nF.
8	(2) Informationen sowie informationsverarbeitende Systeme, Komponenten und Prozesse sind besonders schützenswert. Der Zugriff auf diese darf ausschließlich durch autorisierte Personen oder Programme erfolgen. Die Sicherheit in der Informationstechnik und der damit verbundene Schutz von Informationen und informationsverarbeitenden Systemen vor Angriffen und unautorisierten Zugriffen im Sinne dieses Gesetzes erfordert die Einhaltung bestimmter Sicherheitsstandards zur Gewährleistung der informationstechnischen Grundwerte und Schutzziele. Sicherheit in der Informationstechnik im Sinne dieses		§ 2 Absatz 2 Satz 4 aF. verschoben nach § 2 Absatz 2 Nr. 36 nF.; § 2 Absatz 2 Satz 1-3 aF. enthalten keine Begriffsbestimmung und werden als überflüssiger Teil gestrichen.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Gesetzes bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen		
9	1. in informationstechnischen Systemen, Komponenten oder Prozessen oder		
10	2. bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen.		
11		(1) Im Sinne dieses Gesetzes ist oder sind	Anders als die bisherigen Absätze des § 2 aF. sind die Begriffe in den Nummern dieses Absatzes 1 alphabetisch geordnet. Eine thematische Sortierung scheidet aufgrund der großen Anzahl der Begriffe aus, eine Übersichtlichkeit für den Rechtsanwender könnte dann nicht mehr gewährleistet werden.
12		1. „Beinahevorfall“ ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über informationstechnische Systeme, Komponenten und Prozesse angeboten werden oder zugänglich sind, beeinträchtigt haben könnte, dessen Eintritt jedoch erfolgreich verhindert wurde oder auf andere Weise nicht eingetreten ist;	Umsetzung Art. 6 Ziff. 5 NIS2
13		2. „Cloud Computing-Dienst“ ein digitaler Dienst, der auf Abruf die Verwaltung und den umfassenden Fernzugang zu einem skalierbaren und elastischen Pool	Umsetzung Art. 6 Ziff. 30 NIS2.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		gemeinsam nutzbarer Rechenressourcen ermöglicht, auch wenn diese Ressourcen auf mehrere Standorte verteilt sind;	
14		3. „Content Delivery Network“ ein Netz dezentraler Server zur Gewährleistung einer hohen Verfügbarkeit, Zugänglichkeit oder Zustellung digitaler Inhalte und Dienste für Internetnutzer mit möglichst niedriger Latenz im Auftrag von Inhalte- und Diensteanbietern;	Umsetzung Art. 6 Ziff. 32 NIS2.
15		4. „Cyberbedrohung“ eine Cyberbedrohung im Sinne des Artikel 2 Nummer 8 der Verordnung (EU) 2019/881;	Umsetzung Art. 6 Ziff. 10 NIS2
16	*(9) Datenverkehr im Sinne dieses Gesetzes sind die mittels technischer Protokolle übertragenen Daten. Der Datenverkehr kann Telekommunikationsinhalte nach § 3 Absatz 1 des Telekommunikation-Telemedien-Datenschutz-Gesetzes und Nutzungsdaten nach § 2 Absatz 2 Nummer 3 des Telekommunikation-Telemedien-Datenschutz-Gesetzes enthalten.*	5. „Datenverkehr“ mittels technischer Protokolle übertragene Daten; Telekommunikationsinhalte nach § 3 Absatz 1 des Telekommunikation-Telemedien-Datenschutz-Gesetzes und Nutzungsdaten nach § 2 Absatz 2 Nummer 3 des Telekommunikation-Telemedien-Datenschutz-Gesetzes können enthalten sein,	redaktionelle Änderungen
17	*(11) Digitale Dienste im Sinne dieses Gesetzes sind Dienste im Sinne von Artikel 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1), und die*	6. „digitaler Dienst“ ein Dienst im Sinne von Artikel 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1)	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
18		7. „DNS-Diensteanbieter“ eine Einrichtung, die	Umsetzung Art. 6 Ziff. 20 NIS2
19		a) für Internet-Endnutzer öffentlich verfügbare rekursive Dienste zur Auflösung von Domain-Namen anbietet oder	Umsetzung Art. 6 Ziff. 20 lit. a NIS2
20		b) autoritative Dienste zur Auflösung von Domain-Namen zur Nutzung durch Dritte, mit Ausnahme von Root-Namenservern, anbietet;	Umsetzung Art. 6 Ziff. 20 lit. b NIS2
21		8. „Domain-Name-Registry-Dienstleister“ ein Registrar oder eine Stelle, die im Namen von Registraren tätig ist, insbesondere Anbieter oder Wiederverkäufer von Datenschutz- oder Proxy-Registrierungsdiensten;	Umsetzung Art. 6 Ziff. 22 NIS2
22			
23		9. „erhebliche Cyberbedrohung“ eine Cyberbedrohung, die das Potenzial besitzt, die informationstechnischen Systeme, Komponenten und Prozesse aufgrund ihrer besonderen technischen Merkmale erheblich zu beeinträchtigen; eine Beeinträchtigung ist erheblich, wennsie erheblichen materiellen oder immateriellen Schaden verursachen kann;	Umsetzung Art. 6 Ziff. 11 NIS2;
24		10. „erheblicher Sicherheitsvorfall“ ein Sicherheitsvorfall, der	Umsetzung Art. 23 Abs. 3 NIS2
25		a) schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung	Umsetzung Art. 23 Abs. 3 NIS2

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		verursacht hat oder verursachen kann; oder	
26		b) andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann,	Umsetzung Art. 23 Abs. 3 NIS2
27		soweit nach Absatz 4 keine weitergehende Begriffsbestimmung erfolgt;	Umsetzung Art. 23 Abs. 11 Uabs. 2 NIS2
28		11. „Geschäftsleiter“ diejenigen natürlichen Personen, die nach Gesetz, Satzung oder Gesellschaftsvertrag zur Führung der Geschäfte und zur Vertretung einer Einrichtung berufen sind;	Begriffsbestimmung für Umsetzung Art. 20 NIS-2.
29		12. „Großunternehmen“ ein Unternehmen oder eine rechtlich unselbständige Organisationseinheit einer Gebietskörperschaft, das oder die a) mindestens 250 Mitarbeiter beschäftigt, oder b) einen Jahresumsatz von mindestens 50 Millionen EUR und zudem eine Jahresbilanzsumme von mindestens 43 Millionen EUR aufweist; bei der Bestimmung von Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme ist außer für rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft die Empfehlung 2003/361/EG mit Ausnahme von Artikel 3 Absatz 4 des Anhang anzuwenden; die Daten von Partner- oder verbundenen Unternehmen im Sinne der	Wann ein Unternehmen ein „Großunternehmen“ darstellt, ist der Empfehlung 2003/361/EG nicht ohne Weiteres zu entnehmen, da diese auf die Definition von KMU (kleinen und mittleren Unternehmen) abzielte. Um die einfachere Lesbarkeit der Regelungen zu gewährleisten werden in dieser Begriffsbestimmung die entscheidenden Schwellenwerte und ihre Beziehung zueinander dargestellt. Die Anwendung der Kommissionsempfehlung 2003/361/EG für die Zwecke der Bestimmung des Anwendungsbereichs der NIS-2-Richtlinie kann in bestimmten Fällen zu dem unverhältnismäßigen Ergebnis führen, dass Partner- oder verbundene Unternehmen - die die Schwellenwerte

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		Empfehlung 2003/361/EG sind nicht hinzurechnen, wenn das Unternehmen unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf die Beschaffenheit und den Betrieb der informationstechnischen Systeme, Komponenten und Prozesse, die das Unternehmen für die Erbringung seiner Dienste nutzt, ausübt;	mit eigenen Zahlen nicht erfüllen - sseparat ebenfalls als wichtige und besonders wichtige Einrichtungen erfasst werden. In Einklang mit dem Erwägungsgrund 16 der NIS-2-Richtlinie werden solche Unternehmen unterhalb der Größenschwelle aus dem Anwendungsbereich ausgeschlossen.
30		13. „IKT-Dienst“ ein IKT-Dienst im Sinne des Artikels 2 Nummer 13 der Verordnung (EU) 2019/881;	Umsetzung Art. 6 Ziff. 13 NIS-2. Mit „IKT-Dienst“ ist in der VO (EU) 2019/881 ein Dienst gemeint, der vollständig oder überwiegend aus der Übertragung, Speicherung, Abfrage oder Verarbeitung von Informationen mittels informationstechnischen Systemen, Komponenten und Prozessen besteht.
31	*(9a) IT-Produkte im Sinne dieses Gesetzes sind Software, Hardware sowie alle einzelnen oder miteinander verbundenen Komponenten, die Informationen informationstechnisch verarbeiten.*	14. „IKT-Produkt“ ein IKT-Produkt im Sinne des Artikels 2 Nummer 12 der Verordnung (EU) 2019/881;	Umsetzung Art. 6 Ziff. 13 NIS-2. „IKT-Produkt“ ist in der VO (EU) 2019/881 ein Element oder eine Gruppe von Elementen eines Netz- oder Informationssystems gemeint. Der Begriff wird zur europaweiten Vereinheitlichung der Terminologie im Rahmen der Umsetzung der NIS-2-Richtlinie eingeführt und ersetzt den alten Begriff des IT-Produkts. Inhaltlich ergeben sich zwischen beiden Begriffen keine Unterschiede.
32		15. „IKT-Prozess“ ein IKT-Prozess im Sinne des Artikels 2 Nummer 14 der Verordnung (EU) 2019/881;	Umsetzung Art. 6 Ziff. 14 NIS-2. Mit dem Begriff „IKT-Prozess“ meint die VO (EU) 2019/881 jegliche Tätigkeiten, mit denen ein ITK-Produkt oder -Dienst

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			konzipiert, entwickelt, bereitgestellt oder gepflegt werden soll.
33	*(1) Die Informationstechnik im Sinne dieses Gesetzes umfasst alle technischen Mittel zur Verarbeitung von Informationen.*	16. „Informationstechnik“ ein technisches Mittel zur Verarbeitung von Informationen;	Verschiebung von § 2 Abs. 1 aF.; redaktionelle Änderungen
34		17. „Internet Exchange Point“ oder „IXP“ eine Netzeinrichtung, die die Zusammenschaltung von mehr als zwei unabhängigen Netzen (autonomen Systemen) ermöglicht, in erster Linie zur Erleichterung des Austauschs von Internet-Datenverkehr, der nur der Zusammenschaltung autonomer Systeme dient und weder voraussetzt, dass der Internet-Datenverkehr zwischen zwei beliebigen teilnehmenden autonomen Systemen über ein drittes autonomes System läuft; noch den betreffenden Datenverkehr verändert oder anderweitig beeinträchtigt;	Umsetzung Art. 6 Ziff. 18 NIS-2.
35	*(3) Kommunikationstechnik des Bundes im Sinne dieses Gesetzes ist die Informationstechnik, die von einer oder mehreren Bundesbehörden oder im Auftrag einer oder mehrerer Bundesbehörden betrieben wird und der Kommunikation oder dem Datenaustausch innerhalb einer Bundesbehörde, der Bundesbehörden untereinander oder der Bundesbehörden mit Dritten dient. Kommunikationstechnik des Bundesverfassungsgerichts, der Bundesgerichte, soweit sie nicht öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen, des Bundestages, des Bundesrates, des Bundespräsidenten und des Bundesrechnungshofes ist nicht Kommunikationstechnik des Bundes, soweit sie ausschließlich in deren eigener Zuständigkeit betrieben wird.*	18. „Kommunikationstechnik des Bundes“ Informationstechnik, die von einer oder mehreren Einrichtungen der Bundesverwaltung oder im Auftrag einer oder mehrerer Einrichtungen der Bundesverwaltung betrieben wird und der Kommunikation oder dem Datenaustausch innerhalb einer Einrichtung der Bundesverwaltung, der Einrichtungen der Bundesverwaltung untereinander oder der Einrichtungen der Bundesverwaltung mit Dritten dient; davon ausgenommen ist die Kommunikationstechnik des Bundesverfassungsgerichts, der Bundesgerichte, soweit sie nicht	Verschiebung von § 2 Absatz 3 aF.. Es wurde eine Begriffskonsolidierung vorgenommen - statt Bundesbehörden nun Einrichtungen der Bundesverwaltung. Der Begriff wird über den Anwendungsbereich von § 27 definiert. Die Erweiterung der Definition ist vor dem Hintergrund der Zeitenwende geboten und ist mit Rücksicht darauf erforderlich, dass angesichts der komplexen digitalen Infrastruktur auch IT schutzbedürftig sein kann, die nicht unmittelbar von Bundesbehörden betrieben oder verwendet wird. Eine Kompromittierung der Systeme einer Einrichtung der

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen, des Bundestages, des Bundesrates, des Bundespräsidenten und des Bundesrechnungshofes, soweit sie ausschließlich in deren eigener Zuständigkeit betrieben wird;	Bundesverwaltung ist geeignet, ein Risiko für alle damit vernetzten Einrichtungen darzustellen, auch wenn die konkret betroffene IT nur mittelbar z.B. durch Handeln Einzelner gefährdet ist.
36	*(10) Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die*	19. „kritische Anlage“ eine Anlage die von hoher Bedeutung für das Funktionieren des Gemeinwesens ist, da durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden; welche Anlagen im Einzelnen kritische Anlagen sind, bestimmt sich nach § 26 Absatz 2a;	Verschiebung von § 2 Abs. 10 aF.; Änderungen aufgrund neuer Regelungssystematik. Diese Vorschrift (§ 2 Abs. 10 aF.) ist Gegenstand der Evaluierung gemäß Art. 6 Abs. 1 Nr. 1 Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 18. Mai 2021 (BGBl. I S. 1122). Diese Änderung erfolgt vorbehaltlich der Ergebnisse dieser Evaluierung und wird gegebenenfalls noch auf deren Grundlage angepasst.
37	*1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung angehören und*		s.o.
38	*2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.*		s.o.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
39	*Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmt.*		s.o.
40	*(13) Kritische Komponenten im Sinne dieses Gesetzes sind IT-Produkte,*	20. „kritische Komponenten“ IT-Produkte,	Verschiebung von § 2 Abs. 13 aF.; redaktionelle Änderungen
41	*1. die in Kritischen Infrastrukturen eingesetzt werden,*	a) die in Kritischen Anlagen eingesetzt werden,	s.o.
42	*2. bei denen Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit Kritischer Infrastrukturen oder zu Gefährdungen für die öffentliche Sicherheit führen können und*	b) bei denen Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit Kritischer Anlagen oder zu Gefährdungen für die öffentliche Sicherheit führen können und	s.o.
43	*3. die auf Grund eines Gesetzes unter Verweis auf diese Vorschrift*	c) die auf Grund eines Gesetzes unter Verweis auf diese Vorschrift	s.o.
44	*a) als kritische Komponente bestimmt werden oder*	aa) als kritische Komponente bestimmt werden oder	s.o.
45	*b) eine auf Grund eines Gesetzes als kritisch bestimmte Funktion realisieren.*	bb) eine auf Grund eines Gesetzes als kritisch bestimmte Funktion realisieren,	s.o.
46	*Werden für einen der in Absatz 10 Satz 1 Nummer 1 genannten Sektoren keine kritischen Komponenten und keine kritischen Funktionen, aus denen kritische Komponenten abgeleitet werden können, auf Grund eines Gesetzes unter Verweis auf diese Vorschrift bestimmt, gibt es in diesem Sektor keine kritischen Komponenten im Sinne dieses Gesetzes.*	werden für einen der in dieser Nummer genannten Sektoren keine kritischen Komponenten und keine kritischen Funktionen, aus denen kritische Komponenten abgeleitet werden können, auf Grund eines Gesetzes unter Verweis auf diese Vorschrift bestimmt, gibt es in diesem Sektor keine kritischen	s.o.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		Komponenten im Sinne von dieser Nummer;	
47		21. „Managed Security Service Provider“ oder „MSSP“ ein Anbieter verwalteter Dienste, der Unterstützung für Tätigkeiten im Zusammenhang mit dem Risikomanagement im Bereich der Cybersicherheit durchführt oder erbringt;	Umsetzung Art. 6 Ziff. 40 NIS-2
48		22. „Managed Service Provider“ oder „MSP“ eine Einrichtung, die Dienste im Zusammenhang mit der Installation, der Verwaltung, dem Betrieb oder der Wartung von IKT-Produkten, -Netzen, -Infrastruktur, -Anwendungen oder jeglicher anderer Netz- und Informationssysteme durch Unterstützung oder aktive Verwaltung in den Räumlichkeiten der Kunden oder aus der Ferne erbringt;	Umsetzung Art. 6 Ziff. 39 NIS2;
49		23. „mittleres Unternehmen“ ein Unternehmen oder eine rechtlich unselbständige Organisationseinheiten einer Gebietskörperschaft, das oder die a) mindestens 50 und höchstens 249 Mitarbeiter beschäftigt und zudem einen Jahresumsatz von weniger als 50 Millionen EUR oder eine Jahresbilanzsumme von weniger als 43 Millionen EUR aufweist, oder b) weniger als 50 Mitarbeiter beschäftigt und einen Jahresumsatz und eine Jahresbilanzsumme von jeweils mindestens 10 Millionen EUR und einen Jahresumsatz von höchstens 50 Millionen EUR sowie eine	Um die einfachere Lesbarkeit der Regelungen zu gewährleisten, werden in dieser Begriffsbestimmung die entscheidenden Schwellenwerte und ihre Beziehung zueinander dargestellt. Die Anwendung der Kommissionsempfehlung 2003/361/EG für die Zwecke der Bestimmung des Anwendungsbereichs der NIS-2-Richtlinie kann in bestimmten Fällen zu dem unverhältnismäßigen Ergebnis führen, dass Partner- oder verbundene Unternehmen - die die Schwellenwerte mit eigenen Zahlen nicht erfüllen - separat ebenfalls als wichtige und besonders wichtige Einrichtungen erfasst werden. In Einklang mit dem

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		Bilanzsumme von höchstens 43 Millionen EUR aufweist; bei der Bestimmung von Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme ist außer für rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft die Empfehlung 2003/361/EG mit Ausnahme von Artikel 3 Absatz 4 des Anhang anzuwenden; die Daten von Partner- oder verbundenen Unternehmen im Sinne der Empfehlung 2003/361/EG sind nicht hinzurechnen, wenn das Unternehmen unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf die Beschaffenheit und den Betrieb der informationstechnischen Systeme, Komponenten und Prozesse, die das Unternehmen für die Erbringung seiner Dienste nutzt, ausübt;	Erwägungsgrund 16 der NIS-2-Richtlinie werden solche Unternehmen unterhalb der Größenschwelle aus dem Anwendungsbereich ausgeschlossen.
50		24. „NIS-2-Richtlinie“ die Richtlinie 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (ABl. L 333 vom 27.12.2022, S. 80) in der jeweils geltenden Fassung,	
51		25. „Online-Marktplatz“ ein Dienst im Sinne des § 312l Absatz 3 BGB	Umsetzung Art. 6 Ziff. 28 NIS2;

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
52		26. „Online-Suchmaschine“ ein digitaler Dienst im Sinne des Artikels 2 Nummer 5 der Verordnung (EU) 2019/1150;	Umsetzung Art. 6 Ziff. 29 NIS2;
53		27. „Plattform für Dienste sozialer Netzwerke“ eine Plattform, auf der Endnutzer mit unterschiedlichen Geräten insbesondere durch Chats, Posts, Videos und Empfehlungen miteinander in Kontakt treten und kommunizieren sowie Inhalte teilen und entdecken können;	Umsetzung Art. 6 Ziff. 33 NIS2;
54	*(8) Protokolldaten im Sinne dieses Gesetzes sind Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind. Protokolldaten können Verkehrsdaten gemäß § 3 Nummer 70 des Telekommunikationsgesetzes und Nutzungsdaten nach § 2 Absatz 2 Nummer 3 des Telekommunikation-Telemedien-Datenschutz-Gesetzes enthalten.*	28. „Protokolldaten“ Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind; Verkehrsdaten gemäß § 3 Nummer 70 des Telekommunikationsgesetzes und Nutzungsdaten nach § 2 Absatz 2 Nummer 3 des Telekommunikation-Telemedien-Datenschutz-Gesetzes können enthalten sein,	Verschiebung von § 2 Abs. 8 aF; redaktionelle Änderungen
55	*(8a) Protokollierungsdaten im Sinne dieses Gesetzes sind Aufzeichnungen über technische Ereignisse oder Zustände innerhalb informationstechnischer Systeme.*	29. „Protokollierungsdaten“ Aufzeichnungen über technische Ereignisse oder Zustände innerhalb informationstechnischer Systeme,	Verschiebung von § 2 Abs. 8a aF; redaktionelle Änderungen
56		30. „qualifizierter Vertrauensdienst“ ein qualifizierter Vertrauensdienst im Sinne des Artikels 3 Nummer 17 der Verordnung (EU) Nr. 910/2014;	Umsetzung Art. 6 Ziff. 26 NIS2;

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
57		31. „qualifizierter Vertrauensdiensteanbieter“ ein qualifizierter Vertrauensdiensteanbieter im Sinne des Artikels 3 Nummer 20 der Verordnung (EU) Nr. 910/2014;	Umsetzung Art. 6 Ziff. 27 NIS2;
58		32. „Rechenzentrumsdienst“ ein Dienst, mit dem spezielle Strukturen oder Gruppen von Strukturen für die zentrale Unterbringung, die Verbindung und den Betrieb von IT- und Netzausrüstungen zur Erbringung von Datenspeicher-, Datenverarbeitungs- und Datentransportdiensten sowie alle Anlagen und Infrastrukturen für die Leistungsverteilung und die Umgebungskontrolle bereitgestellt werden;	Umsetzung Art. 6 Ziff. 31 NIS2;
59	*(5) Schadprogramme im Sinne dieses Gesetzes sind Programme und sonstige informationstechnische Routinen und Verfahren, die dem Zweck dienen, unbefugt Daten zu nutzen oder zu löschen oder die dem Zweck dienen, unbefugt auf sonstige informationstechnische Abläufe einzuwirken.*	33. „Schadprogramme“ Programme und sonstige informationstechnische Routinen und Verfahren, die dem Zweck dienen, unbefugt Daten zu nutzen oder zu löschen oder die dem Zweck dienen, unbefugt auf sonstige informationstechnische Abläufe einzuwirken,	redaktionelle Änderungen
60	*(4) Schnittstellen der Kommunikationstechnik des Bundes im Sinne dieses Gesetzes sind sicherheitsrelevante Netzwerkübergänge innerhalb der Kommunikationstechnik des Bundes sowie zwischen dieser und der Informationstechnik der einzelnen Bundesbehörden, Gruppen von Bundesbehörden oder Dritter. Dies gilt nicht für die Komponenten an den Netzwerkübergängen, die in eigener Zuständigkeit der in Absatz 3 Satz 2 genannten Gerichte und Verfassungsorgane betrieben werden.*	34. „Schnittstellen der Kommunikationstechnik des Bundes“ sicherheitsrelevante Netzwerkübergänge innerhalb der Kommunikationstechnik des Bundes sowie zwischen dieser und der Informationstechnik der einzelnen Einrichtungen der Bundesverwaltung, Gruppen von Einrichtungen der Bundesverwaltung oder Dritter; davon ausgenommen sind die Komponenten an den Netzwerkübergängen, die in eigener	Redaktionelle Änderungen. Im Übrigen wird eine Begriffskonsolidierung/Folgeänderung vorgenommen: statt Bundesbehörden nun Einrichtungen der Bundesverwaltung. Durch die Anpassung erweitert sich die Reichweite des Begriffs – mit Blick auf den Schutzzweck der Informationssicherheit der Netze des Bundes bzw. möglicher weiterer

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		Zuständigkeit der in Nummer 23 genannten Gerichte und Verfassungsorgane betrieben werden,	Regierungsnetze bedeutet die Erweiterung die Klarstellung, dass nicht allein Bundesbehörden an diese Netze angeschlossen sein können. Nummer 23 existiert so nicht, kein passender Verweis
61	*(6) Sicherheitslücken im Sinne dieses Gesetzes sind Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Dritte gegen den Willen des Berechtigten Zugang zu fremden informationstechnischen Systemen verschaffen oder die Funktion der informationstechnischen Systeme beeinflussen können.*	35. „Schwachstelle“ eine Schwäche, Anfälligkeit oder Fehlfunktion von IKT-Produkten oder IKT-Diensten, die bei einer Cyberbedrohung ausgenutzt werden kann;	Umsetzung Art. 6 Ziff. 15 NIS2. Der Begriff der „Sicherheitslücke“ (§ 2 Abs. 6 aF) geht in diesem auf.
62	*(2) […]. Sicherheit in der Informationstechnik im Sinne dieses Gesetzes bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen*	36. „Sicherheit in der Informationstechnik“ die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen	
63	*1. in informationstechnischen Systemen, Komponenten oder Prozessen oder*	a) in informationstechnischen Systemen, Komponenten oder Prozessen oder	
64	*2. bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen.*	b) bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen,	
65		37. „Sicherheitsvorfall“ ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über informationstechnische Systeme, Komponenten und Prozesse angeboten	Umsetzung Art. 6 Ziff. 6 NIS-2.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		werden oder zugänglich sind, beeinträchtigt;	
66	*(9b) Systeme zur Angriffserkennung im Sinne dieses Gesetzes sind durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme. Die Angriffserkennung erfolgt dabei durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten.*	38. „Systeme zur Angriffserkennung“ durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme; wobei die Angriffserkennung durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten, erfolgt,	Verschiebung von § 2 Abs. 9b aF.; redaktionelle Änderungen
67		39. „Top Level Domain Name Registry“ eine Einrichtung, welche die Registrierung von Internet-Domain-Namen innerhalb einer spezifischen Top Level Domain (TLD) verwaltet und betreibt, einschließlich des Betriebs ihrer Namenserver, der Pflege ihrer Datenbanken und der Verteilung von TLD-Zonendateien über die Namenserver, zuständig ist, unabhängig davon, ob der Betrieb durch die Einrichtung selbst erfolgt oder ausgelagert wird, jedoch mit Ausnahme von Situationen, in denen TLD-Namen von einem Register nur für seine eigenen Zwecke verwendet werden;	Umsetzung Art. 6 Ziff. 21 NIS-2.
68		40. „Vertrauensdienst“ ein Vertrauensdienst im Sinne des Artikels 3 Nummer 16 der Verordnung (EU) Nr. 910/2014;	Umsetzung Art. 6 Ziff. 24 NIS-2.
69		41. „Vertrauensdiensteanbieter“ ein Vertrauensdiensteanbieter im Sinne des	Umsetzung Art. 6 Ziff. 25 NIS-2.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		Artikels 3 Nummer 19 der Verordnung (EU) Nr. 910/2014;	
70	*(7) Zertifizierung im Sinne dieses Gesetzes ist die Feststellung durch eine Zertifizierungsstelle, dass ein Produkt, ein Prozess, ein System, ein Schutzprofil (Sicherheitszertifizierung), eine Person (Personenzertifizierung) oder ein IT-Sicherheitsdienstleister bestimmte Anforderungen erfüllt.*	42. „Zertifizierung“ die Feststellung einer Zertifizierungsstelle, dass ein Produkt, ein Prozess, ein System, ein Schutzprofil (Sicherheitszertifizierung), eine Person (Personenzertifizierung) oder ein IT-Sicherheitsdienstleister bestimmte Anforderungen erfüllt,	Verschoben von § 2 Abs. 7; redaktionelle Änderungen.
71	(3) Kommunikationstechnik des Bundes im Sinne dieses Gesetzes ist die Informationstechnik, die von einer oder mehreren Bundesbehörden oder im Auftrag einer oder mehrerer Bundesbehörden betrieben wird und der Kommunikation oder dem Datenaustausch innerhalb einer Bundesbehörde, der Bundesbehörden untereinander oder der Bundesbehörden mit Dritten dient. Kommunikationstechnik des Bundesverfassungsgerichts, der Bundesgerichte, soweit sie nicht öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen, des Bundestages, des Bundesrates, des Bundespräsidenten und des Bundesrechnungshofes ist nicht Kommunikationstechnik des Bundes, soweit sie ausschließlich in deren eigener Zuständigkeit betrieben wird.		Verschoben nach § 2 Abs. 1 Nr. 18.
72	(4) Schnittstellen der Kommunikationstechnik des Bundes im Sinne dieses Gesetzes sind sicherheitsrelevante Netzwerkübergänge innerhalb der Kommunikationstechnik des Bundes sowie zwischen dieser und der Informationstechnik der einzelnen Bundesbehörden, Gruppen von Bundesbehörden oder Dritter. Dies gilt nicht für die Komponenten an den Netzwerkübergängen, die in eigener Zuständigkeit der in Absatz 3 Satz 2 genannten Gerichte und Verfassungsorgane betrieben werden.		Verschoben nach § 2 Abs. 1 Nr. 34.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
73	(5) Schadprogramme im Sinne dieses Gesetzes sind Programme und sonstige informationstechnische Routinen und Verfahren, die dem Zweck dienen, unbefugt Daten zu nutzen oder zu löschen oder die dem Zweck dienen, unbefugt auf sonstige informationstechnische Abläufe einzuwirken.		Verschoben nach § 2 Abs. 1 Nr. 33.
74	(6) Sicherheitslücken im Sinne dieses Gesetzes sind Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Dritte gegen den Willen des Berechtigten Zugang zu fremden informationstechnischen Systemen verschaffen oder die Funktion der informationstechnischen Systeme beeinflussen können.		Entfällt, ersetzt durch § 2 Abs. 1 Nr. 35.
75	(7) Zertifizierung im Sinne dieses Gesetzes ist die Feststellung durch eine Zertifizierungsstelle, dass ein Produkt, ein Prozess, ein System, ein Schutzprofil (Sicherheitszertifizierung), eine Person (Personenzertifizierung) oder ein IT-Sicherheitsdienstleister bestimmte Anforderungen erfüllt.		Verschoben nach § 2 Abs. 1 Nr. 42.
76	(8) Protokolldaten im Sinne dieses Gesetzes sind Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind. Protokolldaten können Verkehrsdaten gemäß § 3 Nummer 70 des Telekommunikationsgesetzes und Nutzungsdaten nach § 2 Absatz 2 Nummer 3 des Telekommunikation-Telemedien-Datenschutz-Gesetzes enthalten.		Verschoben nach § 2 Abs. 1 Nr. 28.
77	(8a) Protokollierungsdaten im Sinne dieses Gesetzes sind Aufzeichnungen über technische		Verschoben nach § 2 Abs. 1 Nr. 29.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Ereignisse oder Zustände innerhalb informationstechnischer Systeme.		
78	(9) Datenverkehr im Sinne dieses Gesetzes sind die mittels technischer Protokolle übertragenen Daten. Der Datenverkehr kann Telekommunikationsinhalte nach § 3 Absatz 1 des Telekommunikation-Telemedien-Datenschutz-Gesetzes und Nutzungsdaten nach § 2 Absatz 2 Nummer 3 des Telekommunikation-Telemedien-Datenschutz-Gesetzes enthalten.		Verschoben nach § 2 Abs. 1 Nr. 5.
79	(9a) IT-Produkte im Sinne dieses Gesetzes sind Software, Hardware sowie alle einzelnen oder miteinander verbundenen Komponenten, die Informationen informationstechnisch verarbeiten.		Verschoben nach § 2 Abs. 1 Nr. 22.
80	(9b) Systeme zur Angriffserkennung im Sinne dieses Gesetzes sind durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme. Die Angriffserkennung erfolgt dabei durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten.		Verschoben nach § 2 Abs. 1 Nr. 38.
81	(10) Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die		Verschoben nach § 2 Abs. 1 Nr. 19.
82	1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung angehören und		s.o.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
83	2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.		s.o.
84	Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmt.		s.o.
85	(11) Digitale Dienste im Sinne dieses Gesetzes sind Dienste im Sinne von Artikel 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1), und die		Verschoben nach § 2 Abs. 1 Nr. 6.
86	1. es Verbrauchern oder Unternehmern im Sinne des Artikels 4 Absatz 1 Buchstabe a beziehungsweise Buchstabe b der Richtlinie 2013/11/EU des Europäischen Parlaments und des Rates vom 21. Mai 2013 über die alternative Beilegung verbraucherrechtlicher Streitigkeiten und zur Änderung der Verordnung (EG) Nr. 2006/2004 und der Richtlinie 2009/22/EG (Richtlinie über alternative Streitbeilegung in Verbraucherangelegenheiten) (ABl. L 165 vom 18.6.2013, S. 63) ermöglichen, Kaufverträge oder Dienstleistungsverträge mit Unternehmern entweder auf der Webseite dieser Dienste oder auf der Webseite eines Unternehmers, die von diesen Diensten bereitgestellte Rechendienste		Entfällt.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	verwendet, abzuschließen (Online-Marktplätze);		
87	2. es Nutzern ermöglichen, Suchen grundsätzlich auf allen Webseiten oder auf Webseiten in einer bestimmten Sprache anhand einer Abfrage zu einem beliebigen Thema in Form eines Stichworts, einer Wortgruppe oder einer anderen Eingabe vorzunehmen, die daraufhin Links anzeigen, über die der Abfrage entsprechende Inhalte abgerufen werden können (Online-Suchmaschinen);		Entfällt.
88	3. den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglichen (Cloud-Computing-Dienste),		Entfällt.
89	und nicht zum Schutz grundlegender staatlicher Funktionen eingerichtet worden sind oder für diese genutzt werden.		Entfällt.
90	(12) „Anbieter digitaler Dienste“ im Sinne dieses Gesetzes ist eine juristische Person, die einen digitalen Dienst anbietet.		Entfällt.
91	(13) Kritische Komponenten im Sinne dieses Gesetzes sind IT-Produkte,		Verschoben nach § 2 Abs. 1 Nr. 20.
92	1. die in Kritischen Infrastrukturen eingesetzt werden,		s.o.
93	2. bei denen Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit Kritischer Infrastrukturen oder zu Gefährdungen für		s.o.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	die öffentliche Sicherheit führen können und		
94	3. die auf Grund eines Gesetzes unter Verweis auf diese Vorschrift		s.o.
95	a) als kritische Komponente bestimmt werden oder		s.o.
96	b) eine auf Grund eines Gesetzes als kritisch bestimmte Funktion realisieren.		s.o.
97	Werden für einen der in Absatz 10 Satz 1 Nummer 1 genannten Sektoren keine kritischen Komponenten und keine kritischen Funktionen, aus denen kritische Komponenten abgeleitet werden können, auf Grund eines Gesetzes unter Verweis auf diese Vorschrift bestimmt, gibt es in diesem Sektor keine kritischen Komponenten im Sinne dieses Gesetzes.		s.o.
98		(3) Das Bundesamt kann Vorgaben machen, wann ein Sicherheitsvorfall als erheblich anzusehen ist Für den Fall, dass die Kommission einen oder mehrere Durchführungsrechtsakte gemäß Artikel 23 Absatz 11 Unterabsatz 2 der NIS-2-Richtlinie erlässt, worin näher bestimmt wird, in welchen Fällen ein Sicherheitsvorfall als erheblich anzusehen ist, geht diese den Vorgaben des Bundesamtes nach Satz 1 insoweit vor.	Umsetzung Art. 23 Abs. 11 Uabs. 2 NIS-2. Das Bundesamt kann Vorgaben dazu machen, wann Sicherheitsvorfälle als erheblich gelten. Soweit die Kommission dahingehende Durchführungsrechtsakte erlässt, genießen diese Vorrang. Die Vorgaben des Bundesamtes haben dann nur noch konkretisierende Wirkung, soweit die Durchführungsrechtsakte Auslegungsspielräume lassen.
99	(14) Unternehmen im besonderen öffentlichen Interesse sind Unternehmen, die nicht Betreiber Kritischer Infrastrukturen nach Absatz 10 sind und		Entfällt. Die Kategorie geht in „Wichtige Einrichtungen“ über.
100	1. die Güter nach § 60 Absatz 1 Nummer 1 und 3 der Außenwirtschaftsverordnung in		Übertagung nach § 28 Abs. 4 Nr. 4.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	der jeweils geltenden Fassung herstellen oder entwickeln,		
101	2. die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland sind oder die für solche Unternehmen als Zulieferer wegen ihrer Alleinstellungsmerkmale von wesentlicher Bedeutung sind oder		Entfällt. Die Erfordernis, Unternehmen, die aufgrund ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören, durch diese Vorschrift in den Regelungsbereich des BSIG zu ziehen, entfällt, da durch die Umsetzung der NIS-2-Richtlinie bereits alle relevanten mittleren und großen Unternehmen direkt einbezogen werden.
102	3. die Betreiber eines Betriebsbereichs der oberen Klasse im Sinne der Störfall-Verordnung in der jeweils geltenden Fassung sind oder nach § 1 Absatz 2 der Störfall-Verordnung diesen gleichgestellt sind.		Übertragung nach § 28 Abs. 4 Nr. 5.
103	Die Unternehmen im besonderen öffentlichen Interesse nach Satz 1 Nummer 2 werden durch die Rechtsverordnung nach § 10 Absatz 5 bestimmt, in der festgelegt wird, welche wirtschaftlichen Kennzahlen maßgeblich dafür sind, dass ein Unternehmen zu den größten Unternehmen in Deutschland im Sinne der Nummer 2 gehört und welche Alleinstellungsmerkmale maßgeblich dafür sind, dass Zulieferer für solche Unternehmen von wesentlicher Bedeutung sind.		Entfällt, siehe oben.
104		Teil 2 Das Bundesamt	Neue Gliederung zur Steigerung der Übersichtlichkeit
105		Kapitel 1 Aufgaben und Befugnisse	Neue Gliederung zur Steigerung der Übersichtlichkeit

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
106	§ 3 Aufgaben des Bundesamtes	§ 3 Aufgaben des Bundesamtes	Mit der Umsetzung der NIS-2-Richtlinie wird der Katalog der Aufgaben des Bundesamtes erweitert. Wie es die Erfüllung der Aufgaben priorisiert, hat das Bundesamt im Hinblick auf Art. 31 Abs. 2 S. 1 NIS-2-Richtlinie nach pflichtgemäßen Ermessen zu entscheiden
107	(1) Das Bundesamt fördert die Sicherheit in der Informationstechnik mit dem Ziel, die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen und deren Verarbeitung zu gewährleisten. Hierzu nimmt es folgende wichtige im öffentlichen Interesse liegende Aufgaben wahr:	(1) Das Bundesamt fördert die Sicherheit in der Informationstechnik. Hierzu nimmt es folgende wichtige im öffentlichen Interesse liegende Aufgaben wahr:	Bereinigung der Vorschrift durch Streichung in Satz 1. Da es sich bei „Sicherheit in der Informationstechnik“ um einen in § 2 Abs. 1 Nr. 48 nF. definierten Begriff handelt, welche die gestrichenen Worte bereits beinhaltet, handelte es sich hier um einen Zirkelschluss.
108	1. Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes;	1. Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes;	
109	2. Sammlung und Auswertung von Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen und Zurverfügungstellung der gewonnenen Erkenntnisse für andere Stellen, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist, sowie für Dritte, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist;	2. Sammlung und Auswertung von Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen und Zurverfügungstellung der gewonnenen Erkenntnisse für andere Stellen, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist, sowie für Dritte, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist;	
110		2a. Wahrnehmung der Aufgaben in der Kooperationsgruppe und im CSIRTs-Netzwerk nach Artikel 14 und 15 der NIS-2-Richtlinie;	Umsetzung von Art. 14 und 15 NIS-2 in Form einer Aufgabe des Bundesamtes.
111	3. Untersuchung von Sicherheitsrisiken bei Anwendung der Informationstechnik sowie Entwicklung von Sicherheitsvorkehrungen, insbesondere	3. Untersuchung von Sicherheitsrisiken bei Anwendung der Informationstechnik sowie Entwicklung von Sicherheitsvorkehrungen, insbesondere	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	von informationstechnischen Verfahren und Geräten für die Sicherheit in der Informationstechnik (IT-Sicherheitsprodukte), soweit dies zur Erfüllung von Aufgaben des Bundes erforderlich ist, einschließlich der Forschung im Rahmen seiner gesetzlichen Aufgaben;	von informationstechnischen Verfahren und Geräten für die Sicherheit in der Informationstechnik (IT-Sicherheitsprodukte), soweit dies zur Erfüllung von Aufgaben des Bundes erforderlich ist, einschließlich der Forschung im Rahmen seiner gesetzlichen Aufgaben;	
112	4. Entwicklung von Kriterien, Verfahren und Werkzeugen für die Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen oder Komponenten und für die Prüfung und Bewertung der Konformität im Bereich der IT-Sicherheit;	4. Entwicklung von Kriterien, Verfahren und Werkzeugen für die Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen oder Komponenten und für die Prüfung und Bewertung der Konformität im Bereich der IT-Sicherheit;	
113		4a. Durchführung von Peer Reviews nach Artikel 19 der NIS-2-Richtlinie;	Umsetzung von Art. 19 NIS-2 in Form einer Aufgabe des Bundesamtes.
114	5. Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen oder Komponenten und Erteilung von Sicherheitszertifikaten;	5. Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen oder Komponenten und Erteilung von Sicherheitszertifikaten;	
115	5a. Wahrnehmung der Aufgaben und Befugnisse nach Artikel 58 Absatz 7 und 8 der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit, ABl. L 151 vom 7.6.2019, S. 15) als	5a. Wahrnehmung der Aufgaben und Befugnisse nach Artikel 58 Absatz 7 und 8 der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit, ABl. L 151 vom 7.6.2019, S. 15) als	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	nationale Behörde für die Cybersicherheitszertifizierung;	nationale Behörde für die Cybersicherheitszertifizierung;	
116	6. Prüfung und Bestätigung der Konformität im Bereich der IT-Sicherheit von informationstechnischen Systemen und Komponenten mit technischen Richtlinien des Bundesamtes;	6. Prüfung und Bestätigung der Konformität im Bereich der IT-Sicherheit von informationstechnischen Systemen und Komponenten mit technischen Richtlinien des Bundesamtes;	
117	7. Prüfung, Bewertung und Zulassung von informationstechnischen Systemen oder Komponenten, die für die Verarbeitung amtlich geheim gehaltener Informationen nach § 4 des Sicherheitsüberprüfungsgesetzes im Bereich des Bundes oder bei Unternehmen im Rahmen von Aufträgen des Bundes eingesetzt werden sollen;	7. Prüfung, Bewertung und Zulassung von informationstechnischen Systemen oder Komponenten, die für die Verarbeitung amtlich geheim gehaltener Informationen nach § 4 des Sicherheitsüberprüfungsgesetzes im Bereich des Bundes oder bei Unternehmen im Rahmen von Aufträgen des Bundes eingesetzt werden sollen;	
118	8. Herstellung von Schlüsseldaten und Betrieb von Krypto- und Sicherheitsmanagementsystemen für informationssichernde Systeme des Bundes, die im Bereich des staatlichen Geheimschutzes oder auf Anforderung der betroffenen Behörde auch in anderen Bereichen eingesetzt werden;	8. Herstellung von Schlüsseldaten und Betrieb von Krypto- und Sicherheitsmanagementsystemen für informationssichernde Systeme des Bundes, die im Bereich des staatlichen Geheimschutzes oder auf Anforderung der betroffenen Behörde auch in anderen Bereichen eingesetzt werden;	
119	9. Unterstützung und Beratung bei organisatorischen und technischen Sicherheitsmaßnahmen sowie Durchführung von technischen Prüfungen zum Schutz amtlich geheim gehaltener Informationen nach § 4 des Sicherheitsüberprüfungsgesetzes gegen die Kenntnisnahme durch Unbefugte;	9. Unterstützung und Beratung bei organisatorischen und technischen Sicherheitsmaßnahmen sowie Durchführung von technischen Prüfungen zum Schutz amtlich geheim gehaltener Informationen nach § 4 des Sicherheitsüberprüfungsgesetzes gegen die Kenntnisnahme durch Unbefugte;	
120	10. Entwicklung von sicherheitstechnischen Anforderungen an die einzusetzende	10. Entwicklung von sicherheitstechnischen Anforderungen an die einzusetzende	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Informationstechnik des Bundes und an die Eignung von Auftragnehmern im Bereich von Informationstechnik mit besonderem Schutzbedarf;	Informationstechnik des Bundes und an die Eignung von Auftragnehmern im Bereich von Informationstechnik mit besonderem Schutzbedarf;	
121	11. Bereitstellung von IT-Sicherheitsprodukten für Stellen des Bundes;	11. Bereitstellung von IT-Sicherheitsprodukten für Einrichtungen der Bundesverwaltung;	Begriffskonsolidierung/Erweiterung des Anwendungsbereichs auf Einrichtungen der Bundesverwaltung. Die Erweiterung erfolgt zum Zwecke eines einheitlich hohen Sicherheitsniveaus für alle Einrichtungen, die Informationstechnik des Bundes betreiben.
122	12. Unterstützung der für Sicherheit in der Informationstechnik zuständigen Stellen des Bundes, insbesondere soweit sie Beratungs- oder Kontrollaufgaben wahrnehmen; dies gilt vorrangig für den Bundesbeauftragten für den Datenschutz, dessen Unterstützung im Rahmen der Unabhängigkeit erfolgt, die ihm bei der Erfüllung seiner Aufgaben nach dem Bundesdatenschutzgesetz zusteht;	12. Unterstützung der für Sicherheit in der Informationstechnik zuständigen Stellen des Bundes, insbesondere soweit sie Beratungs- oder Kontrollaufgaben wahrnehmen; dies gilt vorrangig für den Bundesbeauftragten für den Datenschutz, dessen Unterstützung im Rahmen der Unabhängigkeit erfolgt, die ihm bei der Erfüllung seiner Aufgaben nach dem Bundesdatenschutzgesetz zusteht;	Hier Beibehaltung von Stellen des Bundes, da eine Erweiterung auch alle Einrichtungen der Bundesverwaltung zu erheblich größerem Erfüllungsaufwand führen würde, was nicht im Verhältnis zum Nutzen stehen würde.
123	12a. Beratung und Unterstützung der Stellen des Bundes in Fragen der Sicherheit in der Informationstechnik;	12a. Beratung und Unterstützung der Einrichtungen der Bundesverwaltung in Fragen der Sicherheit in der Informationstechnik;	Begriffskonsolidierung zu Einrichtungen der Bundesverwaltung. Komplementär zur Verpflichtung weiterer Einrichtungen auf Vorgaben des Bundesamts ist auch die Beratungs- und Unterstützungsaufgabe des BSI auf diese Einrichtungen zu erweitern.
124	13. Unterstützung	13. Unterstützung	
125	a) der Polizeien und Strafverfolgungsbehörden bei der Wahrnehmung ihrer gesetzlichen Aufgaben,	a) der Polizeien und Strafverfolgungsbehörden bei der Wahrnehmung ihrer gesetzlichen Aufgaben,	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
126	b) der Verfassungsschutzbehörden und des Militärischen Abschirmdienstes bei der Auswertung und Bewertung von Informationen, die bei der Beobachtung terroristischer Bestrebungen oder nachrichtendienstlicher Tätigkeiten im Rahmen der gesetzlichen Befugnisse nach den Verfassungsschutzgesetzen des Bundes und der Länder beziehungsweise dem MAD-Gesetz anfallen,	b) der Verfassungsschutzbehörden und des Militärischen Abschirmdienstes bei der Auswertung und Bewertung von Informationen, die bei der Beobachtung terroristischer Bestrebungen oder nachrichtendienstlicher Tätigkeiten im Rahmen der gesetzlichen Befugnisse nach den Verfassungsschutzgesetzen des Bundes und der Länder beziehungsweise dem MAD-Gesetz anfallen,	
127	c) des Bundesnachrichtendienstes bei der Wahrnehmung seiner gesetzlichen Aufgaben.	c) des Bundesnachrichtendienstes bei der Wahrnehmung seiner gesetzlichen Aufgaben,	
128	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. Die Unterstützungsersuchen sind durch das Bundesamt aktenkundig zu machen;	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; die Unterstützungsersuchen sind durch das Bundesamt aktenkundig zu machen;	Redaktionelle Änderung
129	13a. auf Ersuchen der zuständigen Stellen der Länder Unterstützung dieser Stellen in Fragen der Abwehr von Gefahren für die Sicherheit in der Informationstechnik;	13a. auf Ersuchen der zuständigen Stellen der Länder Unterstützung dieser Stellen in Fragen der Abwehr von Gefahren für die Sicherheit in der Informationstechnik;	
130	14. Beratung, Information und Warnung der Stellen des Bundes, der Länder sowie der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik, insbesondere unter Berücksichtigung der möglichen Folgen	14. Beratung, Information und Warnung der Einrichtungen der Bundesverwaltung, der Länder sowie der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik, insbesondere unter Berücksichtigung der möglichen	Begriffskonsolidierung zu Einrichtungen der Bundesverwaltung, damit Umkehrschluss vermieden wird, dass die über Stellen des Bundes hinausgehenden Einrichtungen nicht erfasst seien.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	fehlender oder unzureichender Sicherheitsvorkehrungen;	Folgen fehlender oder unzureichender Sicherheitsvorkehrungen;	
131	14a. Verbraucherschutz und Verbraucherinformation im Bereich der Sicherheit in der Informationstechnik, insbesondere durch Beratung und Warnung von Verbrauchern in Fragen der Sicherheit in der Informationstechnik und unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen;	14a. Verbraucherschutz und Verbraucherinformation im Bereich der Sicherheit in der Informationstechnik, insbesondere durch Beratung und Warnung von Verbrauchern in Fragen der Sicherheit in der Informationstechnik und unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen;	
132	15. Aufbau geeigneter Kommunikationsstrukturen zur Krisenfrüherkennung, Krisenreaktion und Krisenbewältigung sowie Koordinierung der Zusammenarbeit zum Schutz der Sicherheit in der Informationstechnik Kritischer Infrastrukturen im Verbund mit der Privatwirtschaft;	15. Aufbau geeigneter Kommunikationsstrukturen zur Krisenfrüherkennung, Krisenreaktion und Krisenbewältigung sowie Koordinierung der Zusammenarbeit zum Schutz der Sicherheit in der Informationstechnik Kritischer Anlagen im Verbund mit der Privatwirtschaft;	
133	16. Aufgaben als zentrale Stelle im Bereich der Sicherheit in der Informationstechnik im Hinblick auf die Zusammenarbeit mit den zuständigen Stellen im Ausland, unbeschadet besonderer Zuständigkeiten anderer Stellen;	16. Aufgaben als zentrale Stelle im Bereich der Sicherheit in der Informationstechnik im Hinblick auf die Zusammenarbeit mit den zuständigen Stellen im Ausland, unbeschadet besonderer Zuständigkeiten anderer Stellen;	
134	17. Aufgaben nach den §§ 8a bis 8c und 8f als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen, digitaler Dienste und der Unternehmen im besonderen öffentlichen Interesse;	17. Aufgaben nach § 40 als zentrale Stelle für die Sicherheit in der Informationstechnik von Betreibern kritischer Anlagen, besonders wichtigen Einrichtungen und wichtigen Einrichtungen einschließlich des Ersuchens und Erbringens von Amtshilfe nach Artikel 37 der NIS-2-Richtinie;	Folgeänderung Aufgrund Anpassung der Systematik – Betreiber Kritischer Infrastrukturen nunmehr einheitlich Betreiber kritischer Anlagen, ferner gehen Anbieter digitaler Dienste und UBI in Wesentliche Einrichtungen und Wichtige Einrichtungen auf.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
135	18. Unterstützung bei der Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen nach § 5a;	18. Unterstützung bei der Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen nach § 11;	Redaktionelle Änderung aufgrund fehlerhaftem Verweis auf § 5a aF. anstatt § 5b aF., letzterer nunmehr § 11.
136	19. Empfehlungen für Identifizierungs- und Authentisierungsverfahren und Bewertung dieser Verfahren im Hinblick auf die Informationssicherheit;	19. Empfehlungen für Identifizierungs- und Authentisierungsverfahren und Bewertung dieser Verfahren im Hinblick auf die Informationssicherheit;	
137	20. Beschreibung und Veröffentlichung eines Stands der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte unter Berücksichtigung bestehender Normen und Standards sowie Einbeziehung der betroffenen Wirtschaftsverbände.	20. Beschreibung und Veröffentlichung eines Stands der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte unter Berücksichtigung bestehender Normen und Standards sowie Einbeziehung der betroffenen Wirtschaftsverbände.	
138		21. Kooperation mit und Unterstützung für nationale Computer-Notfallteams von Drittländern oder gleichwertigen Stellen von Drittländern; im Fall von Einsätzen des Bundesamtes im Ausland darf dies nicht gegen den Willen des Staates erfolgen, auf dessen Hoheitsgebiet die Maßnahme stattfinden soll; die Entscheidung über einen Einsatz des Bundesamtes im Ausland trifft das Bundesministerium des Innern und für Heimat.	Umsetzung Art. 10 Abs. 8 NIS-2.
139	(2) Das Bundesamt kann die Länder auf Ersuchen bei der Sicherung ihrer Informationstechnik unterstützen.	(2) Das Bundesamt kann die Länder auf Ersuchen bei der Sicherung ihrer Informationstechnik unterstützen.	
140	(3) Das Bundesamt kann Betreiber Kritischer Infrastrukturen auf deren Ersuchen bei der Sicherung ihrer Informationstechnik beraten und unterstützen	(3) Das Bundesamt kann Betreiber kritischer Anlagen auf deren Ersuchen bei der Sicherung ihrer	Folgeänderung aufgrund neuer Systematik

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	oder auf qualifizierte Sicherheitsdienstleister verweisen.	Informationstechnik beraten und unterstützen oder auf qualifizierte Sicherheitsdienstleister verweisen.	
141	§ 3a Verarbeitung personenbezogener Daten		Verschoben nach § 20 nF.
142	(1) Die Verarbeitung personenbezogener Daten durch das Bundesamt ist zulässig, wenn die Verarbeitung zur Erfüllung seiner im öffentlichen Interesse liegenden Aufgaben erforderlich ist.		s.o.
143	(2) Die Verarbeitung personenbezogener Daten durch das Bundesamt zu anderen Zwecken als demjenigen, zu dem die Daten ursprünglich erhoben wurden, ist unbeschadet von Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2) in der jeweils geltenden Fassung und von § 23 des Bundesdatenschutzgesetzes zulässig, wenn		s.o.
144	1. die Verarbeitung erforderlich ist		s.o.
145	a) zur Sammlung, Auswertung oder Untersuchung von Informationen über Sicherheitsrisiken oder Sicherheitsvorkehrungen für die Informationstechnik oder		s.o.
146	b) zur Unterstützung, Beratung oder Warnung in Fragen der Sicherheit in der Informationstechnik und		s.o.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
147	2. kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.		s.o.
148	(3) Eine Verarbeitung von besonderen Kategorien personenbezogener Daten durch das Bundesamt ist abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 und unbeschadet des § 22 Absatz 1 des Bundesdatenschutzgesetzes zulässig, wenn		s.o.
149	1. die Verarbeitung erforderlich ist zur Abwehr einer erheblichen Gefahr für die Netz-, Daten- oder Informationssicherheit,		s.o.
150	2. ein Ausschluss dieser Daten von der Verarbeitung die Erfüllung der Aufgaben des Bundesamtes unmöglich machen oder diese erheblich gefährden würde und		s.o.
151	3. kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss dieser Daten von der Verarbeitung überwiegt.		s.o.
152	(4) Das Bundesamt sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2 des Bundesdatenschutzgesetzes vor.		s.o.
153	§ 4 Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes	§ 4 Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes	
154	(1) Das Bundesamt ist die zentrale Meldestelle für die Zusammenarbeit der Bundesbehörden in	(1) Das Bundesamt ist die zentrale Meldestelle für die Zusammenarbeit der Einrichtungen der	Begriffskonsolidierung: Einrichtungen der Bundesverwaltung

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Angelegenheiten der Sicherheit in der Informationstechnik.	Bundesverwaltung in Angelegenheiten der Sicherheit in der Informationstechnik.	
155	(2) Das Bundesamt hat zur Wahrnehmung dieser Aufgabe	(2) Das Bundesamt hat zur Wahrnehmung dieser Aufgabe	(unverändert)
156	1. alle für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik erforderlichen Informationen, insbesondere zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und der dabei beobachteten Vorgehensweise, zu sammeln und auszuwerten,	1. alle für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik erforderlichen Informationen, insbesondere zu Schwachstellen, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und der dabei beobachteten Vorgehensweise, zu sammeln und auszuwerten,	redaktionelle Anpassung, da nur noch Schwachstelle definiert wird
157	2. die Bundesbehörden unverzüglich über die sie betreffenden Informationen nach Nummer 1 und die in Erfahrung gebrachten Zusammenhänge zu unterrichten.	2. die Einrichtungen der Bundesverwaltung unverzüglich über die sie betreffenden Informationen nach Nummer 1 und die in Erfahrung gebrachten Zusammenhänge zu unterrichten.	Begriffskonsolidierung: Einrichtungen der Bundesverwaltung
158	(3) Werden anderen Bundesbehörden Informationen nach Absatz 2 Nummer 1 bekannt, die für die Erfüllung von Aufgaben oder die Sicherheit der Informationstechnik anderer Behörden von Bedeutung sind, unterrichten diese ab dem 1. Januar 2010 das Bundesamt hierüber unverzüglich, soweit andere Vorschriften dem nicht entgegenstehen.		Verschoben nach § 43 nF. da es sich um eine Pflicht für Einrichtungen der Bundesverwaltung handelt.
159	(4) Ausgenommen von den Unterrichtungspflichten nach Absatz 2 Nummer 2 und Absatz 3 sind Informationen, die aufgrund von Regelungen zum Geheimschutz oder Vereinbarungen mit Dritten nicht weitergegeben werden dürfen oder deren Weitergabe im Widerspruch zu der verfassungsrechtlichen Stellung eines Abgeordneten des Bundestages oder eines	(4) Ausgenommen von den Unterrichtungspflichten nach Absatz 2 Nummer 2 sind Informationen, die aufgrund von Regelungen zum Geheimschutz oder Vereinbarungen mit Dritten nicht weitergegeben werden dürfen oder deren Weitergabe im Widerspruch zu der verfassungsrechtlichen Stellung eines Abgeordneten des Bundestages oder eines	Folgeänderung wg. Verschiebung von Abs. 3 aF.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Verfassungsorgans oder der gesetzlich geregelten Unabhängigkeit einzelner Stellen stünde.	Verfassungsorgans oder der gesetzlich geregelten Unabhängigkeit einzelner Stellen stünde.	
160	(5) Die Vorschriften zum Schutz personenbezogener Daten bleiben unberührt.		Entfällt mangels eigener Regelungswirkung.
161	(6) Das Bundesministerium des Innern, für Bau und Heimat erlässt nach Zustimmung durch den Rat der IT-Beauftragten der Bundesregierung allgemeine Verwaltungsvorschriften zur Durchführung des Absatzes 3.		Verschoben nach § 43 nF. (Folgeänderung zu Abs. 3)
162	*§ 4b* *Allgemeine Meldestelle für die Sicherheit in der Informationstechnik*	§ 5 Allgemeine Meldestelle für die Sicherheit in der Informationstechnik	Verschoben von § 4b aF.
163	*(1) Zur Wahrnehmung der Aufgaben nach § 3 nimmt das Bundesamt als zentrale Stelle für Meldungen von Dritten Informationen über Sicherheitsrisiken in der Informationstechnik entgegen und wertet diese Informationen aus.*	(1) Zur Wahrnehmung der Aufgaben nach § 3 nimmt das Bundesamt als zentrale Stelle für Meldungen von Dritten Informationen über Sicherheitsrisiken in der Informationstechnik entgegen und wertet diese Informationen aus. Das Bundesamt ist dabei der nationale Koordinator für die Zwecke einer koordinierten Offenlegung von Schwachstellen im Sinne des Artikels 12 Absatz 1 der NIS-2-Richtlinie.	Umsetzung Art. 12 Abs. 1 Satz 1 NIS-2 (entsprechend zu § 9a BSIG aF.).
164	*(2) Das Bundesamt nimmt zur Wahrnehmung der Aufgaben nach Absatz 1 Informationen zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und der dabei beobachteten Vorgehensweisen entgegen. Das Bundesamt richtet hierzu geeignete Meldemöglichkeiten ein. Die Meldungen können anonym erfolgen. Soweit die Meldung nicht anonym erfolgt, kann der Meldende mit der Meldung oder später verlangen, dass seine personenbezogenen Daten nur anonymisiert weitergegeben werden dürfen. Dies gilt nicht in den Fällen des § 5 Absatz 5 und 6 Satz 1. Eine Übermittlung*	(2) Das Bundesamt nimmt zur Wahrnehmung der Aufgaben nach Absatz 1 Informationen zu Schwachstellen, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und der dabei beobachteten Vorgehensweisen sowie zu Sicherheitsvorfällen, Cyberbedrohungen und Beinahevorfällen entgegen. Das Bundesamt richtet hierzu geeignete Meldemöglichkeiten ein. Die Meldungen können anonym erfolgen. Soweit die Meldung nicht anonym erfolgt, kann der Meldende mit der Meldung oder später verlangen, dass seine personenbezogenen Daten nur anonymisiert weitergegeben werden dürfen. Dies gilt	Anpassung zur Umsetzung Art. 30 Abs. 1 NIS-2; im Übrigen redaktionelle Änderung von „Sicherheitslücke“ auf „Schwachstelle“.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	der personenbezogenen Daten in den Fällen von § 5 Absatz 5 und 6 Satz 1 hat zu unterbleiben, wenn für das Bundesamt erkennbar ist, dass die schutzwürdigen Interessen des Meldenden das Allgemeininteresse an der Übermittlung überwiegen. Zu berücksichtigen ist dabei auch die Art und Weise, mittels derer der Meldende die Erkenntnisse gewonnen hat. Die Entscheidung nach Satz 6 muss dem oder der behördlichen Datenschutzbeauftragten des Bundesamtes sowie einem oder einer weiteren Bediensteten des Bundesamtes, der oder die die Befähigung zum Richteramt hat, zur vorherigen Prüfung vorgelegt werden.	nicht in den Fällen des § 8 Absatz 5 und 6 Satz 1. Eine Übermittlung der personenbezogenen Daten in den Fällen von § 8 Absatz 5 und 6 Satz 1 hat zu unterbleiben, wenn für das Bundesamt erkennbar ist, dass die schutzwürdigen Interessen des Meldenden das Allgemeininteresse an der Übermittlung überwiegen. Zu berücksichtigen ist dabei auch die Art und Weise, mittels derer der Meldende die Erkenntnisse gewonnen hat. Die Entscheidung nach Satz 6 muss dem oder der behördlichen Datenschutzbeauftragten des Bundesamtes sowie einem oder einer weiteren Bediensteten des Bundesamtes, der oder die die Befähigung zum Richteramt hat, zur vorherigen Prüfung vorgelegt werden.	
165	*(3) Das Bundesamt soll die gemäß Absatz 2 gemeldeten Informationen nutzen, um*	(3) Das Bundesamt soll die gemäß Absatz 2 gemeldeten Informationen nutzen, um	
166	*1. Dritte über bekannt gewordene Sicherheitslücken, Schadprogramme, erfolgte oder versuchte Angriffe auf die Sicherheit in der Informationstechnik zu informieren, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist,*	1. Dritte über bekannt gewordene Schwachstellen, Schadprogramme, erfolgte oder versuchte Angriffe auf die Sicherheit in der Informationstechnik zu informieren, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist,	redaktionelle Anpassung, da nur noch Schwachstelle definiert wird
167	*2. die Öffentlichkeit oder betroffene Kreise gemäß § 7 zu warnen und zu informieren,*	2. die Öffentlichkeit oder betroffene Kreise gemäß § 13 zu warnen und zu informieren,	
168	*3. Bundesbehörden gemäß § 4 Absatz 2 Nummer 2 über die sie betreffenden Informationen zu unterrichten,*	3. Einrichtungen der Bundesverwaltung gemäß § 4 Absatz 2 Nummer 2 über die sie betreffenden Informationen zu unterrichten,	Begriffskonsolidierung: Einrichtungen der Bundesverwaltung.
169	*4. Betreiber Kritischer Infrastrukturen und Unternehmen im öffentlichen Interesse gemäß § 8b Absatz 2 Nummer 4*	4. Betreiber kritischer Anlagen, besonders wichtige Einrichtungen und wichtige Einrichtungen gemäß § 38 Absatz 2	Folgeänderung aufgrund der neuen Systematik

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Buchstabe a über die sie betreffenden Informationen zu unterrichten.	Nummer 4 Buchstabe a über die sie betreffenden Informationen zu unterrichten.	
170		5. seine Aufgaben als zuständige Behörde, CSIRT und zentrale Anlaufstelle im Sinne der NIS-2-Richtlinie wahrzunehmen	Umsetzung Art. 30 Abs. 2 NIS-2.
171	*(4) Eine Weitergabe nach Absatz 3 Nummer 1, 2 oder 4 erfolgt nicht, soweit die gemäß Absatz 2 gemeldeten Informationen*	(4) Eine Weitergabe nach Absatz 3 Nummer 1, 2 oder 4 erfolgt nicht, soweit die gemäß Absatz 2 gemeldeten Informationen	
172	*1. Betriebs- und Geschäftsgeheimnisse von Dritten beinhalten und die Maßnahmen nach Absatz 3 nicht ohne Bekanntgabe dieser Betriebs- und Geschäftsgeheimnisse durchgeführt werden können oder*	1. Betriebs- und Geschäftsgeheimnisse von Dritten beinhalten und die Maßnahmen nach Absatz 3 nicht ohne Bekanntgabe dieser Betriebs- und Geschäftsgeheimnisse durchgeführt werden können oder	
173	*2. auf Grund von Vereinbarungen des Bundesamtes mit Dritten nicht übermittelt werden dürfen.*	2. auf Grund von Vereinbarungen des Bundesamtes mit Dritten nicht übermittelt werden dürfen.	
174	*(5) Sonstige gesetzliche Meldepflichten, Regelungen zum Geheimschutz, gesetzliche Übermittlungshindernisse und Übermittlungsregelungen bleiben unberührt.*	(5) Sonstige gesetzliche Meldepflichten, Regelungen zum Geheimschutz, gesetzliche Übermittlungshindernisse und Übermittlungsregelungen bleiben unberührt.	
175		§ 6 Informationsaustausch	Umsetzung Art. 29 NIS-2
176		(1) Das Bundesamt ermöglicht den Informationsaustausch von Betreibern kritischer Anlagen, besonders wichtigen Einrichtungen und wichtigen Einrichtungen, Einrichtungen der Bundesverwaltung sowie deren jeweiligen Lieferanten oder Dienstleistern untereinander zu Cyberbedrohungen, Beinahevorfällen, Schwachstellen,	Das Bundesamt ermöglicht den Informationsaustausch zu Cyberbedrohungen (§ 2 Abs. 1 Nr. 4), Beinahevorfällen (§ 2 Abs. 1 Nr. 1), Schwachstellen (§ 2 Abs. 1 Nr. 35), Techniken und Verfahren (*techniques and procedures*),

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		Techniken und Verfahren, Kompromittierungsindikatoren, gegnerische Taktiken, bedrohungsspezifische Informationen, Cybersicherheitswarnungen und Empfehlungen für die Konfiguration von Cybersicherheitsinstrumenten sowie zur Aufdeckung von Cyberangriffen. Es betreibt dazu ein geeignetes Online-Portal.	Kompromittierungsindikatoren (*indicators of compromise*), gegnerische Taktiken (*adversarial tactics*), bedrohungsspezifische Informationen (*threat-actor-specific information*), Cybersicherheitswarnungen und Empfehlungen für die Konfiguration von Cybersicherheitsinstrumenten sowie zur Aufdeckung von Cyberangriffen.
177		(2) Die Teilnahme am Informationsaustausch steht grundsätzlich allen Betreibern kritischer Anlagen, besonders wichtigen Einrichtungen, wichtigen Einrichtungen, Einrichtungen der Bundesverwaltung sowie deren jeweiligen Lieferanten oder Dienstleistern offen. Das Bundesamt kann entsprechende Teilnahmebedingungen erstellen, die die Teilnahme am Informationsaustausch regeln. Das Bundesamt kann weiteren Stellen die Teilnahme ermöglichen.	
178	§ 4a Kontrolle der Kommunikationstechnik des Bundes, Betretensrechte	§ 7 Kontrolle der Kommunikationstechnik des Bundes, Betretensrechte	Neue Enummerierung.
179	(1) Das Bundesamt ist befugt, die Sicherheit der Kommunikationstechnik des Bundes und ihrer Komponenten, einschließlich technischer Infrastrukturen, die zum Betrieb der Kommunikationstechnik des Bundes erforderlich sind, zu kontrollieren. Es kann hierzu die Bereitstellung der zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1 und 14 erforderlichen Informationen, insbesondere zu technischen Details, zu Strategien, Planungen und Regelungen mit Bezug zur Kommunikationstechnik des Bundes einschließlich Aufbau- und Ablauforganisation verlangen sowie	(1) Das Bundesamt ist befugt, die Sicherheit der Kommunikationstechnik des Bundes und ihrer Komponenten, einschließlich technischer Infrastrukturen, die zum Betrieb der Kommunikationstechnik des Bundes erforderlich sind, zu kontrollieren. Es kann hierzu die Bereitstellung der zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1 und 14 erforderlichen Informationen, insbesondere zu technischen Details, zu Strategien, Planungen und Regelungen mit Bezug zur Kommunikationstechnik des Bundes einschließlich Aufbau- und Ablauforganisation verlangen sowie	Redaktionelle Änderung.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Unterlagen und Datenträger des Betreibers der jeweiligen Kommunikationstechnik des Bundes oder eines mit Betriebsleistungen beauftragten Dritten einsehen und die unentgeltliche Herausgabe von Kopien dieser Unterlagen und Dokumente, auch in elektronischer Form, verlangen, soweit nicht Geheimschutzinteressen oder überwiegende Sicherheitsinteressen des Betreibers im Sinne des Satzes 2 entgegenstehen.	Unterlagen und Datenträger des Betreibers der jeweiligen Kommunikationstechnik des Bundes oder eines mit Betriebsleistungen beauftragten Dritten einsehen und die unentgeltliche Herausgabe von Kopien dieser Unterlagen und Dokumente, auch in elektronischer Form, verlangen, soweit nicht Geheimschutzinteressen oder überwiegende Sicherheitsinteressen des Betreibers entgegenstehen.	
180	(2) Dem Bundesamt ist in den Zeiten, zu denen die Räume normalerweise für die jeweilige geschäftliche oder betriebliche Nutzung zur Verfügung stehen, zu den Grundstücken und Betriebsräumen, einschließlich Datenverarbeitungsanlagen und -geräten, die für die Kommunikationstechnik des Bundes verwendet werden, Zugang zu gewähren, soweit dies zur Erfüllung der Zwecke nach Absatz 1 erforderlich ist.	(2) Dem Bundesamt ist in den Zeiten, zu denen die Räume normalerweise für die jeweilige geschäftliche oder betriebliche Nutzung zur Verfügung stehen, zu den Grundstücken und Betriebsräumen, einschließlich Datenverarbeitungsanlagen und -geräten, die für die Kommunikationstechnik des Bundes verwendet werden, Zugang zu gewähren, soweit dies zur Erfüllung der Zwecke nach Absatz 1 erforderlich ist.	(unverändert)
181	(3) Bei Einrichtungen eines Dritten, bei dem eine Schnittstelle zur Kommunikationstechnik des Bundes besteht, kann das Bundesamt auf der Schnittstellenseite der Einrichtung nur mit Zustimmung des Dritten die Sicherheit der Schnittstelle kontrollieren. Es kann hierzu mit Zustimmung des Dritten die zur Aufgabenerfüllung erforderlichen Informationen, insbesondere zu technischen Details, zu Strategien, Planungen und Regelungen sowie Unterlagen und Datenträger des Betreibers einsehen und unentgeltlich Kopien, auch in elektronischer Form, anfertigen.	(3) Bei Anlagen eines Dritten, bei dem eine Schnittstelle zur Kommunikationstechnik des Bundes besteht, kann das Bundesamt auf der Schnittstellenseite der Einrichtung nur mit Zustimmung des Dritten die Sicherheit der Schnittstelle kontrollieren. Es kann hierzu mit Zustimmung des Dritten die zur Aufgabenerfüllung erforderlichen Informationen, insbesondere zu technischen Details, zu Strategien, Planungen und Regelungen sowie Unterlagen und Datenträger des Betreibers einsehen und unentgeltlich Kopien, auch in elektronischer Form, anfertigen.	(unverändert)
182	(4) Das Bundesamt teilt das Ergebnis seiner Kontrolle nach den Absätzen 1 bis 3 dem jeweiligen überprüften Betreiber sowie im Falle einer öffentlichen Stelle des Bundes der zuständigen Rechts- und Fachaufsicht mit. Mit der Mitteilung soll es Vorschläge zur Verbesserung der Informationssicherheit,	(4) Das Bundesamt teilt das Ergebnis seiner Kontrolle nach den Absätzen 1 bis 3 dem jeweiligen überprüften Betreiber, im Falle einer Einrichtung der Bundesverwaltung zusätzlich der zuständigen Rechts- und Fachaufsicht, der oder dem jeweiligen Informationssicherheitsbeauftragten des Ressorts sowie dem Koordinator oder der Koordinatorin für Informationssicherheit mit. Mit der Mitteilung soll es	Begriffskonsolidierung: Einrichtungen der Bundesverwaltung. Ausweitung der Mitteilungspflichten des Bundesamtes auf die mit diesem Gesetz geschaffenen verantwortlichen Stellen für das Informationssicherheitsmanagements des Bundes.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	insbesondere zur Beseitigung der festgestellten Mängel, verbinden.	Vorschläge zur Verbesserung der Informationssicherheit, insbesondere zur Beseitigung der festgestellten Mängel, verbinden.	
183	(5) Ausgenommen von den Befugnissen nach den Absätzen 1 bis 3 sind Kontrollen der Auslandsinformations- und -kommunikationstechnik im Sinne des § 9 Absatz 2 des Gesetzes über den Auswärtigen Dienst, soweit sie ausschließlich im Ausland belegen ist oder für das Ausland oder für Anwender im Ausland betrieben wird. Die Bestimmungen für die Schnittstellen der Kommunikationstechnik des Bundes im Inland bleiben davon unberührt. Näheres zu Satz 1 regelt eine Verwaltungsvereinbarung zwischen dem Bundesministerium des Innern, für Bau und Heimat und dem Auswärtigen Amt.	(5) Ausgenommen von den Befugnissen nach den Absätzen 1 bis 3 sind Kontrollen der Auslandsinformations- und -kommunikationstechnik im Sinne des § 9 Absatz 2 des Gesetzes über den Auswärtigen Dienst, soweit sie ausschließlich im Ausland belegen ist oder für das Ausland oder für Anwender im Ausland betrieben wird. Die Bestimmungen für die Schnittstellen der Kommunikationstechnik des Bundes im Inland bleiben davon unberührt. Näheres zu Satz 1 regelt eine Verwaltungsvereinbarung zwischen dem Bundesministerium des Innern und für Heimat und dem Auswärtigen Amt.	Redaktionelle Änderung.
184	(6) Die Befugnisse nach den Absätzen 1 bis 3 gelten im Geschäftsbereich des Bundesministeriums der Verteidigung nicht für die Kontrolle der Informations- und Kommunikationstechnik, die von den Streitkräften für ihre Zwecke oder dem Militärischen Abschirmdienst genutzt wird. Nicht ausgenommen ist die Informations- und Kommunikationstechnik von Dritten, insbesondere von IT-Dienstleistern, soweit sie nicht ausschließlich für die Zwecke der Streitkräfte betrieben wird. Die Bestimmungen für die Schnittstellen der Kommunikationstechnik des Bundes bleiben von den Sätzen 1 und 2 unberührt. Näheres regelt eine Verwaltungsvereinbarung zwischen dem Bundesministerium des Innern, für Bau und Heimat und dem Bundesministerium der Verteidigung.	(6) Die Befugnisse nach den Absätzen 1 bis 3 gelten im Geschäftsbereich des Bundesministeriums der Verteidigung nicht für die Kontrolle der Informations- und Kommunikationstechnik, die von den Streitkräften für ihre Zwecke oder dem Militärischen Abschirmdienst genutzt wird. Nicht ausgenommen ist die Informations- und Kommunikationstechnik von Dritten, insbesondere von IT-Dienstleistern, soweit sie nicht ausschließlich für die Zwecke der Streitkräfte betrieben wird. Die Bestimmungen für die Schnittstellen der Kommunikationstechnik des Bundes bleiben von den Sätzen 1 und 2 unberührt. Näheres regelt eine Verwaltungsvereinbarung zwischen dem Bundesministerium des Innern und für Heimat und dem Bundesministerium der Verteidigung.	Redaktionelle Änderungen.
185		(7) Das Bundesamt unterrichtet kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres den Haushaltsausschuss des	Die Vorschrift dient dem Ziel, mehr Umsetzungsverantwortung zu schaffen. Bislang sind die Prüfungen nach § 4a BSIG aF. ohne greifbare Konsequenz für die überprüften Stellen. Der Bericht

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		Deutschen Bundestages über die Anwendung dieser Vorschrift.	erfolgt an den Haushaltsauschuss des Deutschen Bundestages, weil dadurch an die Stelle berichtet wird, die über Mittel verfügt, eine Beseitigung von Missständen zu ermöglichen. Eine allgemeine Berichtspflicht gegenüber dem Ausschuss für Inneres und Heimat des Deutschen Bundestages besteht gem. § 53 Absatz 3 ohnehin, sie schließt Berichterstattung über die Anwendung dieser Vorschrift ein.
186	§ 4b Allgemeine Meldestelle für die Sicherheit in der Informationstechnik		§ 4b aF. verschoben nach § 5 nF.
187	(1) Zur Wahrnehmung der Aufgaben nach § 3 nimmt das Bundesamt als zentrale Stelle für Meldungen von Dritten Informationen über Sicherheitsrisiken in der Informationstechnik entgegen und wertet diese Informationen aus.		s.o.
188	(2) Das Bundesamt nimmt zur Wahrnehmung der Aufgaben nach Absatz 1 Informationen zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und der dabei beobachteten Vorgehensweisen entgegen. Das Bundesamt richtet hierzu geeignete Meldemöglichkeiten ein. Die Meldungen können anonym erfolgen. Soweit die Meldung nicht anonym erfolgt, kann der Meldende mit der Meldung oder später verlangen, dass seine personenbezogenen Daten nur anonymisiert weitergegeben werden dürfen. Dies gilt nicht in den Fällen des § 5 Absatz 5 und 6 Satz 1. Eine Übermittlung der personenbezogenen Daten in den Fällen von § 5 Absatz 5 und 6 Satz 1 hat zu unterbleiben, wenn für das		s.o.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Bundesamt erkennbar ist, dass die schutzwürdigen Interessen des Meldenden das Allgemeininteresse an der Übermittlung überwiegen. Zu berücksichtigen ist dabei auch die Art und Weise, mittels derer der Meldende die Erkenntnisse gewonnen hat. Die Entscheidung nach Satz 6 muss dem oder der behördlichen Datenschutzbeauftragten des Bundesamtes sowie einem oder einer weiteren Bediensteten des Bundesamtes, der oder die die Befähigung zum Richteramt hat, zur vorherigen Prüfung vorgelegt werden.		
189	(3) Das Bundesamt soll die gemäß Absatz 2 gemeldeten Informationen nutzen, um		s.o.
190	1. Dritte über bekannt gewordene Sicherheitslücken, Schadprogramme, erfolgte oder versuchte Angriffe auf die Sicherheit in der Informationstechnik zu informieren, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist,		s.o.
191	2. die Öffentlichkeit oder betroffene Kreise gemäß § 7 zu warnen und zu informieren,		s.o.
192	3. Bundesbehörden gemäß § 4 Absatz 2 Nummer 2 über die sie betreffenden Informationen zu unterrichten,		s.o.
193	4. Betreiber Kritischer Infrastrukturen und Unternehmen im öffentlichen Interesse gemäß § 8b Absatz 2 Nummer 4 Buchstabe a über die sie betreffenden Informationen zu unterrichten.		s.o.
194	(4) Eine Weitergabe nach Absatz 3 Nummer 1, 2 oder 4 erfolgt nicht, soweit die gemäß Absatz 2 gemeldeten Informationen		s.o.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
195	1. Betriebs- und Geschäftsgeheimnisse von Dritten beinhalten und die Maßnahmen nach Absatz 3 nicht ohne Bekanntgabe dieser Betriebs- und Geschäftsgeheimnisse durchgeführt werden können oder		s.o.
196	2. auf Grund von Vereinbarungen des Bundesamtes mit Dritten nicht übermittelt werden dürfen.		s.o.
197	(5) Sonstige gesetzliche Meldepflichten, Regelungen zum Geheimschutz, gesetzliche Übermittlungshindernisse und Übermittlungsregelungen bleiben unberührt.		s.o.
198	§ 5 Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes	§ 8 Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes	Neue Enummerierung.
199	(1) Das Bundesamt darf zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes	(1) Das Bundesamt darf zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes	(unverändert)
200	1. Protokolldaten, die beim Betrieb von Kommunikationstechnik des Bundes anfallen, erheben und automatisiert auswerten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern bei der Kommunikationstechnik des Bundes oder von Angriffen auf die Informationstechnik des Bundes erforderlich ist,	1. Protokolldaten, die beim Betrieb von Kommunikationstechnik des Bundes anfallen, erheben und automatisiert auswerten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern bei der Kommunikationstechnik des Bundes oder von Angriffen auf die Informationstechnik des Bundes erforderlich ist,	(unverändert)
201	2. die an den Schnittstellen der Kommunikationstechnik des Bundes anfallenden Daten automatisiert auswerten, soweit dies für die Erkennung	2. die an den Schnittstellen der Kommunikationstechnik des Bundes anfallenden Daten automatisiert auswerten, soweit dies für die Erkennung	(unverändert)

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	und Abwehr von Schadprogrammen erforderlich ist.	und Abwehr von Schadprogrammen erforderlich ist.	
202	Sofern nicht die nachfolgenden Absätze eine weitere Verwendung gestatten, muss die automatisierte Auswertung dieser Daten unverzüglich erfolgen und müssen diese nach erfolgtem Abgleich sofort und spurenlos gelöscht werden. Die Verwendungsbeschränkungen gelten nicht für Protokolldaten, sofern diese weder personenbezogene noch dem Fernmeldegeheimnis unterliegende Daten beinhalten. Die Bundesbehörden sind verpflichtet, das Bundesamt bei Maßnahmen nach Satz 1 zu unterstützen und hierbei den Zugang des Bundesamtes zu behördeninternen Protokolldaten nach Satz 1 Nummer 1 sowie Schnittstellendaten nach Satz 1 Nummer 2 sicherzustellen. Protokolldaten der Bundesgerichte dürfen nur in deren Einvernehmen erhoben werden.	Sofern nicht die nachfolgenden Absätze eine weitere Verwendung gestatten, muss die automatisierte Auswertung dieser Daten unverzüglich erfolgen und müssen diese nach erfolgtem Abgleich sofort und spurenlos gelöscht werden. Die Verwendungsbeschränkungen gelten nicht für Protokolldaten, sofern diese weder personenbezogene noch dem Fernmeldegeheimnis unterliegende Daten beinhalten. Die Einrichtungen der Bundesverwaltung sind verpflichtet, das Bundesamt bei Maßnahmen nach Satz 1 zu unterstützen und hierbei den Zugang des Bundesamtes zu einrichtungsinternen Protokolldaten nach Satz 1 Nummer 1 sowie Schnittstellendaten nach Satz 1 Nummer 2 sicherzustellen. Protokolldaten der Bundesgerichte dürfen nur in deren Einvernehmen erhoben werden.	Begriffskonsolidierung: Einrichtungen der Bundesverwaltung. Die Erweiterung des Anwendungsbereichs erfolgt zum Zweck des Schutzes der gesamten Kommunikationstechnik des Bundes.
203	(2) Protokolldaten nach Absatz 1 Satz 1 Nummer 1 dürfen über den für die automatisierte Auswertung nach Absatz 1 Satz 1 Nummer 1 erforderlichen Zeitraum hinaus, längstens jedoch für 18 Monate, gespeichert werden, soweit tatsächliche Anhaltspunkte dafür bestehen, dass diese im Falle der Bestätigung eines Verdachts nach Absatz 3 Satz 2 zur Abwehr von Gefahren, die von dem gefundenen Schadprogramm ausgehen oder zur Erkennung und Abwehr anderer Schadprogramme erforderlich sein können. Durch organisatorische und technische Maßnahmen ist sicherzustellen, dass eine Auswertung der nach diesem Absatz gespeicherten Daten nur automatisiert erfolgt und dass ein Zugriff auf Daten, die länger als drei Monate gespeichert sind, nur bei Vorliegen tatsächlicher Erkenntnisse über die Betroffenheit des Bundes mit einem Schadprogramm erfolgt. Die Daten	(2) Protokolldaten nach Absatz 1 Satz 1 Nummer 1 dürfen über den für die automatisierte Auswertung nach Absatz 1 Satz 1 Nummer 1 erforderlichen Zeitraum hinaus, längstens jedoch für 18 Monate, gespeichert werden, soweit tatsächliche Anhaltspunkte dafür bestehen, dass diese im Falle der Bestätigung eines Verdachts nach Absatz 3 Satz 2 zur Abwehr von Gefahren, die von dem gefundenen Schadprogramm ausgehen oder zur Erkennung und Abwehr anderer Schadprogramme erforderlich sein können. Durch organisatorische und technische Maßnahmen ist sicherzustellen, dass eine Auswertung der nach diesem Absatz gespeicherten Daten nur automatisiert erfolgt und dass ein Zugriff auf Daten, die länger als drei Monate gespeichert sind, nur bei Vorliegen tatsächlicher Erkenntnisse über die Betroffenheit des Bundes mit einem Schadprogramm erfolgt. Die Daten	(unverändert)

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	sind zu pseudonymisieren, soweit dies automatisiert möglich ist. Eine nicht automatisierte Verarbeitung ist nur nach Maßgabe der nachfolgenden Absätze zulässig. Soweit hierzu die Wiederherstellung pseudonymisierter Protokolldaten erforderlich ist, muss diese durch die Präsidentin oder den Präsidenten des Bundesamtes oder die Vertretung im Amt angeordnet werden. Die Entscheidung ist zu dokumentieren.	sind zu pseudonymisieren, soweit dies automatisiert möglich ist. Eine nicht automatisierte Verarbeitung ist nur nach Maßgabe der nachfolgenden Absätze zulässig. Soweit hierzu die Wiederherstellung pseudonymisierter Protokolldaten erforderlich ist, muss diese durch die Präsidentin oder den Präsidenten des Bundesamtes oder die Vertretung im Amt angeordnet werden. Die Entscheidung ist zu dokumentieren.	
204	(2a) Protokolldaten dürfen vor ihrer Pseudonymisierung und Speicherung nach Absatz 2 zur Sicherstellung einer fehlerfreien automatisierten Auswertung manuell verarbeitet werden. Liegen Hinweise vor, dass die fehlerfreie automatisierte Auswertung wegen eines erheblichen Fehlers erschwert wird, darf der Personenbezug von Protokolldaten zur Sicherstellung der fehlerfreien automatisierten Auswertung wiederhergestellt werden, sofern dies im Einzelfall erforderlich ist. Absatz 2 Satz 3 bis 6 gilt entsprechend.	(2a) Protokolldaten dürfen vor ihrer Pseudonymisierung und Speicherung nach Absatz 2 zur Sicherstellung einer fehlerfreien automatisierten Auswertung manuell verarbeitet werden. Liegen Hinweise vor, dass die fehlerfreie automatisierte Auswertung wegen eines erheblichen Fehlers erschwert wird, darf der Personenbezug von Protokolldaten zur Sicherstellung der fehlerfreien automatisierten Auswertung wiederhergestellt werden, sofern dies im Einzelfall erforderlich ist. Absatz 2 Satz 3 bis 6 gilt entsprechend.	(unverändert)
205	(3) Eine über die Absätze 1 und 2 hinausgehende Verwendung personenbezogener Daten ist nur zulässig, wenn bestimmte Tatsachen den Verdacht begründen, dass	(3) Eine über die Absätze 1 und 2 hinausgehende Verwendung personenbezogener Daten ist nur zulässig, wenn bestimmte Tatsachen den Verdacht begründen, dass	(unverändert)
206	1. diese ein Schadprogramm enthalten,	1. diese ein Schadprogramm enthalten,	(unverändert)
207	2. diese durch ein Schadprogramm übermittelt wurden oder	2. diese durch ein Schadprogramm übermittelt wurden oder	(unverändert)
208	3. sich aus ihnen Hinweise auf ein Schadprogramm ergeben können,	3. sich aus ihnen Hinweise auf ein Schadprogramm ergeben können,	(unverändert)
209	und soweit die Datenverarbeitung erforderlich ist, um den Verdacht zu bestätigen oder zu widerlegen. Im Falle der Bestätigung ist die weitere Verarbeitung personenbezogener Daten zulässig, soweit dies	und soweit die Datenverarbeitung erforderlich ist, um den Verdacht zu bestätigen oder zu widerlegen. Im Falle der Bestätigung ist die weitere Verarbeitung personenbezogener Daten zulässig, soweit dies	(unverändert)

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
210	1. zur Abwehr des Schadprogramms,	1. zur Abwehr des Schadprogramms,	(unverändert)
211	2. zur Abwehr von Gefahren, die von dem aufgefundenen Schadprogramm ausgehen, oder	2. zur Abwehr von Gefahren, die von dem aufgefundenen Schadprogramm ausgehen, oder	(unverändert)
212	3. zur Erkennung und Abwehr anderer Schadprogramme erforderlich ist.	3. zur Erkennung und Abwehr anderer Schadprogramme erforderlich ist.	(unverändert)
213	Ein Schadprogramm kann beseitigt oder in seiner Funktionsweise gehindert werden. Die nicht automatisierte Verwendung der Daten nach den Sätzen 1 und 2 darf nur durch einen Bediensteten des Bundesamtes mit der Befähigung zum Richteramt angeordnet werden.	Ein Schadprogramm kann beseitigt oder in seiner Funktionsweise gehindert werden. Die nicht automatisierte Verwendung der Daten nach den Sätzen 1 und 2 darf nur durch einen Bediensteten des Bundesamtes mit der Befähigung zum Richteramt angeordnet werden.	(unverändert)
214	(4) Die Beteiligten des Kommunikationsvorgangs sind spätestens nach dem Erkennen und der Abwehr eines Schadprogramms oder von Gefahren, die von einem Schadprogramm ausgehen, zu benachrichtigen, wenn sie bekannt sind oder ihre Identifikation ohne unverhältnismäßige weitere Ermittlungen möglich ist und nicht überwiegende schutzwürdige Belange Dritter entgegenstehen. Die Unterrichtung kann unterbleiben, wenn die Person nur unerheblich betroffen wurde, und anzunehmen ist, dass sie an einer Benachrichtigung kein Interesse hat. Das Bundesamt legt Fälle, in denen es von einer Benachrichtigung absieht, dem behördlichen Datenschutzbeauftragten des Bundesamtes sowie einem weiteren Bediensteten des Bundesamtes, der die Befähigung zum Richteramt hat, zur Kontrolle vor. Wenn der behördliche Datenschutzbeauftragte der Entscheidung des Bundesamtes widerspricht, ist die Benachrichtigung nachzuholen. Die Entscheidung über die Nichtbenachrichtigung ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist nach zwölf Monaten zu löschen. In den Fällen der Absätze 5	(4) Die Beteiligten des Kommunikationsvorgangs sind spätestens nach dem Erkennen und der Abwehr eines Schadprogramms oder von Gefahren, die von einem Schadprogramm ausgehen, zu benachrichtigen, wenn sie bekannt sind oder ihre Identifikation ohne unverhältnismäßige weitere Ermittlungen möglich ist und nicht überwiegende schutzwürdige Belange Dritter entgegenstehen. Die Unterrichtung kann unterbleiben, wenn die Person nur unerheblich betroffen wurde, und anzunehmen ist, dass sie an einer Benachrichtigung kein Interesse hat. Das Bundesamt legt Fälle, in denen es von einer Benachrichtigung absieht, dem behördlichen Datenschutzbeauftragten des Bundesamtes sowie einem weiteren Bediensteten des Bundesamtes, der die Befähigung zum Richteramt hat, zur Kontrolle vor. Wenn der behördliche Datenschutzbeauftragte der Entscheidung des Bundesamtes widerspricht, ist die Benachrichtigung nachzuholen. Die Entscheidung über die Nichtbenachrichtigung ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist nach zwölf Monaten zu löschen. In den Fällen der Absätze 5	(unverändert)

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	und 6 erfolgt die Benachrichtigung durch die dort genannten Behörden in entsprechender Anwendung der für diese Behörden geltenden Vorschriften. Enthalten diese keine Bestimmungen zu Benachrichtigungspflichten, sind die Vorschriften der Strafprozessordnung entsprechend anzuwenden.	und 6 erfolgt die Benachrichtigung durch die dort genannten Behörden in entsprechender Anwendung der für diese Behörden geltenden Vorschriften. Enthalten diese keine Bestimmungen zu Benachrichtigungspflichten, sind die Vorschriften der Strafprozessordnung entsprechend anzuwenden.	
215	(5) Das Bundesamt kann die nach Absatz 3 verwendeten personenbezogenen Daten an die Strafverfolgungsbehörden zur Verfolgung einer mittels eines Schadprogramms begangenen Straftat nach den §§ 202a, 202b, 303a oder 303b des Strafgesetzbuches übermitteln. Es kann diese Daten ferner übermitteln	(5) Das Bundesamt kann die nach Absatz 3 verwendeten personenbezogenen Daten an die Strafverfolgungsbehörden zur Verfolgung einer mittels eines Schadprogramms begangenen Straftat nach den §§ 202a, 202b, 303a oder 303b des Strafgesetzbuches übermitteln. Es kann diese Daten ferner übermitteln	(unverändert)
216	1. zur Abwehr einer Gefahr für die öffentliche Sicherheit, die unmittelbar von einem Schadprogramm ausgeht, an die Polizeien des Bundes und der Länder,	1. zur Abwehr einer Gefahr für die öffentliche Sicherheit, die unmittelbar von einem Schadprogramm ausgeht, an die Polizeien des Bundes und der Länder,	(unverändert)
217	2. zur Unterrichtung über Tatsachen, die sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht erkennen lassen, an das Bundesamt für Verfassungsschutz sowie an den Militärischen Abschirmdienst, wenn sich diese Tätigkeiten gegen Personen, Dienststellen oder Einrichtungen im Geschäftsbereich des Bundesministeriums der Verteidigung richten,	2. zur Unterrichtung über Tatsachen, die sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht erkennen lassen, an das Bundesamt für Verfassungsschutz sowie an den Militärischen Abschirmdienst, wenn sich diese Tätigkeiten gegen Personen, Dienststellen oder Einrichtungen im Geschäftsbereich des Bundesministeriums der Verteidigung richten,	(unverändert)
218	3. zur Unterrichtung über Tatsachen, die einen internationalen kriminellen, terroristischen oder staatlichen Angriff mittels Schadprogrammen oder vergleichbaren schädlich wirkenden informationstechnischen Mitteln auf die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Systemen in Fällen	3. zur Unterrichtung über Tatsachen, die einen internationalen kriminellen, terroristischen oder staatlichen Angriff mittels Schadprogrammen oder vergleichbaren schädlich wirkenden informationstechnischen Mitteln auf die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Systemen in Fällen	(unverändert)

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	von erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland erkennen lassen, an den Bundesnachrichtendienst.	von erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland erkennen lassen, an den Bundesnachrichtendienst.	
219	(6) Für sonstige Zwecke kann das Bundesamt die Daten übermitteln	(6) Für sonstige Zwecke kann das Bundesamt die Daten übermitteln	(unverändert)
220	1. an die Strafverfolgungsbehörden zur Verfolgung einer Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere einer in § 100a Absatz 2 der Strafprozessordnung bezeichneten Straftat,	1. an die Strafverfolgungsbehörden zur Verfolgung einer Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere einer in § 100a Absatz 2 der Strafprozessordnung bezeichneten Straftat,	(unverändert)
221	2. an die Polizeien des Bundes und der Länder zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Staates oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse geboten ist,	2. an die Polizeien des Bundes und der Länder zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Staates oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse geboten ist,	(unverändert)
222	3. an die Verfassungsschutzbehörden des Bundes und der Länder sowie an den Militärischen Abschirmdienst, wenn tatsächliche Anhaltspunkte für Bestrebungen in der Bundesrepublik Deutschland vorliegen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen gegen die in § 3 Absatz 1 des Bundesverfassungsschutzgesetzes beziehungsweise § 1 Absatz 1 des MAD-Gesetzes genannten Schutzgüter gerichtet sind,	3. an die Verfassungsschutzbehörden des Bundes und der Länder sowie an den Militärischen Abschirmdienst, wenn tatsächliche Anhaltspunkte für Bestrebungen in der Bundesrepublik Deutschland vorliegen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen gegen die in § 3 Absatz 1 des Bundesverfassungsschutzgesetzes beziehungsweise § 1 Absatz 1 des MAD-Gesetzes genannten Schutzgüter gerichtet sind,	(unverändert)
223	4. an den Bundesnachrichtendienst, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand	4. an den Bundesnachrichtendienst, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand	(unverändert)

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Straftaten nach § 3 Absatz 1 Nummer 8 des Artikel 10-Gesetzes plant, begeht oder begangen hat und dies von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland ist.	Straftaten nach § 3 Absatz 1 Nummer 8 des Artikel 10-Gesetzes plant, begeht oder begangen hat und dies von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland ist.	
224	Die Übermittlung nach Satz 1 Nummer 1 und 2 bedarf der vorherigen gerichtlichen Zustimmung. Für das Verfahren nach Satz 1 Nummer 1 und 2 gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Zuständig ist das Amtsgericht, in dessen Bezirk das Bundesamt seinen Sitz hat. Die Übermittlung nach Satz 1 Nummer 3 und Nummer 4 erfolgt nach Zustimmung des Bundesministeriums des Innern, für Bau und Heimat; die §§ 9 bis 16 des Artikel 10-Gesetzes gelten entsprechend.	Die Übermittlung nach Satz 1 Nummer 1 und 2 bedarf der vorherigen gerichtlichen Zustimmung. Für das Verfahren nach Satz 1 Nummer 1 und 2 gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Zuständig ist das Amtsgericht, in dessen Bezirk das Bundesamt seinen Sitz hat. Die Übermittlung nach Satz 1 Nummer 3 und Nummer 4 erfolgt nach Zustimmung des Bundesministeriums des Innern und für Heimat; die §§ 9 bis 16 des Artikel 10-Gesetzes gelten entsprechend.	Redaktionelle Änderungen.
225	(7) Eine über die vorstehenden Absätze hinausgehende inhaltliche Auswertung zu anderen Zwecken und die Weitergabe von personenbezogenen Daten an Dritte sind unzulässig. Soweit möglich, ist technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Werden aufgrund der Maßnahmen der Absätze 1 bis 3 Erkenntnisse aus dem Kernbereich privater Lebensgestaltung oder Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 erlangt, dürfen diese nicht verwendet werden. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung sind unverzüglich zu löschen. Dies gilt auch in Zweifelsfällen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des	(7) Eine über die vorstehenden Absätze hinausgehende inhaltliche Auswertung zu anderen Zwecken und die Weitergabe von personenbezogenen Daten an Dritte sind unzulässig. Soweit möglich, ist technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Werden aufgrund der Maßnahmen der Absätze 1 bis 3 Erkenntnisse aus dem Kernbereich privater Lebensgestaltung oder Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 erlangt, dürfen diese nicht verwendet werden. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung sind unverzüglich zu löschen. Dies gilt auch in Zweifelsfällen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des	(unverändert)

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Kalenderjahres, das dem Jahr der Dokumentation folgt. Werden im Rahmen der Absätze 4 oder 5 Inhalte oder Umstände der Kommunikation von in § 53 Absatz 1 Satz 1 der Strafprozessordnung genannten Personen übermittelt, auf die sich das Zeugnisverweigerungsrecht der genannten Personen erstreckt, ist die Verwertung dieser Daten zu Beweiszwecken in einem Strafverfahren nur insoweit zulässig, als Gegenstand dieses Strafverfahrens eine Straftat ist, die im Höchstmaß mit mindestens fünf Jahren Freiheitsstrafe bedroht ist.	Kalenderjahres, das dem Jahr der Dokumentation folgt. Werden im Rahmen der Absätze 4 oder 5 Inhalte oder Umstände der Kommunikation von in § 53 Absatz 1 Satz 1 der Strafprozessordnung genannten Personen übermittelt, auf die sich das Zeugnisverweigerungsrecht der genannten Personen erstreckt, ist die Verwertung dieser Daten zu Beweiszwecken in einem Strafverfahren nur insoweit zulässig, als Gegenstand dieses Strafverfahrens eine Straftat ist, die im Höchstmaß mit mindestens fünf Jahren Freiheitsstrafe bedroht ist.	
226	(8) Vor Aufnahme der Datenerhebung und -verwendung hat das Bundesamt ein Datenerhebungs- und -verwendungskonzept zu erstellen und für Kontrollen durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit bereitzuhalten. Das Konzept hat dem besonderen Schutzbedürfnis der Regierungskommunikation Rechnung zu tragen. Die für die automatisierte Auswertung verwendeten Kriterien sind zu dokumentieren. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit teilt das Ergebnis seiner Kontrollen nach § 16 des Bundesdatenschutzgesetzes auch dem Rat der IT-Beauftragten der Bundesregierung mit.	(8) Vor Aufnahme der Datenerhebung und -verwendung hat das Bundesamt ein Datenerhebungs- und -verwendungskonzept zu erstellen und für Kontrollen durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit bereitzuhalten. Das Konzept hat dem besonderen Schutzbedürfnis der Regierungskommunikation Rechnung zu tragen. Die für die automatisierte Auswertung verwendeten Kriterien sind zu dokumentieren. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit teilt das Ergebnis seiner Kontrollen nach § 16 des Bundesdatenschutzgesetzes auch den Ressorts mit.	Redaktionelle Änderung, um Gremienstruktur untergesetzlich regeln zu können.
227	(9) Das Bundesamt unterrichtet den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres über	(9) Das Bundesamt unterrichtet den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres über	(unverändert)
228	1. die Anzahl der Vorgänge, in denen Daten nach Absatz 5 Satz 1, Absatz 5 Satz 2 Nummer 1 oder Absatz 6 Nummer 1 übermittelt wurden, aufgegliedert nach den einzelnen Übermittlungsbefugnissen,	1. die Anzahl der Vorgänge, in denen Daten nach Absatz 5 Satz 1, Absatz 5 Satz 2 Nummer 1 oder Absatz 6 Nummer 1 übermittelt wurden, aufgegliedert nach den einzelnen Übermittlungsbefugnissen,	(unverändert)

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
229	2. die Anzahl der personenbezogenen Auswertungen nach Absatz 3 Satz 1, in denen der Verdacht widerlegt wurde,	2. die Anzahl der personenbezogenen Auswertungen nach Absatz 3 Satz 1, in denen der Verdacht widerlegt wurde,	(unverändert)
230	3. die Anzahl der Fälle, in denen das Bundesamt nach Absatz 4 Satz 2 oder 3 von einer Benachrichtigung der Betroffenen abgesehen hat.	3. die Anzahl der Fälle, in denen das Bundesamt nach Absatz 4 Satz 2 oder 3 von einer Benachrichtigung der Betroffenen abgesehen hat.	(unverändert)
231	(10) Das Bundesamt unterrichtet kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres den Innenausschuss des Deutschen Bundestages über die Anwendung dieser Vorschrift.	(10) Das Bundesamt unterrichtet kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres den Innenausschuss des Deutschen Bundestages über die Anwendung dieser Vorschrift.	(unverändert)
232	§ 5a Verarbeitung behördeninterner Protokollierungsdaten	§ 9 Verarbeitung von Protokollierungsdaten der Kommunikationstechnik des Bundes	Neue Enummerierung Geänderte Bezeichnung spiegelt Begriffskonsolidierung und inhaltlichen Bezug zu § 5 a.F./§ 9 n.F. wider.
233	Das Bundesamt darf zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes und ihrer Komponenten, einschließlich technischer Infrastrukturen, die zum Betrieb der Kommunikationstechnik des Bundes erforderlich sind, Protokollierungsdaten, die durch den Betrieb von Kommunikationstechnik des Bundes anfallen, verarbeiten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen, Fehlern oder Sicherheitsvorfällen in der Kommunikationstechnik des Bundes oder von Angriffen auf die Informationstechnik des Bundes erforderlich ist und Geheimschutzinteressen oder überwiegende Sicherheitsinteressen der betroffenen Stellen nicht entgegenstehen. Die Bundesbehörden sind verpflichtet, das Bundesamt bei Maßnahmen nach Satz 1 zu unterstützen und hierbei den Zugang des Bundesamtes zu behördeninternen Protokollierungsdaten nach Satz 1 sicherzustellen. Hierzu dürfen sie dem Bundesamt die entsprechenden	Das Bundesamt darf zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes und ihrer Komponenten, einschließlich technischer Infrastrukturen, die zum Betrieb der Kommunikationstechnik des Bundes erforderlich sind, Protokollierungsdaten, die durch den Betrieb von Kommunikationstechnik des Bundes anfallen, verarbeiten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen, Fehlern oder Sicherheitsvorfällen in der Kommunikationstechnik des Bundes oder von Angriffen auf die Informationstechnik des Bundes erforderlich ist und Geheimschutzinteressen oder überwiegende Sicherheitsinteressen der betroffenen Stellen nicht entgegenstehen. Die Einrichtungen der Bundesverwaltung sind verpflichtet, das Bundesamt bei Maßnahmen nach Satz 1 zu unterstützen und hierbei den Zugang des Bundesamtes zu einrichtungsinternen Protokollierungsdaten nach Satz 1 sicherzustellen. Hierzu dürfen sie dem Bundesamt die entsprechenden	Begriffskonsolidierung: Einrichtungen der Bundesverwaltung. Die Erweiterung des Anwendungsbereichs erfolgt zum Zweck des Schutzes der gesamten Kommunikationstechnik des Bundes.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Protokollierungsdaten übermitteln. § 5 Absatz 1 Satz 5, Absatz 2 bis 4, 8 und 9 gilt entsprechend. § 4a Absatz 6 gilt für die Verpflichtung nach Satz 2 entsprechend.	Protokollierungsdaten übermitteln. § 8 Absatz 1 Satz 5, Absatz 2 bis 4, 8 und 9 gilt entsprechend. § 7 Absatz 6 gilt für die Verpflichtung nach Satz 2 entsprechend.	
234		§ 10 Anordnungen von Maßnahmen zur Abwendung oder Behebung von Sicherheitsvorfällen	
235		Das Bundesamt kann gegenüber Einrichtungen der Bundesverwaltung Maßnahmen anweisen, die zur Abwendung oder Behebung eines Sicherheitsvorfalls erforderlich sind. Ferner kann das Bundesamt die Einrichtungen zur Berichterstattung innerhalb einer angemessenen Frist zu den nach Satz 1 angeordneten Maßnahmen auffordern. Der Bericht ist dem Bundesamt sowie zugleich an den Informationssicherheitsbeauftragten des jeweils zuständigen Ressorts sowie den Koordinator oder die Koordinatorin für Informationssicherheit zu übermitteln.	Umsetzung Art. 32 Abs. 4 lit. b und d NIS-2 gegenüber Einrichtungen der Bundesverwaltung. Die Berichterstattung erfolgt neben BSI als gesetzliche Aufsichtsbehörde für die Informationssicherheit an die jeweiligen Ressort-ISBs wegen der dort liegenden Zuständigkeit und an CISO Bund wegen Lagebild.
236	§ 5b Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen	§ 11 Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen	Neue Enummerierung.
237	(1) Handelt es sich bei einer Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines informationstechnischen Systems einer Stelle des Bundes oder eines Betreibers einer Kritischen Infrastruktur oder eines Unternehmens im besonderen öffentlichen Interesse um einen herausgehobenen Fall, so kann das Bundesamt auf Ersuchen der betroffenen Stelle oder des betroffenen Betreibers die Maßnahmen treffen, die zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich sind. Soweit das Bundesamt erste Maßnahmen zur Schadensbegrenzung und Sicherstellung des	(1) Handelt es sich bei einer Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines informationstechnischen Systems einer Einrichtung der Bundesverwaltung oder Betreibers kritischer Anlagen oder einer besonders wichtigen Einrichtung oder einer wichtigen Einrichtung um einen herausgehobenen Fall, so kann das Bundesamt auf Ersuchen der betroffenen Stelle oder der betroffenen Einrichtung oder einer anderen für die Einrichtung zuständigen Behörde die Maßnahmen treffen, die zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich sind. Soweit das Bundesamt erste Maßnahmen zur	Folgeänderungen aufgrund neuer Einrichtungskategorien; Anpassung in Umsetzung von Art. 11 Abs. 1 lit. d. NIS-2. Begriffskonsolidierung: Einrichtung der Bundesverwaltung

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Notbetriebes vor Ort ergreift, werden hierfür keine Gebühren oder Auslagen für die Tätigkeit des Bundesamtes erhoben. Hiervon unberührt bleiben etwaige Kosten für die Hinzuziehung qualifizierter Dritter.	Schadensbegrenzung und Sicherstellung des Notbetriebes vor Ort ergreift, werden hierfür keine Gebühren oder Auslagen für die Tätigkeit des Bundesamtes erhoben. Hiervon unberührt bleiben etwaige Kosten für die Hinzuziehung qualifizierter Dritter.	
238	(2) Ein herausgehobener Fall nach Absatz 1 liegt insbesondere dann vor, wenn es sich um einen Angriff von besonderer technischer Qualität handelt oder die zügige Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems von besonderem öffentlichem Interesse ist.	(2) Ein herausgehobener Fall nach Absatz 1 liegt insbesondere dann vor, wenn es sich um einen Angriff von besonderer technischer Qualität handelt oder die zügige Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems von besonderem öffentlichem Interesse ist.	(unverändert)
239	(3) Das Bundesamt darf bei Maßnahmen nach Absatz 1 personenbezogene oder dem Fernmeldegeheimnis unterliegende Daten erheben und verarbeiten, soweit dies zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich und angemessen ist. Die Daten sind unverzüglich zu löschen, sobald sie für die Wiederherstellung der Sicherheit oder Funktionsfähigkeit des informationstechnischen Systems nicht mehr benötigt werden. Wenn die Daten in Fällen des Absatzes 4 an eine andere Behörde zur Erfüllung von deren gesetzlichen Aufgaben weitergegeben worden sind, darf das Bundesamt die Daten abweichend von Satz 2 bis zur Beendigung der Unterstützung dieser Behörden weiterverarbeiten. Eine Nutzung zu anderen Zwecken ist unzulässig. § 5 Absatz 7 ist entsprechend anzuwenden.	(3) Das Bundesamt darf bei Maßnahmen nach Absatz 1 personenbezogene oder dem Fernmeldegeheimnis unterliegende Daten erheben und verarbeiten, soweit dies zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich und angemessen ist. Die Daten sind unverzüglich zu löschen, sobald sie für die Wiederherstellung der Sicherheit oder Funktionsfähigkeit des informationstechnischen Systems nicht mehr benötigt werden. Wenn die Daten in Fällen des Absatzes 4 an eine andere Behörde zur Erfüllung von deren gesetzlichen Aufgaben weitergegeben worden sind, darf das Bundesamt die Daten abweichend von Satz 2 bis zur Beendigung der Unterstützung dieser Behörden weiterverarbeiten. Eine Nutzung zu anderen Zwecken ist unzulässig. § 8 Absatz 7 ist entsprechend anzuwenden.	(unverändert)
240	(4) Das Bundesamt darf Informationen, von denen es im Rahmen dieser Vorschrift Kenntnis erlangt, nur mit Einwilligung des Ersuchenden weitergeben, es sei denn, die Informationen lassen keine Rückschlüsse auf die Identität des Ersuchenden zu oder die	(4) Das Bundesamt darf Informationen, von denen es im Rahmen dieser Vorschrift Kenntnis erlangt, nur mit Einwilligung des Ersuchenden weitergeben, es sei denn, die Informationen lassen keine Rückschlüsse auf die Identität des Ersuchenden zu oder die	(unverändert)

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Informationen können entsprechend § 5 Absatz 5 und 6 übermittelt werden. Zugang zu den in Verfahren nach Absatz 1 geführten Akten wird Dritten nicht gewährt.	Informationen können entsprechend § 8 Absatz 5 und 6 übermittelt werden. Zugang zu den in Verfahren nach Absatz 1 geführten Akten wird Dritten nicht gewährt.	
241	(5) Das Bundesamt kann sich bei Maßnahmen nach Absatz 1 mit der Einwilligung des Ersuchenden der Hilfe qualifizierter Dritter bedienen, wenn dies zur rechtzeitigen oder vollständigen Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich ist. Die hierdurch entstehenden Kosten hat der Ersuchende zu tragen. Das Bundesamt kann den Ersuchenden auch auf qualifizierte Dritte verweisen. Das Bundesamt und vom Ersuchenden oder vom Bundesamt nach Satz 1 beauftragte Dritte können einander bei Maßnahmen nach Absatz 1 mit der Einwilligung des Ersuchenden Daten übermitteln. Hierfür gilt Absatz 3 entsprechend.	(5) Das Bundesamt kann sich bei Maßnahmen nach Absatz 1 mit der Einwilligung des Ersuchenden der Hilfe qualifizierter Dritter bedienen, wenn dies zur rechtzeitigen oder vollständigen Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich ist. Die hierdurch entstehenden Kosten hat der Ersuchende zu tragen. Das Bundesamt kann den Ersuchenden auch auf qualifizierte Dritte verweisen. Das Bundesamt und vom Ersuchenden oder vom Bundesamt nach Satz 1 beauftragte Dritte können einander bei Maßnahmen nach Absatz 1 mit der Einwilligung des Ersuchenden Daten übermitteln. Hierfür gilt Absatz 3 entsprechend.	(unverändert)
242	(6) Soweit es zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des informationstechnischen Systems erforderlich ist, kann das Bundesamt vom Hersteller des informationstechnischen Systems verlangen, an der Wiederherstellung der Sicherheit oder Funktionsfähigkeit mitzuwirken.	(6) Soweit es zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des informationstechnischen Systems erforderlich ist, kann das Bundesamt vom Hersteller des informationstechnischen Systems verlangen, an der Wiederherstellung der Sicherheit oder Funktionsfähigkeit mitzuwirken.	(unverändert)
243	(7) In begründeten Einzelfällen kann das Bundesamt auch bei anderen als den in Absatz 1 genannten Einrichtungen tätig werden, wenn es darum ersucht wurde und es sich um einen herausgehobenen Fall im Sinne des Absatzes 2 handelt. Ein begründeter Einzelfall liegt in der Regel vor, wenn eine Stelle eines Landes betroffen ist.	(7) In begründeten Einzelfällen kann das Bundesamt auch bei anderen als den in Absatz 1 genannten Einrichtungen tätig werden, wenn es darum ersucht wurde und es sich um einen herausgehobenen Fall im Sinne des Absatzes 2 handelt. Ein begründeter Einzelfall liegt in der Regel vor, wenn eine Stelle eines Landes betroffen ist.	(unverändert)
244	(8) Im Falle von Anlagen oder Tätigkeiten, die einer Genehmigung nach dem Atomgesetz bedürfen, ist in Fällen der Absätze 1, 4, 5 und 7 vor Tätigwerden des Bundesamtes das Benehmen mit den zuständigen atomrechtlichen Aufsichtsbehörden des Bundes und der Länder herzustellen. Im Falle von Anlagen oder	(8) Im Falle von Anlagen oder Tätigkeiten, die einer Genehmigung nach dem Atomgesetz bedürfen, ist in Fällen der Absätze 1, 4, 5 und 7 vor Tätigwerden des Bundesamtes das Benehmen mit den zuständigen atomrechtlichen Aufsichtsbehörden des Bundes und der Länder herzustellen. Im Falle von Anlagen oder	(unverändert)

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Tätigkeiten, die einer Genehmigung nach dem Atomgesetz bedürfen, haben bei Maßnahmen des Bundesamtes nach § 5b die Vorgaben aufgrund des Atomgesetzes Vorrang.	Tätigkeiten, die einer Genehmigung nach dem Atomgesetz bedürfen, haben bei Maßnahmen des Bundesamtes nach § 11 die Vorgaben aufgrund des Atomgesetzes Vorrang.	
245	§ 5c Bestandsdatenauskunft	§ 12 Bestandsdatenauskunft	Neue Enummerierung
246	(1) Das Bundesamt darf zur Erfüllung seiner gesetzlichen Aufgabe nach § 3 Absatz 1 Satz 1 Nummer 1, 2, 14, 17 oder 18 von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, über Bestandsdaten gemäß § 3 Nummer 6 des Telekommunikationsgesetzes und über die nach § 172 des Telekommunikationsgesetzes erhobenen Daten (§ 174 Absatz 1 Satz 1 des Telekommunikationsgesetzes) Auskunft verlangen. Die Auskunft nach Satz 1 darf nur verlangt werden zum Schutz der Versorgung der Bevölkerung in den Bereichen des § 2 Absatz 10 Satz 1 Nummer 1 oder der öffentlichen Sicherheit, um damit eine Beeinträchtigung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme	(1) Das Bundesamt darf zur Erfüllung seiner gesetzlichen Aufgabe nach § 3 Absatz 1 Satz 1 Nummer 1, 2, 14, 17 oder 18 von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, über Bestandsdaten gemäß § 3 Nummer 6 des Telekommunikationsgesetzes und über die nach § 172 des Telekommunikationsgesetzes erhobenen Daten (§ 174 Absatz 1 Satz 1 des Telekommunikationsgesetzes) Auskunft verlangen. Die Auskunft nach Satz 1 darf nur verlangt werden zum Schutz der Versorgung der Bevölkerung in den Bereichen des § 57 Absatz 1 oder der öffentlichen Sicherheit, um damit eine Beeinträchtigung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme	(unverändert)
247	1. einer Kritischen Infrastruktur oder	1. einer kritischen Anlage oder	Anpassung an neue Bezeichnung
248	2. eines Unternehmens von besonderem öffentlichem Interesse	2. einer besonders wichtigen Einrichtung oder wichtigen Einrichtung	Anpassung an neue Einrichtungskategorien
249	abzuwenden, wenn Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, das auf die informationstechnischen Systeme bestimmbarer Infrastrukturen oder Unternehmen abzielen wird, und die in die Auskunft aufzunehmenden Daten im Einzelfall erforderlich sind, um die Betroffenen nach Absatz 4 vor dieser Beeinträchtigung zu warnen, über	abzuwenden, wenn Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, das auf die informationstechnischen Systeme bestimmbarer Infrastrukturen oder Unternehmen abzielen wird, und die in die Auskunft aufzunehmenden Daten im Einzelfall erforderlich sind, um die Betroffenen nach Absatz 4 vor dieser Beeinträchtigung zu warnen, über	(unverändert)

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	diese zu informieren oder sie bei deren Beseitigung zu beraten oder zu unterstützen.	diese zu informieren oder sie bei deren Beseitigung zu beraten oder zu unterstützen.	
250	(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 174 Absatz 1 Satz 3, § 177 Absatz 1 Nummer 3 des Telekommunikationsgesetzes). Die rechtlichen und tatsächlichen Grundlagen des Auskunftsverlangens sind aktenkundig zu machen.	(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 174 Absatz 1 Satz 3, § 177 Absatz 1 Nummer 3 des Telekommunikationsgesetzes). Die rechtlichen und tatsächlichen Grundlagen des Auskunftsverlangens sind aktenkundig zu machen.	
251	(3) Der auf Grund eines Auskunftsverlangens Verpflichtete hat die zur Auskunftserteilung erforderlichen Daten unverzüglich und vollständig zu übermitteln.	(3) Der auf Grund eines Auskunftsverlangens Verpflichtete hat die zur Auskunftserteilung erforderlichen Daten unverzüglich und vollständig zu übermitteln.	
252	(4) Nach erfolgter Auskunft weist das Bundesamt den Betreiber der betroffenen Kritischen Infrastruktur oder das betroffene Unternehmen im besonderen öffentlichen Interesse auf die bei ihm drohenden Beeinträchtigungen hin. Nach Möglichkeit weist das Bundesamt den Betreiber der betroffenen Kritischen Infrastruktur oder das betroffene Unternehmen im besonderen öffentlichen Interesse auf technische Mittel hin, mittels derer die festgestellten Beeinträchtigungen durch den Betreiber der betroffenen Kritischen Infrastruktur oder das betroffene Unternehmen im besonderen öffentlichen Interesse selbst beseitigt werden können.	(4) Nach erfolgter Auskunft weist das Bundesamt Betreiber der kritischen Anlage oder die besonders wichtige Einrichtung oder die wichtige Einrichtung auf die bei ihm drohenden Beeinträchtigungen hin. Nach Möglichkeit weist das Bundesamt den Betreiber der kritischen Anlage oder die besonders wichtige Einrichtung oder die wichtige Einrichtung auf technische Mittel hin, mittels derer die festgestellten Beeinträchtigungen durch den Betreiber kritischer Anlagen oder die besonders wichtige Einrichtung oder die wichtige Einrichtung selbst beseitigt werden können.	Folgeänderung aufgrund neuer Kategorien
253	(5) Das Bundesamt kann personenbezogene Daten, die es im Rahmen dieser Vorschrift verarbeitet, entsprechend § 5 Absatz 5 und 6 übermitteln.	(5) Das Bundesamt kann personenbezogene Daten, die es im Rahmen dieser Vorschrift verarbeitet, entsprechend § 8 Absatz 5 und 6 übermitteln.	(unverändert)
254	(6) In den Fällen des Absatzes 2 ist die betroffene Person über die Auskunft zu benachrichtigen. Im Falle der Weitergabe der Information nach § 5 Absatz 5 oder wenn Tatsachen die Annahme rechtfertigen, dass die Voraussetzungen einer Weitergabe nach § 5 Absatz 5	(6) In den Fällen des Absatzes 2 ist die betroffene Person über die Auskunft zu benachrichtigen. Im Falle der Weitergabe der Information nach § 8 Absatz 5 oder wenn Tatsachen die Annahme rechtfertigen, dass die Voraussetzungen einer Weitergabe nach § 8 Absatz 5	(unverändert)

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	vorliegen, ergeht darüber keine Benachrichtigung an die betroffene Person, sofern und solange überwiegende schutzwürdige Belange Dritter entgegenstehen. Wird nach Satz 2 die Benachrichtigung zurückgestellt oder wird von ihr abgesehen, sind die Gründe aktenkundig zu machen.	vorliegen, ergeht darüber keine Benachrichtigung an die betroffene Person, sofern und solange überwiegende schutzwürdige Belange Dritter entgegenstehen. Wird nach Satz 2 die Benachrichtigung zurückgestellt oder wird von ihr abgesehen, sind die Gründe aktenkundig zu machen.	
255	(7) Das Bundesamt unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres über	(7) Das Bundesamt unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres über	(unverändert)
256	1. die Gesamtzahl der Vorgänge, in denen Daten nach Absatz 1 oder Absatz 2 an das Bundesamt übermittelt wurden und	1. die Gesamtzahl der Vorgänge, in denen Daten nach Absatz 1 oder Absatz 2 an das Bundesamt übermittelt wurden und	(unverändert)
257	2. die Übermittlungen nach Absatz 5.	2. die Übermittlungen nach Absatz 5.	(unverändert)
258	(8) Das Bundesamt hat den Verpflichteten für ihm erteilte Auskünfte eine Entschädigung zu gewähren. Der Umfang der Entschädigung bemisst sich nach § 23 und Anlage 3 des Justizvergütungs- und -entschädigungsgesetzes; die Vorschriften über die Verjährung in § 2 Absatz 1 und 4 des Justizvergütungs- und -entschädigungsgesetzes finden entsprechende Anwendung.	(8) Das Bundesamt hat den Verpflichteten für ihm erteilte Auskünfte eine Entschädigung zu gewähren. Der Umfang der Entschädigung bemisst sich nach § 23 und Anlage 3 des Justizvergütungs- und -entschädigungsgesetzes; die Vorschriften über die Verjährung in § 2 Absatz 1 und 4 des Justizvergütungs- und -entschädigungsgesetzes finden entsprechende Anwendung.	(unverändert)
259	§ 6 Beschränkungen der Rechte der betroffenen Person		Verschoben nach § 21 nF.
260	Für die Rechte der betroffenen Person gegen das Bundesamt gelten ergänzend zu den in der Verordnung (EU) 2016/679 enthaltenen Ausnahmen die nachfolgenden Beschränkungen. Soweit dieses Gesetz keine oder geringere Beschränkungen der Rechte der betroffenen Person enthält, gelten für die		s.o.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Beschränkungen im Übrigen die Regelungen des Bundesdatenschutzgesetzes ergänzend.		
261	§ 6a Informationspflicht bei Erhebung von personenbezogenen Daten		Verschoben nach § 22 nF.
262	(1) Die Pflicht zur Information gemäß den Artikeln 13 und 14 der Verordnung (EU) 2016/679 besteht ergänzend zu den in Artikel 13 Absatz 4 und Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht, wenn		s.o.
263	1. die Informationserteilung die ordnungsgemäße Erfüllung der in der Zuständigkeit des Bundesamtes liegenden Aufgaben gefährden würde oder		s.o.
264	2. die Informationserteilung die öffentliche Sicherheit oder Ordnung oder die Gewährleistung der Netz- und Informationssicherheit auf sonstige Weise gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde		s.o.
265	und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss.		s.o.
266	(2) Unterbleibt eine Information der betroffenen Person nach Maßgabe des Absatzes 1, ergreift das Bundesamt geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung der in Artikel 13 Absatz 1 und 2 und Artikel 14 Absatz 1 und 2 der Verordnung (EU) 2016/679 genannten Informationen für die		s.o.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Öffentlichkeit in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache. Das Bundesamt hält schriftlich fest, aus welchen Gründen es von einer Information der betroffenen Person abgesehen hat.		
267	§ 6b Auskunftsrecht der betroffenen Person		Verschoben nach § 23 nF.
268	(1) Das Recht auf Auskunft gemäß Artikel 15 Absatz 1 und 2 der Verordnung (EU) 2016/679 besteht nicht, wenn und soweit		s.o.
269	1. die Auskunftserteilung die ordnungsgemäße Erfüllung der Aufgaben gefährden würde, die in der Zuständigkeit des Bundesamtes liegen,		s.o.
270	2. die Auskunftserteilung		s.o.
271	a) die öffentliche Sicherheit oder Ordnung oder die Gewährleistung der Netz- und Informationssicherheit gefährden würde oder		s.o.
272	b) sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde oder		s.o.
273	3. die Auskunftserteilung strafrechtliche Ermittlungen oder die Verfolgung von Straftaten gefährden würde		s.o.
274	und deswegen das Interesse der betroffenen Person an der Auskunftserteilung zurücktreten muss.		s.o.
275	(2) § 34 Absatz 2 bis 4 des Bundesdatenschutzgesetzes gilt entsprechend.		s.o.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
276	§ 6c Recht auf Berichtigung		Verschoben nach § 24 nF.
277	(1) Das Recht der betroffenen Person auf Berichtigung und Vervollständigung gemäß Artikel 16 der Verordnung (EU) 2016/679 besteht nicht, wenn und soweit die Erfüllung der Rechte der betroffenen Person die ordnungsgemäße Erfüllung der in der Zuständigkeit des Bundesamtes liegenden Aufgaben gefährden würde und deswegen das Interesse der betroffenen Person an der Ausübung dieser Rechte zurücktreten muss.		s.o.
278	(2) In den Fällen des Absatzes 1 hat die betroffene Person einen Anspruch darauf, den Daten für die Dauer der Verarbeitung eine Gegendarstellung beizufügen, sofern dies für eine faire und transparente Verarbeitung erforderlich ist.		s.o.
279	§ 6d Recht auf Löschung		Verschoben nach § 25 nF.
280	(1) Im Fall der nicht automatisierten Verarbeitung besteht die Pflicht des Bundesamtes zur Löschung personenbezogener Daten gemäß Artikel 17 Absatz 1 und 2 der Verordnung (EU) 2016/679 ergänzend zu den in Artikel 17 Absatz 3 genannten Ausnahmen nicht, wenn		s.o.
281	1. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist und		s.o.
282	2. das Interesse der betroffenen Person an der Löschung als gering anzusehen ist.		s.o.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
283	In diesem Fall tritt an die Stelle der Löschung eine Einschränkung der Verarbeitung gemäß Artikel 18 der Verordnung (EU) 2016/679. Die Sätze 1 und 2 sind nicht anzuwenden, wenn die personenbezogenen Daten unrechtmäßig verarbeitet wurden.		s.o.
284	(2) Ist die Löschung lediglich für eine etwaige gerichtliche Überprüfung von Maßnahmen nach § 5 Absatz 3 zurückgestellt, dürfen die Daten ohne Einwilligung der betroffenen Person nur zu diesem Zweck verwendet werden; sie sind für andere Zwecke in der Verarbeitung einzuschränken. § 5 Absatz 7 bleibt unberührt.		s.o.
285	§ 6e Recht auf Einschränkung der Verarbeitung		Verschoben nach § 26 nF.
286	Die Pflicht des Bundesamtes zur Einschränkung der Verarbeitung gemäß Artikel 18 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679 besteht für die Dauer der Überprüfung der Richtigkeit der personenbezogenen Daten nicht, wenn		s.o.
287	1. die Verarbeitung oder Weiterverarbeitung durch dieses Gesetz ausdrücklich geregelt ist oder		s.o.
288	2. die Einschränkung der Verarbeitung die Abwehr von Gefahren für die Sicherheit in der Informationstechnik gefährden würde		s.o.
289	und deswegen das Interesse der betroffenen Person an der Einschränkung zurücktreten muss.		s.o.
290	§ 6f Widerspruchsrecht		Verschoben nach § 27 nF.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
291	Das Recht der betroffenen Person auf Widerspruch gemäß Artikel 21 Absatz 1 der Verordnung (EU) 2016/679 besteht nicht, wenn		s.o.
292	1. an der Verarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der betroffenen Person überwiegt, oder		s.o.
293	2. eine Rechtsvorschrift das Bundesamt zur Verarbeitung verpflichtet.		s.o.
294	Darüber hinaus darf das Bundesamt die personenbezogenen Daten ergänzend zu Artikel 21 Absatz 1 Satz 2 der Verordnung (EU) 2016/679 so lange verarbeiten, bis das Bundesamt geprüft hat, ob zwingende schutzwürdige Gründe für die Verarbeitung bestehen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen.		s.o.
295	§ 7 Warnungen	§ 13 Warnungen	Neue Enummerierung
296	(1) Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 14 und 14a kann das Bundesamt	(1) Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 14 und 14a kann das Bundesamt	(unverändert)
297	1. die folgenden Warnungen und Informationen an die Öffentlichkeit oder an die betroffenen Kreise richten:	1. die folgenden Warnungen und Informationen an die Öffentlichkeit oder an die betroffenen Kreise richten:	(unverändert)
298	a) Warnungen vor Sicherheitslücken in informationstechnischen Produkten und Diensten,	a) Warnungen vor Schwachstellen und anderen Sicherheitsrisiken in informationstechnischen Produkten und Diensten,	Redaktionelle Anpassung von Sicherheitslücke auf Schwachstelle.
299	b) Warnungen vor Schadprogrammen,	b) Warnungen vor Schadprogrammen,	(unverändert)

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
300	c) Warnungen bei einem Verlust oder einem unerlaubten Zugriff auf Daten und	c) Warnungen bei einem Verlust oder einem unerlaubten Zugriff auf Daten und	(unverändert)
301	d) Informationen über sicherheitsrelevante IT-Eigenschaften von Produkten.	d) Informationen über sicherheitsrelevante IT-Eigenschaften von Produkten.	(unverändert)
302		e) Informationen über Verstöße besonders wichtiger Einrichtungen oder wichtiger Einrichtungen gegen die Pflichten aus diesem Gesetz und [*einfügen*: *andere Gesetze, die die NIS-2-Richtlinie umsetzen*].	Umsetzung Art. 32 Abs. 4 lit. a und Art. 33 Abs. 4 NIS-2 [*Anm. BMI CI 1 – Die Ausgestaltung der Umsetzung der NIS-2-Richtlinie in den Fachgesetzen (wie zB. TKG) wird Gegenstand der Ressortabstimmung sein.*]
303	2. Sicherheitsmaßnahmen sowie den Einsatz bestimmter Sicherheitsprodukte empfehlen.	2. Sicherheitsmaßnahmen sowie den Einsatz bestimmter Sicherheitsprodukte empfehlen.	(unverändert)
304	Das Bundesamt kann zur Wahrnehmung der Aufgaben nach Satz 1 Dritte einbeziehen, wenn dies für eine wirksame und rechtzeitige Warnung erforderlich ist.	Das Bundesamt kann zur Wahrnehmung der Aufgaben nach Satz 1 Dritte einbeziehen, wenn dies für eine wirksame und rechtzeitige Warnung erforderlich ist.	(unverändert)
305	(1a) Die Hersteller betroffener Produkte sind rechtzeitig vor Veröffentlichung der Warnungen zu informieren. Diese Informationspflicht besteht nicht,	(1a) Die Hersteller betroffener Produkte sind rechtzeitig vor Veröffentlichung der Warnungen zu informieren. Diese Informationspflicht besteht nicht,	(unverändert)
306	1. wenn hierdurch die Erreichung des mit der Maßnahme verfolgten Zwecks gefährdet wird oder	1. wenn hierdurch die Erreichung des mit der Maßnahme verfolgten Zwecks gefährdet wird oder	(unverändert)
307	2. wenn berechtigterweise davon ausgegangen werden kann, dass der Hersteller an einer vorherigen Benachrichtigung kein Interesse hat.	2. wenn berechtigterweise davon ausgegangen werden kann, dass der Hersteller an einer vorherigen Benachrichtigung kein Interesse hat.	(unverändert)

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
308	Soweit entdeckte Sicherheitslücken oder Schadprogramme nicht allgemein bekannt werden sollen, um eine Weiterverbreitung oder rechtswidrige Ausnutzung zu verhindern oder weil das Bundesamt gegenüber Dritten zur Vertraulichkeit verpflichtet ist, kann es den Kreis der zu warnenden Personen einschränken. Kriterien für die Auswahl des zu warnenden Personenkreises nach Satz 3 sind insbesondere die besondere Gefährdung bestimmter Einrichtungen oder die besondere Zuverlässigkeit des Empfängers.	Soweit entdeckte Schwachstellen oder Schadprogramme nicht allgemein bekannt werden sollen, um eine Weiterverbreitung oder rechtswidrige Ausnutzung zu verhindern oder weil das Bundesamt gegenüber Dritten zur Vertraulichkeit verpflichtet ist, kann es den Kreis der zu warnenden Personen einschränken. Kriterien für die Auswahl des zu warnenden Personenkreises nach Satz 3 sind insbesondere die besondere Gefährdung bestimmter Einrichtungen oder die besondere Zuverlässigkeit des Empfängers.	(unverändert)redaktionelle Anpassung, da nur noch Schwachstelle definiert wird
309	(2) Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 14 und 14a kann das Bundesamt die Öffentlichkeit unter Nennung der Bezeichnung und des Herstellers des betroffenen Produkts und Dienstes vor Sicherheitslücken in informationstechnischen Produkten und Diensten und vor Schadprogrammen warnen, wenn hinreichende Anhaltspunkte dafür vorliegen, dass Gefahren für die Sicherheit in der Informationstechnik hiervon ausgehen, oder Sicherheitsmaßnahmen sowie den Einsatz bestimmter informationstechnischer Produkte und Dienste empfehlen. Stellen sich die an die Öffentlichkeit gegebenen Informationen im Nachhinein als falsch oder die zugrunde liegenden Umstände als unzutreffend wiedergegeben heraus, ist dies unverzüglich öffentlich bekannt zu machen.	(2) Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 14 und 14a kann das Bundesamt die Öffentlichkeit unter Nennung der Bezeichnung und des Herstellers des betroffenen Produkts und Dienstes vor Schwachstellen in informationstechnischen Produkten und Diensten und vor Schadprogrammen warnen, wenn hinreichende Anhaltspunkte dafür vorliegen, dass Gefahren für die Sicherheit in der Informationstechnik hiervon ausgehen, oder Sicherheitsmaßnahmen sowie den Einsatz bestimmter informationstechnischer Produkte und Dienste empfehlen. Stellen sich die an die Öffentlichkeit gegebenen Informationen im Nachhinein als falsch oder die zugrunde liegenden Umstände als unzutreffend wiedergegeben heraus, ist dies unverzüglich öffentlich bekannt zu machen. Warnungen nach Satz 1 sind sechs Monate nach der Veröffentlichung zu entfernen, wenn nicht weiterhin hinreichende Anhaltspunkte dafür vorliegen, dass Gefahren für die Sicherheit in der Informationstechnik bestehen. Wird eine Warnung nach Satz 3 nicht entfernt, so ist diese Entscheidung regelmäßig zu überprüfen.	§ 7 Abs. 2 BSIG aF. muss um eine Regelung zur Archivierung von Warnungen ergänzt werden. Hintergrund ist der Beschluss des BVerfG vom 21. März 2018 (– 1 BvF 1/13 –) zu § 40 LFGB. Eine gesetzliche Regelung zur zeitlichen Begrenzung der Informationsverbreitung fehlte im LFGB. Dies ist mit dem Grundsatz der Verhältnismäßigkeit nicht vereinbar, da mit Zeitablauf nach der Veröffentlichung der Grundrechtseingriff zulasten des Herstellers einerseits und der mit Warnung verfolgte Zweck andererseits außer Verhältnis geraten.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
310	§ 7a Untersuchung der Sicherheit in der Informationstechnik	§ 14 Untersuchung der Sicherheit in der Informationstechnik	Neue Enummerierung
311	(1) Das Bundesamt kann zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 14, 14a, 17 oder 18 auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene informationstechnische Produkte und Systeme untersuchen. Es kann sich hierbei der Unterstützung Dritter bedienen, soweit berechtigte Interessen des Herstellers der betroffenen Produkte und Systeme dem nicht entgegenstehen.	(1) Das Bundesamt kann zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 14, 14a, 17 oder 18 auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene informationstechnische Produkte und Systeme untersuchen. Es kann sich hierbei der Unterstützung Dritter bedienen, soweit berechtigte Interessen des Herstellers der betroffenen Produkte und Systeme dem nicht entgegenstehen.	(unverändert)
312	(2) Soweit erforderlich, kann das Bundesamt für Untersuchungen nach Absatz 1 von Herstellern informationstechnischer Produkte und Systeme alle notwendigen Auskünfte, insbesondere auch zu technischen Details, verlangen. In dem Auskunftsverlangen gibt das Bundesamt die Rechtsgrundlage, den Zweck des Auskunftsverlangens und die benötigten Auskünfte an und legt eine angemessene Frist für die Übermittlung der Auskünfte fest. Das Auskunftsverlangen enthält ferner einen Hinweis auf die in § 14 vorgesehenen Sanktionen.	(2) Soweit erforderlich, kann das Bundesamt für Untersuchungen nach Absatz 1 von Herstellern informationstechnischer Produkte und Systeme alle notwendigen Auskünfte, insbesondere auch zu technischen Details, verlangen. In dem Auskunftsverlangen gibt das Bundesamt die Rechtsgrundlage, den Zweck des Auskunftsverlangens und die benötigten Auskünfte an und legt eine angemessene Frist für die Übermittlung der Auskünfte fest. Das Auskunftsverlangen enthält ferner einen Hinweis auf die in § 60 vorgesehenen Sanktionen.	(unverändert)
313	(3) Das Bundesamt gibt Auskünfte sowie die aus den Untersuchungen gewonnen Erkenntnisse unverzüglich an die zuständigen Aufsichtsbehörden des Bundes oder, sofern keine Aufsichtsbehörde vorhanden ist, an das jeweilige Ressort weiter, wenn Anhaltspunkte bestehen, dass diese sie zur Erfüllung ihrer Aufgaben benötigen.	(3) Das Bundesamt gibt Auskünfte sowie die aus den Untersuchungen gewonnen Erkenntnisse unverzüglich an die zuständigen Aufsichtsbehörden des Bundes oder, sofern keine Aufsichtsbehörde vorhanden ist, an das jeweilige Ressort weiter, wenn Anhaltspunkte bestehen, dass diese sie zur Erfüllung ihrer Aufgaben benötigen.	(unverändert)
314	(4) Die Auskünfte und die aus den Untersuchungen gewonnenen Erkenntnisse dürfen nur zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 14, 14a, 17 und 18 genutzt werden. Das Bundesamt darf seine	(4) Die Auskünfte und die aus den Untersuchungen gewonnenen Erkenntnisse dürfen nur zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 14, 14a, 17 und 18 genutzt werden. Das Bundesamt darf seine	Die Ergänzung ist erforderlich, um einen Austausch zu Dritten (wie bspw. auch zu anderen Aufsichtsbehörden) zu ermöglichen und zu vereinfachen, wenn

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Erkenntnisse weitergeben und veröffentlichen, soweit dies zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 14, 14a, 17 und 18 erforderlich ist. Zuvor ist dem Hersteller der betroffenen Produkte und Systeme mit angemessener Frist Gelegenheit zur Stellungnahme zu geben.	Erkenntnisse weitergeben und veröffentlichen, soweit dies zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 14, 14a, 17 und 18 erforderlich ist. Zuvor ist dem Hersteller der betroffenen Produkte und Systeme mit angemessener Frist Gelegenheit zur Stellungnahme zu geben. Von einer Gelegenheit zur Stellungnahme kann abgesehen werden, wenn die Erkenntnisse ohne erkennbaren Bezug zum Hersteller oder der untersuchten informationstechnischen Produkte und Systeme weitergegeben oder veröffentlicht werden.	es bspw. nur um Kategorien von Produkttypen und gefundenen Schwachstellen geht, die auch ohne konkreten Hersteller-/Produktbezug weitergegeben werden sollen. Da in diesem Fall die Eingriffsintensität gegenüber den Herstellern der untersuchten Produkte und Systeme mangels Bezugnahme als sehr gering anzusehen ist, würde eine vorab einzuholende Stellungnahme die Weitergabe kritischer Schwachstellen an Dritte (wie bspw. andere Aufsichtsbehörden) unnötig erschweren.
315	(5) Kommt ein Hersteller der Aufforderung des Bundesamtes nach Absatz 2 Satz 1 nicht oder nur unzureichend nach, kann das Bundesamt hierüber die Öffentlichkeit informieren. Es kann hierbei den Namen des Herstellers sowie die Bezeichnung des betroffenen Produkts oder Systems angeben und darlegen, inwieweit der Hersteller seiner Auskunftspflicht nicht nachgekommen ist. Zuvor ist dem Hersteller mit 1angemessener Frist Gelegenheit zur Stellungnahme zu gewähren. § 7 Absatz 2 Satz 2 gilt entsprechend.	(5) Kommt ein Hersteller der Aufforderung des Bundesamtes nach Absatz 2 Satz 1 nicht oder nur unzureichend nach, kann das Bundesamt hierüber die Öffentlichkeit informieren. Es kann hierbei den Namen des Herstellers sowie die Bezeichnung des betroffenen Produkts oder Systems angeben und darlegen, inwieweit der Hersteller seiner Auskunftspflicht nicht nachgekommen ist. Zuvor ist dem Hersteller mit angemessener Frist Gelegenheit zur Stellungnahme zu gewähren. § 7 Absatz 2 Satz 2 gilt entsprechend.	(unverändert)
316	§ 7b Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden	§ 15 Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden	Neue Enummerierung
317	(1) Das Bundesamt kann im Rahmen seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 2, 14 oder 17 zur Detektion von Sicherheitslücken und anderen Sicherheitsrisiken bei Einrichtungen des Bundes oder der in § 2 Absatz 10, 11 und 14 genannten Unternehmen Maßnahmen an den Schnittstellen öffentlich erreichbarer informationstechnischer	(1) Das Bundesamt kann im Rahmen seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 2, 14 oder 17 zur Detektion von Schwachstellen und anderen Sicherheitsrisiken bei Einrichtungen der Bundesverwaltung oder Betreibern kritischer Anlagen, besonders wichtigen Einrichtungen oder wichtigen Einrichtungen Maßnahmen an den Schnittstellen	Art. 11 Abs. 3 lit. e, Art. 32 Abs. 2 lit. d und Art. 33 Abs. 2 lit. c NIS-2 sehen die Durchführung von Schwachstellenscans bei wichtigen und wesentlichen Einrichtungen als zwingende Aufgabe der CSIRTs und Aufsichtsmaßnahme an.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Systeme zu öffentlichen Telekommunikationsnetzen (Portscans) durchführen, wenn Tatsachen die Annahme rechtfertigen, dass diese ungeschützt im Sinne des Absatzes 2 sein können und dadurch in ihrer Sicherheit oder Funktionsfähigkeit gefährdet sein können. Die Maßnahmen müssen sich auf einen vorher bestimmten Bereich von Internet-Protokolladressen, die regelmäßig den informationstechnischen Systemen	öffentlich erreichbarer informationstechnischer Systeme zu öffentlichen Telekommunikationsnetzen durchführen, um festzustellen, ob diese ungeschützt und dadurch in ihrer Sicherheit oder Funktionsfähigkeit gefährdet sein können oder wenn die entsprechenden Einrichtungen darum ersuchen.	Einschränkungen auf bestimmte Arten von Scans oder einen Anlass als Voraussetzungen für diese Schwachstellenscans sehen die Regelungen der NIS-2 nicht vor, so dass der bisher in § 7b Abs. 1 enthaltene Verweis auf bloße Portscans ebenso zu streichen war, wie die Annahme eines ungeschützten Systems als Voraussetzung. Dabei war eine Einschränkung auf bloße Portscans auch deswegen nicht angezeigt, da die Detektion von Sicherheitslücken ist nicht nur über Portscans, sondern auch über weitere webseiten-/ domainbasierte Methoden möglich ist. Da sich die Art von Sicherheitsscans durch den technischen Fortschritt verändern kann, war eine ebenso entwicklungsoffene Formulierung zu wählen, wie sie die NIS-2 enthält. Zudem ist die Regelung an die neuen Einrichtungskategorien aus der NIS-2 anzupassen. Statt des Begriffes der Sicherheitslücke wird zur europaweiten Vereinheitlichung der Terminologie der der Schwachstelle im Sinne von Art. 6 Nr. 15 NIS-2 verwendet, ohne dass damit eine inhaltliche Änderung verbunden ist.
318	1. des Bundes oder		s.o.
319	2. Kritischer Infrastrukturen, digitaler Dienste und der Unternehmen im besonderen öffentlichen Interesse		s.o.
320	zugeordnet sind (Weiße Liste), beschränken. Die Weiße Liste ist stetig durch geeignete Überprüfungen	Erlangt das Bundesamt dabei Informationen, die durch Artikel 10 des Grundgesetzes geschützt sind,	s.o.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	anzupassen, um Änderungen bei der Zuordnung von Internetprotokoll-Adressen zu den in den Nummern 1 und 2 bezeichneten Stellen zu berücksichtigen. Erlangt das Bundesamt dabei Informationen, die durch Artikel 10 des Grundgesetzes geschützt sind, darf es diese nur zum Zwecke der Übermittlung nach § 5 Absatz 5 und 6 verarbeiten. Sofern die Voraussetzungen des § 5 Absatz 5 und 6 nicht vorliegen, sind Informationen, die nach Artikel 10 des Grundgesetzes geschützt sind, unverzüglich zu löschen. Maßnahmen nach Satz 1 dürfen nur durch eine Bedienstete oder einen Bediensteten des Bundesamtes mit der Befähigung zum Richteramt angeordnet werden.	darf es diese nur zum Zwecke der Übermittlung nach § 8 Absatz 5 und 6 verarbeiten. Sofern die Voraussetzungen des § 8 Absatz 5 und 6 nicht vorliegen, sind Informationen, die nach Artikel 10 des Grundgesetzes geschützt sind, unverzüglich zu löschen.	
321	(2) Ein informationstechnisches System ist ungeschützt im Sinne des Absatzes 1, wenn in diesem öffentlich bekannte Sicherheitslücken bestehen oder wenn auf Grund sonstiger offensichtlich unzureichender Sicherheitsvorkehrungen unbefugt von Dritten auf das System zugegriffen werden kann.	.	Streichung, da eine entsprechende einschränkende Definition z.B. auf öffentlich bekannte Schwachstellen von der NIS-2-Richtlinie nicht vorgesehen ist.
322	(3) Wird durch Maßnahmen gemäß Absatz 1 eine Sicherheitslücke oder ein anderes Sicherheitsrisiko eines informationstechnischen Systems erkannt, sind die für das informationstechnische System Verantwortlichen unverzüglich darüber zu informieren. Das Bundesamt soll dabei auf bestehende Abhilfemöglichkeiten hinweisen. Sind dem Bundesamt die Verantwortlichen nicht bekannt oder ist ihre Identifikation nur mit unverhältnismäßigem Aufwand oder über eine Bestandsdatenabfrage nach § 5c möglich, ist hilfsweise der betreibende Dienstleister des jeweiligen Netzes oder Systems unverzüglich zu benachrichtigen, wenn überwiegende Sicherheitsinteressen nicht entgegenstehen. Das Bundesamt unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit jeweils bis zum 30. Juni des	(2) Wird durch Maßnahmen gemäß Absatz 1 eine Schwachstelle oder ein anderes Sicherheitsrisiko eines informationstechnischen Systems erkannt, sind die für das informationstechnische System Verantwortlichen unverzüglich darüber zu informieren. Das Bundesamt soll dabei auf bestehende Abhilfemöglichkeiten hinweisen. Sind dem Bundesamt die Verantwortlichen nicht bekannt oder ist ihre Identifikation nur mit unverhältnismäßigem Aufwand oder über eine Bestandsdatenabfrage nach § 12 möglich, ist hilfsweise der betreibende Dienstleister des jeweiligen Netzes oder Systems unverzüglich zu benachrichtigen, wenn überwiegende Sicherheitsinteressen nicht entgegenstehen. Das Bundesamt unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit jeweils bis zum 30. Juni des Folgejahres über die Anzahl der	Redaktionelle Änderung von „Sicherheitslücke“ auf „Schwachstelle“

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Folgejahres über die Anzahl der gemäß Absatz 1 ergriffenen Maßnahmen. Das Bundesamt legt die Weiße Liste nach Absatz 1 Satz 3 der Bundesbeauftragten oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vierteljährlich zur Kontrolle vor.	gemäß Absatz 1 ergriffenen Maßnahmen. Das Bundesamt legt die Weiße Liste nach Absatz 1 Satz 3 der Bundesbeauftragten oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vierteljährlich zur Kontrolle vor.	
323	(4) Das Bundesamt darf zur Erfüllung seiner Aufgaben Systeme und Verfahren einsetzen, welche einem Angreifer einen erfolgreichen Angriff vortäuschen, um den Einsatz von Schadprogrammen oder andere Angriffsmethoden zu erheben und auszuwerten. Das Bundesamt darf dabei die zur Auswertung der Funktionsweise der Schadprogramme und Angriffsmethoden erforderlichen Daten verarbeiten.	(3) Das Bundesamt darf zur Erfüllung seiner Aufgaben Systeme und Verfahren einsetzen, welche einem Angreifer einen erfolgreichen Angriff vortäuschen, um den Einsatz von Schadprogrammen oder andere Angriffsmethoden zu erheben und auszuwerten. Das Bundesamt darf dabei die zur Auswertung der Funktionsweise der Schadprogramme und Angriffsmethoden erforderlichen Daten verarbeiten.	(unverändert)
324	§ 7c Anordnungen des Bundesamtes gegenüber Diensteanbietern	§ 16 Anordnungen des Bundesamtes gegenüber Diensteanbietern	Neue Enummerierung
325	(1) Zur Abwehr konkreter erheblicher Gefahren für die in Absatz 2 genannten Schutzziele kann das Bundesamt gegenüber einem Anbieter von Telekommunikationsdiensten im Sinne des Telekommunikationsgesetzes (Diensteanbieter) mit mehr als 100 000 Kunden anordnen, dass er	(1) Zur Abwehr konkreter erheblicher Gefahren für die in Absatz 2 genannten Schutzziele kann das Bundesamt gegenüber einem Anbieter von Telekommunikationsdiensten im Sinne des Telekommunikationsgesetzes (Diensteanbieter) mit mehr als 100 000 Kunden anordnen, dass er	(unverändert)
326	1. die in § 169 Absatz 6 und 7 des Telekommunikationsgesetzes bezeichneten Maßnahmen trifft oder	1. die in § 169 Absatz 6 und 7 des Telekommunikationsgesetzes bezeichneten Maßnahmen trifft oder	(unverändert)
327	2. technische Befehle zur Bereinigung von einem konkret benannten Schadprogramm an betroffene informationstechnische Systeme verteilt,	2. technische Befehle zur Bereinigung von einem konkret benannten Schadprogramm an betroffene informationstechnische Systeme verteilt,	(unverändert)

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
328	sofern und soweit der Diensteanbieter dazu technisch in der Lage ist und es ihm wirtschaftlich zumutbar ist. Vor der Anordnung der Maßnahmen nach Satz 1 Nummer 1 oder 2 durch das Bundesamt ist Einvernehmen mit der Bundesnetzagentur herzustellen. Vor der Anordnung der Maßnahme nach Satz 1 Nummer 2 durch das Bundesamt ist zusätzlich Einvernehmen mit der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit herzustellen. Die Daten, auf die mit der Maßnahme nach Satz 1 Nummer 2 zugegriffen werden soll, sind in der Anordnung zu benennen. § 5 Absatz 7 Satz 2 bis 8 gilt entsprechend. Widerspruch und Anfechtungsklage gegen die Anordnungen nach Satz 1 haben keine aufschiebende Wirkung.	sofern und soweit der Diensteanbieter dazu technisch in der Lage ist und es ihm wirtschaftlich zumutbar ist. Vor der Anordnung der Maßnahmen nach Satz 1 Nummer 1 oder 2 durch das Bundesamt ist Einvernehmen mit der Bundesnetzagentur herzustellen. Vor der Anordnung der Maßnahme nach Satz 1 Nummer 2 durch das Bundesamt ist zusätzlich Einvernehmen mit der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit herzustellen. Die Daten, auf die mit der Maßnahme nach Satz 1 Nummer 2 zugegriffen werden soll, sind in der Anordnung zu benennen. § 8 Absatz 7 Satz 2 bis 8 gilt entsprechend. Widerspruch und Anfechtungsklage gegen die Anordnungen nach Satz 1 haben keine aufschiebende Wirkung.	(unverändert)
329	(2) Schutzziele gemäß Absatz 1 Satz 1 sind die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit	(2) Schutzziele gemäß Absatz 1 Satz 1 sind die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit	(unverändert)
330	1. der Kommunikationstechnik des Bundes, eines Betreibers Kritischer Infrastrukturen, eines Unternehmens im besonderen öffentlichen Interesse oder eines Anbieters digitaler Dienste,	1. der Kommunikationstechnik des Bundes, eines Betreibers kritischer Anlagen, einer besonders wichtigen Einrichtung oder einer wichtigen Einrichtung,	Folgeänderung aufgrund neuer Einrichtungskategorien
331	2. von Informations- oder Kommunikationsdiensten oder	2. von Informations- oder Kommunikationsdiensten oder	(unverändert)
332	3. von Informationen, sofern deren Verfügbarkeit, Unversehrtheit oder Vertraulichkeit durch unerlaubte Zugriffe auf eine erhebliche Anzahl von telekommunikations- oder informationstechnischen Systemen von Nutzern eingeschränkt wird.	3. von Informationen, sofern deren Verfügbarkeit, Unversehrtheit oder Vertraulichkeit durch unerlaubte Zugriffe auf eine erhebliche Anzahl von telekommunikations- oder informationstechnischen Systemen von Nutzern eingeschränkt wird.	(unverändert)
333	(3) Ordnet das Bundesamt eine Maßnahme nach Absatz 1 Satz 1 Nummer 1 an, so kann es gegenüber dem Diensteanbieter auch anordnen, den	(3) Ordnet das Bundesamt eine Maßnahme nach Absatz 1 Satz 1 Nummer 1 an, so kann es gegenüber dem Diensteanbieter auch anordnen, den	(unverändert)

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Datenverkehr an eine vom Bundesamt benannte Anschlusskennung umzuleiten.	Datenverkehr an eine vom Bundesamt benannte Anschlusskennung umzuleiten.	
334	(4) Das Bundesamt darf Daten, die von einem Diensteanbieter nach Absatz 1 Satz 1 Nummer 1 und Absatz 3 umgeleitet wurden, verarbeiten, um Informationen über Schadprogramme oder andere Sicherheitsrisiken in informationstechnischen Systemen zu erlangen. Die übermittelten Daten dürfen durch das Bundesamt so lange gespeichert werden, wie dies für die Erfüllung des in Satz 1 genannten Zwecks erforderlich ist, längstens jedoch für drei Monate. § 5 Absatz 7 Satz 2 bis 8 gilt entsprechend. Das Bundesamt unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit jeweils bis zum 30. Juni des Folgejahres über die Gesamtzahl der angeordneten Datenumleitungen.	(4) Das Bundesamt darf Daten, die von einem Diensteanbieter nach Absatz 1 Satz 1 Nummer 1 und Absatz 3 umgeleitet wurden, verarbeiten, um Informationen über Schadprogramme oder andere Sicherheitsrisiken in informationstechnischen Systemen zu erlangen. Die übermittelten Daten dürfen durch das Bundesamt so lange gespeichert werden, wie dies für die Erfüllung des in Satz 1 genannten Zwecks erforderlich ist, längstens jedoch für drei Monate. § 8 Absatz 7 Satz 2 bis 8 gilt entsprechend. Das Bundesamt unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit jeweils bis zum 30. Juni des Folgejahres über die Gesamtzahl der angeordneten Datenumleitungen.	(unverändert)
335	§ 7d Anordnungen des Bundesamtes gegenüber Anbietern von Telemediendiensten	§ 17 Anordnungen des Bundesamtes gegenüber Anbietern von Telemediendiensten	Neue Enummerierung
336	Das Bundesamt kann in begründeten Einzelfällen zur Abwehr konkreter, erheblicher Gefahren für informationstechnische Systeme einer Vielzahl von Nutzern, die von Telemedienangeboten von Anbietern von Telemedien im Sinne des § 2 Absatz 2 Nummer 1 des Telekommunikation-Telemedien-Datenschutz-Gesetzes ausgehen, die durch ungenügende technische und organisatorische Vorkehrungen im Sinne des § 19 Absatz 4 des Telekommunikation-Telemedien-Datenschutz-Gesetzes unzureichend gesichert sind und dadurch keinen hinreichenden Schutz bieten vor	Das Bundesamt kann in begründeten Einzelfällen zur Abwehr konkreter, erheblicher Gefahren für informationstechnische Systeme einer Vielzahl von Nutzern, die von Telemedienangeboten von Anbietern von Telemedien im Sinne des § 2 Absatz 2 Nummer 1 des Telekommunikation-Telemedien-Datenschutz-Gesetzes ausgehen, die durch ungenügende technische und organisatorische Vorkehrungen im Sinne des § 19 Absatz 4 des Telekommunikation-Telemedien-Datenschutz-Gesetzes unzureichend gesichert sind und dadurch keinen hinreichenden Schutz bieten vor	(unverändert)

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
337	1. unerlaubten Zugriffen auf die für diese Telemedienangebote genutzten technischen Einrichtungen oder	1. unerlaubten Zugriffen auf die für diese Telemedienangebote genutzten technischen Einrichtungen oder	(unverändert)
338	2. Störungen, auch soweit sie durch äußere Angriffe bedingt sind,	2. Störungen, auch soweit sie durch äußere Angriffe bedingt sind,	(unverändert)
339	gegenüber dem jeweiligen Anbieter von Telemedien im Sinne des § 2 Absatz 2 Nummer 1 des Telekommunikation-Telemedien-Datenschutz-Gesetzes anordnen, dass dieser die jeweils zur Herstellung des ordnungsgemäßen Zustands seiner Telemedienangebote erforderlichen technischen und organisatorischen Maßnahmen ergreift, um den ordnungsgemäßen Zustand seiner Telemedienangebote herzustellen. Die Zuständigkeit der Aufsichtsbehörden der Länder bleibt im Übrigen unberührt.	gegenüber dem jeweiligen Anbieter von Telemedien im Sinne des § 2 Absatz 2 Nummer 1 des Telekommunikation-Telemedien-Datenschutz-Gesetzes anordnen, dass dieser die jeweils zur Herstellung des ordnungsgemäßen Zustands seiner Telemedienangebote erforderlichen technischen und organisatorischen Maßnahmen ergreift, um den ordnungsgemäßen Zustand seiner Telemedienangebote herzustellen. Die Zuständigkeit der Aufsichtsbehörden der Länder bleibt im Übrigen unberührt.	(unverändert)
340		§ 18 Anordnungen des Bundesamtes gegenüber Herstellern von IKT-Produkten	
341	*(6) Soweit erforderlich kann das Bundesamt vom Hersteller der betroffenen informationstechnischen Produkte und Systeme die Mitwirkung an der Beseitigung oder Vermeidung einer Störung nach Absatz 4, oder § 8f Absatz 7 oder 8 verlangen. Satz 1 gilt für Störungen bei Betreibern und Genehmigungsinhabern im Sinne von § 8d Absatz 3 entsprechend.*	Soweit erforderlich kann das Bundesamt von einem Hersteller betroffener IKT-Produkte die Mitwirkung an der Beseitigung oder Vermeidung von erheblichen Sicherheitsvorfällen bei Betreibern kritischer Anlagen, besonders wichtigen Einrichtungen und wichtigen Einrichtungen verlangen.	Verschoben von § 8b Abs. 6 aF; Anpassung an die neuen Kategorien.
342	§ 8 Vorgaben des Bundesamtes	§ 19 Bereitstellung von IT-Sicherheitsprodukten	§ 8 aF größtenteils verschoben zu Teil 3 Kapitel 3 - hier verbleibt Abs. 3 S. 1-3, da RGL zur Bereitstellung von IT-Sicherheitsprodukten (ohne Nutzungszwang, der dann in S. 4-6 enthalten war und nun, weil er die

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			Einrichtungen des Bundes verpflichtet, verschoben ist)
343	(1) Das Bundesamt legt im Benehmen mit den Ressorts Mindeststandards für die Sicherheit der Informationstechnik des Bundes fest, die von		Verschoben nach § 42 nF.,
344	1. Stellen des Bundes,		Entfällt, da es im Anwendungsbereich von Teil 3 unter „Einrichtungen der Bundesverwaltung“ aufgeht
345	2. Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie ihren Vereinigungen ungeachtet ihrer Rechtsform auf Bundesebene, soweit von der jeweils zuständigen obersten Bundesbehörde angeordnet, sowie		Entfällt, da es im Anwendungsbereich von Teil 3 unter „Einrichtungen der Bundesverwaltung“ aufgeht
346	3. öffentlichen Unternehmen, die mehrheitlich im Eigentum des Bundes stehen und die IT-Dienstleistungen für die Bundesverwaltung erbringen,		Entfällt, da es im Anwendungsbereich von Teil 3 unter „Einrichtungen der Bundesverwaltung aufgeht
347	umzusetzen sind. Abweichungen von den Mindeststandards sind nur in sachlich gerechtfertigten Fällen zulässig und sind zu dokumentieren und zu begründen. Das Bundesamt berät die in Satz 1 genannten Stellen auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards. Für die in § 2 Absatz 3 Satz 2 genannten Gerichte und Verfassungsorgane haben die Vorschriften nach Satz 1 empfehlenden Charakter. Für die Verpflichtung nach Satz 1 gilt die Ausnahme nach § 4a Absatz 6 entsprechend.		Verschoben nach § 42 nF. (dort geänderte Fassung)
348	(1a) Das Bundesministerium des Innern, für Bau und Heimat kann im Benehmen mit der Konferenz der IT-Beauftragten der Ressorts bei bedeutenden Mindeststandards die Überwachung und Kontrolle ihrer		Regelungsgehalte verschoben nach Teil 3 Kapitel 3 nF.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Einhaltung durch das Bundesamt anordnen. Das Bundesamt teilt das Ergebnis seiner Kontrolle der jeweiligen überprüften Stelle, deren zuständiger Aufsichtsbehörde sowie der Konferenz der IT-Beauftragten der Ressorts mit. Für andere öffentlich-rechtlich oder privatrechtlich organisierte Stellen dürfen nur dann Schnittstellen zur Kommunikationstechnik des Bundes eingerichtet werden, soweit die für die Einrichtung verantwortliche Stelle vertraglich sicherstellt, dass die öffentlich- oder privatrechtlich organisierte Stelle sich zur Einhaltung der Mindeststandards verpflichtet. Das Bundesamt kann im Einvernehmen mit dem Dritten die Einhaltung der Mindeststandards überprüfen und kontrollieren.		
349	(2) Das Bundesamt stellt im Rahmen seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 10 technische Richtlinien bereit, die von den Stellen des Bundes als Rahmen für die Entwicklung sachgerechter Anforderungen an Auftragnehmer (Eignung) und IT-Produkte (Spezifikation) für die Durchführung von Vergabeverfahren berücksichtigt werden. Die Vorschriften des Vergaberechts und des Geheimschutzes bleiben unberührt.		Verschoben nach § 42 Abs. 3 nF.
350	(3) Die Bereitstellung von IT-Sicherheitsprodukten durch das Bundesamt nach § 3 Absatz 1 Satz 2 Nummer 11 erfolgt durch Eigenentwicklung oder nach Durchführung von Vergabeverfahren aufgrund einer entsprechenden Bedarfsfeststellung. IT-Sicherheitsprodukte können nur in begründeten Ausnahmefällen durch eine Eigenentwicklung des Bundesamtes zur Verfügung gestellt werden. Die Vorschriften des Vergaberechts bleiben unberührt. Wenn das Bundesamt IT-Sicherheitsprodukte bereitstellt, können die Stellen des Bundes oder von ihnen beauftragte Dritte diese Produkte beim Bundesamt abrufen. Durch Beschluss des Rats der IT-	Die Bereitstellung von IT-Sicherheitsprodukten durch das Bundesamt nach § 3 Absatz 1 Satz 2 Nummer 11 erfolgt durch Eigenentwicklung oder nach Durchführung von Vergabeverfahren aufgrund einer entsprechenden Bedarfsfeststellung. IT-Sicherheitsprodukte können nur in begründeten Ausnahmefällen durch eine Eigenentwicklung des Bundesamtes zur Verfügung gestellt werden. Die Vorschriften des Vergaberechts bleiben unberührt. Wenn das Bundesamt IT-Sicherheitsprodukte bereitstellt, können die Einrichtungen der Bundesverwaltung oder von ihnen beauftragte Dritte diese Produkte beim Bundesamt abrufen.	Sätze 4-6 verschoben in Vorgaben des Bundesamtes, § 42 Abs. 4. Aufgrund Verschiebung bzw. Entfallen der übrigen Absätze wird § 8 Abs. 3 aF. der einzige Absatz der Vorschrift. Begriffskonsolidierung: Einrichtungen der Bundesverwaltung. Erweiterung des Anwendungsbereichs zum Schutz der gesamten Kommunikationstechnik des Bundes.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Beauftragten der Bundesregierung kann festgelegt werden, dass die Bundesbehörden verpflichtet sind, diese Produkte beim Bundesamt abzurufen. Eigenbeschaffungen anderer Bundesbehörden sind in diesem Fall nur zulässig, wenn das spezifische Anforderungsprofil den Einsatz abweichender Produkte erfordert. Die Sätze 5 und 6 gelten nicht für die in § 2 Absatz 3 Satz 2 genannten Gerichte und Verfassungsorgane.		
351	(4) Zur Gewährleistung der Sicherheit in der Informationstechnik bei der Planung und Umsetzung von wesentlichen Digitalisierungsvorhaben des Bundes soll die jeweils verantwortliche Stelle das Bundesamt frühzeitig beteiligen und dem Bundesamt Gelegenheit zur Stellungnahme geben.		Verschoben nach § 43b Abs. 2 nF.
352		Kapitel 2 Datenverarbeitungen	Neue Gliederung zur Steigerung der Übersichtlichkeit
353	*§ 3a* *Verarbeitung personenbezogener Daten*	§ 20 Verarbeitung personenbezogener Daten	Verschoben von § 3a aF., neue Enummerierung.
354	*(1) Die Verarbeitung personenbezogener Daten durch das Bundesamt ist zulässig, wenn die Verarbeitung zur Erfüllung seiner im öffentlichen Interesse liegenden Aufgaben erforderlich ist.*	(1) Die Verarbeitung personenbezogener Daten durch das Bundesamt ist zulässig, wenn die Verarbeitung zur Erfüllung seiner im öffentlichen Interesse liegenden Aufgaben erforderlich ist.	(unverändert)
355	*(2) Die Verarbeitung personenbezogener Daten durch das Bundesamt zu anderen Zwecken als demjenigen, zu dem die Daten ursprünglich erhoben wurden, ist unbeschadet von Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom*	(2) Die Verarbeitung personenbezogener Daten durch das Bundesamt zu anderen Zwecken als demjenigen, zu dem die Daten ursprünglich erhoben wurden, ist unbeschadet von Artikel 6 Absatz 4 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom	(unverändert)

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2) in der jeweils geltenden Fassung und von § 23 des Bundesdatenschutzgesetzes zulässig, wenn	4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2) in der jeweils geltenden Fassung und von § 23 des Bundesdatenschutzgesetzes zulässig, wenn	
356	*1. die Verarbeitung erforderlich ist*	1. die Verarbeitung erforderlich ist	(unverändert)
357	*a) zur Sammlung, Auswertung oder Untersuchung von Informationen über Sicherheitsrisiken oder Sicherheitsvorkehrungen für die Informationstechnik oder*	a) zur Sammlung, Auswertung oder Untersuchung von Informationen über Sicherheitsrisiken oder Sicherheitsvorkehrungen für die Informationstechnik oder	(unverändert)
358	*b) zur Unterstützung, Beratung oder Warnung in Fragen der Sicherheit in der Informationstechnik und*	b) zur Unterstützung, Beratung oder Warnung in Fragen der Sicherheit in der Informationstechnik und	(unverändert)
359	*2. kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.*	2. kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.	(unverändert)
360	*(3) Eine Verarbeitung von besonderen Kategorien personenbezogener Daten durch das Bundesamt ist abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 und unbeschadet des § 22 Absatz 1 des Bundesdatenschutzgesetzes zulässig, wenn*	(3) Eine Verarbeitung von besonderen Kategorien personenbezogener Daten durch das Bundesamt ist abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 und unbeschadet des § 22 Absatz 1 des Bundesdatenschutzgesetzes zulässig, wenn	(unverändert)
361	*1. die Verarbeitung erforderlich ist zur Abwehr einer erheblichen Gefahr für die Netz-, Daten- oder Informationssicherheit,*	1. die Verarbeitung erforderlich ist zur Abwehr einer erheblichen Gefahr für die Netz-, Daten- oder Informationssicherheit,	(unverändert)
362	*2. ein Ausschluss dieser Daten von der Verarbeitung die Erfüllung der Aufgaben des Bundesamtes unmöglich machen oder diese erheblich gefährden würde und*	2. ein Ausschluss dieser Daten von der Verarbeitung die Erfüllung der Aufgaben des Bundesamtes unmöglich machen oder diese erheblich gefährden würde und	(unverändert)

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
363	*3. kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss dieser Daten von der Verarbeitung überwiegt.*	3. kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss dieser Daten von der Verarbeitung überwiegt.	(unverändert)
364	*(4) Das Bundesamt sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2 des Bundesdatenschutzgesetzes vor.*	(4) Das Bundesamt sieht angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person gemäß § 22 Absatz 2 Satz 2 des Bundesdatenschutzgesetzes vor.	(unverändert)
365	*§ 6* *Beschränkungen der Rechte der betroffenen Person*	§ 21 Beschränkungen der Rechte der betroffenen Person	Verschoben von § 6 aF., neue Enummerierung.
366	*Für die Rechte der betroffenen Person gegen das Bundesamt gelten ergänzend zu den in der Verordnung (EU) 2016/679 enthaltenen Ausnahmen die nachfolgenden Beschränkungen. Soweit dieses Gesetz keine oder geringere Beschränkungen der Rechte der betroffenen Person enthält, gelten für die Beschränkungen im Übrigen die Regelungen des Bundesdatenschutzgesetzes ergänzend.*	Für die Rechte der betroffenen Person gegen das Bundesamt gelten ergänzend zu den in der Verordnung (EU) 2016/679 enthaltenen Ausnahmen die nachfolgenden Beschränkungen. Soweit dieses Gesetz keine oder geringere Beschränkungen der Rechte der betroffenen Person enthält, gelten für die Beschränkungen im Übrigen die Regelungen des Bundesdatenschutzgesetzes ergänzend.	(unverändert)
367	*§ 6a* *Informationspflicht bei Erhebung von personenbezogenen Daten*	§ 22 Informationspflicht bei Erhebung von personenbezogenen Daten	Verschoben von § 6a aF., neue Enummerierung.
368	*(1) Die Pflicht zur Information gemäß den Artikeln 13 und 14 der Verordnung (EU) 2016/679 besteht ergänzend zu den in Artikel 13 Absatz 4 und Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht, wenn*	(1) Die Pflicht zur Information gemäß den Artikeln 13 und 14 der Verordnung (EU) 2016/679 besteht ergänzend zu den in Artikel 13 Absatz 4 und Artikel 14 Absatz 5 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht, wenn	(unverändert)
369	*1. die Informationserteilung die ordnungsgemäße Erfüllung der in der Zuständigkeit des Bundesamtes*	1. die Informationserteilung die ordnungsgemäße Erfüllung der in der Zuständigkeit des Bundesamtes	(unverändert)

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	liegenden Aufgaben gefährden würde oder	liegenden Aufgaben gefährden würde oder	
370	*2. die Informationserteilung die öffentliche Sicherheit oder Ordnung oder die Gewährleistung der Netz- und Informationssicherheit auf sonstige Weise gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde*	2. die Informationserteilung die öffentliche Sicherheit oder Ordnung oder die Gewährleistung der Netz- und Informationssicherheit auf sonstige Weise gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde	(unverändert)
371	*und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss.*	und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss.	(unverändert)
372	*(2) Unterbleibt eine Information der betroffenen Person nach Maßgabe des Absatzes 1, ergreift das Bundesamt geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung der in Artikel 13 Absatz 1 und 2 und Artikel 14 Absatz 1 und 2 der Verordnung (EU) 2016/679 genannten Informationen für die Öffentlichkeit in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache. Das Bundesamt hält schriftlich fest, aus welchen Gründen es von einer Information der betroffenen Person abgesehen hat.*	(2) Unterbleibt eine Information der betroffenen Person nach Maßgabe des Absatzes 1, ergreift das Bundesamt geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person, einschließlich der Bereitstellung der in Artikel 13 Absatz 1 und 2 und Artikel 14 Absatz 1 und 2 der Verordnung (EU) 2016/679 genannten Informationen für die Öffentlichkeit in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache. Das Bundesamt hält schriftlich fest, aus welchen Gründen es von einer Information der betroffenen Person abgesehen hat.	(unverändert)
373	*§ 6b* *Auskunftsrecht der betroffenen Person*	§ 23 Auskunftsrecht der betroffenen Person	Verschoben von § 6b aF., neue Enummerierung.
374	*(1) Das Recht auf Auskunft gemäß Artikel 15 Absatz 1 und 2 der Verordnung (EU) 2016/679 besteht nicht, wenn und soweit*	(1) Das Recht auf Auskunft gemäß Artikel 15 Absatz 1 und 2 der Verordnung (EU) 2016/679 besteht nicht, wenn und soweit	(unverändert)
375	*1. die Auskunftserteilung die ordnungsgemäße Erfüllung der Aufgaben*	1. die Auskunftserteilung die ordnungsgemäße Erfüllung der Aufgaben	(unverändert)

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	gefährden würde, die in der Zuständigkeit des Bundesamtes liegen,	gefährden würde, die in der Zuständigkeit des Bundesamtes liegen,	
376	*2. die Auskunftserteilung*	2. die Auskunftserteilung	(unverändert)
377	*a) die öffentliche Sicherheit oder Ordnung oder die Gewährleistung der Netz- und Informationssicherheit gefährden würde oder*	a) die öffentliche Sicherheit oder Ordnung oder die Gewährleistung der Netz- und Informationssicherheit gefährden würde oder	(unverändert)
378	*b) sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde oder*	b) sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde oder	(unverändert)
379	*3. die Auskunftserteilung strafrechtliche Ermittlungen oder die Verfolgung von Straftaten gefährden würde*	3. die Auskunftserteilung strafrechtliche Ermittlungen oder die Verfolgung von Straftaten gefährden würde	(unverändert)
380	*und deswegen das Interesse der betroffenen Person an der Auskunftserteilung zurücktreten muss.*	und deswegen das Interesse der betroffenen Person an der Auskunftserteilung zurücktreten muss.	(unverändert)
381	*(2) § 34 Absatz 2 bis 4 des Bundesdatenschutzgesetzes gilt entsprechend.*	(2) § 34 Absatz 2 bis 4 des Bundesdatenschutzgesetzes gilt entsprechend.	(unverändert)
382	*§ 6c* *Recht auf Berichtigung*	§ 24 Recht auf Berichtigung	Verschoben von § 6c aF., neue Enummerierung.
383	*(1) Das Recht der betroffenen Person auf Berichtigung und Vervollständigung gemäß Artikel 16 der Verordnung (EU) 2016/679 besteht nicht, wenn und soweit die Erfüllung der Rechte der betroffenen Person die ordnungsgemäße Erfüllung der in der Zuständigkeit des Bundesamtes liegenden Aufgaben gefährden würde und deswegen das Interesse der betroffenen Person an der Ausübung dieser Rechte zurücktreten muss.*	(1) Das Recht der betroffenen Person auf Berichtigung und Vervollständigung gemäß Artikel 16 der Verordnung (EU) 2016/679 besteht nicht, wenn und soweit die Erfüllung der Rechte der betroffenen Person die ordnungsgemäße Erfüllung der in der Zuständigkeit des Bundesamtes liegenden Aufgaben gefährden würde und deswegen das Interesse der betroffenen Person an der Ausübung dieser Rechte zurücktreten muss.	(unverändert)

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
384	*(2) In den Fällen des Absatzes 1 hat die betroffene Person einen Anspruch darauf, den Daten für die Dauer der Verarbeitung eine Gegendarstellung beizufügen, sofern dies für eine faire und transparente Verarbeitung erforderlich ist.*	(2) In den Fällen des Absatzes 1 hat die betroffene Person einen Anspruch darauf, den Daten für die Dauer der Verarbeitung eine Gegendarstellung beizufügen, sofern dies für eine faire und transparente Verarbeitung erforderlich ist.	(unverändert)
385	*§ 6d* *Recht auf Löschung*	§ 25 Recht auf Löschung	Verschoben von § 6d aF., neue Enummerierung.
386	*(1) Im Fall der nicht automatisierten Verarbeitung besteht die Pflicht des Bundesamtes zur Löschung personenbezogener Daten gemäß Artikel 17 Absatz 1 und 2 der Verordnung (EU) 2016/679 ergänzend zu den in Artikel 17 Absatz 3 genannten Ausnahmen nicht, wenn*	(1) Im Fall der nicht automatisierten Verarbeitung besteht die Pflicht des Bundesamtes zur Löschung personenbezogener Daten gemäß Artikel 17 Absatz 1 und 2 der Verordnung (EU) 2016/679 ergänzend zu den in Artikel 17 Absatz 3 genannten Ausnahmen nicht, wenn	(unverändert)
387	*1. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist und*	1. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist und	(unverändert)
388	*2. das Interesse der betroffenen Person an der Löschung als gering anzusehen ist.*	2. das Interesse der betroffenen Person an der Löschung als gering anzusehen ist.	(unverändert)
389	*In diesem Fall tritt an die Stelle der Löschung eine Einschränkung der Verarbeitung gemäß Artikel 18 der Verordnung (EU) 2016/679. Die Sätze 1 und 2 sind nicht anzuwenden, wenn die personenbezogenen Daten unrechtmäßig verarbeitet wurden.*	In diesem Fall tritt an die Stelle der Löschung eine Einschränkung der Verarbeitung gemäß Artikel 18 der Verordnung (EU) 2016/679. Die Sätze 1 und 2 sind nicht anzuwenden, wenn die personenbezogenen Daten unrechtmäßig verarbeitet wurden.	(unverändert)
390	*(2) Ist die Löschung lediglich für eine etwaige gerichtliche Überprüfung von Maßnahmen nach § 5 Absatz 3 zurückgestellt, dürfen die Daten ohne Einwilligung der betroffenen Person nur zu diesem Zweck verwendet werden; sie sind für andere Zwecke in der Verarbeitung einzuschränken. § 5 Absatz 7 bleibt unberührt.*	(2) Ist die Löschung lediglich für eine etwaige gerichtliche Überprüfung von Maßnahmen nach § 8 Absatz 3 zurückgestellt, dürfen die Daten ohne Einwilligung der betroffenen Person nur zu diesem Zweck verwendet werden; sie sind für andere Zwecke in der Verarbeitung einzuschränken. § 8 Absatz 7 bleibt unberührt.	Anpassung des Verweises.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
391	*§ 6e* *Recht auf Einschränkung der Verarbeitung*	§ 26 Recht auf Einschränkung der Verarbeitung	Verschoben von § 6e aF., neue Enummerierung.
392	*Die Pflicht des Bundesamtes zur Einschränkung der Verarbeitung gemäß Artikel 18 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679 besteht für die Dauer der Überprüfung der Richtigkeit der personenbezogenen Daten nicht, wenn*	Die Pflicht des Bundesamtes zur Einschränkung der Verarbeitung gemäß Artikel 18 Absatz 1 Buchstabe a der Verordnung (EU) 2016/679 besteht für die Dauer der Überprüfung der Richtigkeit der personenbezogenen Daten nicht, wenn	(unverändert)
393	*1. die Verarbeitung oder Weiterverarbeitung durch dieses Gesetz ausdrücklich geregelt ist oder*	1. die Verarbeitung oder Weiterverarbeitung durch dieses Gesetz ausdrücklich geregelt ist oder	(unverändert)
394	*2. die Einschränkung der Verarbeitung die Abwehr von Gefahren für die Sicherheit in der Informationstechnik gefährden würde*	2. die Einschränkung der Verarbeitung die Abwehr von Gefahren für die Sicherheit in der Informationstechnik gefährden würde	(unverändert)
395	*und deswegen das Interesse der betroffenen Person an der Einschränkung zurücktreten muss.*	und deswegen das Interesse der betroffenen Person an der Einschränkung zurücktreten muss.	(unverändert)
396	§ 6f Widerspruchsrecht	§ 27 Widerspruchsrecht	Verschoben von § 6b aF., neue Enummerierung.
397	Das Recht der betroffenen Person auf Widerspruch gemäß Artikel 21 Absatz 1 der Verordnung (EU) 2016/679 besteht nicht, wenn	Das Recht der betroffenen Person auf Widerspruch gemäß Artikel 21 Absatz 1 der Verordnung (EU) 2016/679 besteht nicht, wenn	(unverändert)
398	1. an der Verarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der betroffenen Person überwiegt, oder	1. an der Verarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der betroffenen Person überwiegt, oder	
399	2. eine Rechtsvorschrift das Bundesamt zur Verarbeitung verpflichtet.	2. eine Rechtsvorschrift das Bundesamt zur Verarbeitung verpflichtet.	
400	Darüber hinaus darf das Bundesamt die personenbezogenen Daten ergänzend zu Artikel 21	Darüber hinaus darf das Bundesamt die personenbezogenen Daten ergänzend zu Artikel 21	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Absatz 1 Satz 2 der Verordnung (EU) 2016/679 so lange verarbeiten, bis das Bundesamt geprüft hat, ob zwingende schutzwürdige Gründe für die Verarbeitung bestehen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen.	Absatz 1 Satz 2 der Verordnung (EU) 2016/679 so lange verarbeiten, bis das Bundesamt geprüft hat, ob zwingende schutzwürdige Gründe für die Verarbeitung bestehen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen.	
401		Teil 3 Sicherheit in der Informationstechnik von Einrichtungen	Neue Gliederung zur Steigerung der Übersichtlichkeit
402		Kapitel 1 Anwendungsbereich	s.o.
403		§ 28 Anwendungsbereich, Betreiber kritischer Anlagen, besonders wichtige Einrichtungen und wichtige Einrichtungen	Umsetzung Art. 3 NIS-2
404		(1) Teil 3 Kapitel 2 und Teil 7 sind auf Betreiber kritischer Anlagen, besonders wichtige Einrichtungen und wichtige Einrichtungen nur anwendbar, soweit dies durch die Rechtsverordnung nach § 53 Absatz 1 festgelegt wurde.	Die Regelungssystematik bereitet die Verschiebung der in Abs. 2 ff. enthaltenen Definitionen von Betreibern kritischer Anlagen, besonders wichtigen Einrichtungen und wichtigen Einrichtungen in das zukünftige KRITIS-Dachgesetz vor. Ob die vorgenannten Betreiber und Einrichtungen (auch) Gegenstand der Cybersicherheitsregulierung sind, wird in der Rechtsverordnung bestimmt, die perspektivisch auch bestimmen wird, ob die Betreiber und Einrichtungen auch Gegenstand der Regulierung der physischen Sicherheit sind.
405	*(10) Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die*	(2) Ein Betreiber kritischer Anlagen ist eine natürliche oder juristische Personen oder eine rechtlich unselbständige Organisationseinheit einer Gebietskörperschaft, die unter Berücksichtigung der	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung angehören und *2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.* *Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmt.* *(§ 1 Abs. 1 Nr. 2 BSI-KritisV)* *(1) Im Sinne dieser Verordnung ist oder sind* *(...)* *2. Betreiber* *eine natürliche oder juristische Person, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf die Beschaffenheit und den Betrieb einer Anlage oder Teilen davon ausübt,*	rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf eine kritische Anlage ausübt.	
406		(2a) Eine kritische Anlage ist eine Anlage, den Sektoren Energie, Verkehr und Transport, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, Ernährung, Digitale	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		Infrastruktur, sowie Siedlungsabfallentsorgung angehört und die von hoher Bedeutung für das Funktionieren des Gemeinwesens ist, da durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden; welche Anlagen im Einzelnen kritische Anlagen sind, bestimmt sich nach der Rechtsverordnung nach § 53 Absatz 1.	
407		(2b) Eine Anlage ist ab dem durch die Rechtsverordnung nach § 53 Absatz 1 festgelegten Stichtag eine kritische Anlage, wenn sie einer der durch Verordnung festgelegten Anlagenarten zuzuordnen ist und die durch Verordnung festgelegten Schwellenwerte erreicht oder überschreitet.	
408		(2c) Eine Anlage ist ab dem nächsten folgenden durch die Rechtsverordnung nach § 53 Absatz 1 als Stichtag festgelegten Tag keine kritische Anlage mehr, wenn sie die durch die Verordnung festgelegten Schwellenwerte unterschreitet.	
409		(3) Eine besonders wichtige Einrichtung ist	Umsetzung Art. 3 Abs. 1 NIS-2
410		1. ein Großunternehmen, das einer der durch Rechtsverordnung nach § 53 Absatz 1 bestimmten Einrichtungsarten der Sektoren Energie, Verkehr und Transport, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, digitale Infrastruktur, Verwaltung von IKT-Diensten (Business-to-Business) oder Weltraum zuzuordnen ist,	Umsetzung Art. 3 Abs. 1 lit. a NIS-2
411		2. ein qualifizierter Vertrauensdiensteanbieter, Top Level Domain Name Registries oder DNS-	Umsetzung Art. 3 Abs. 1 lit. b NIS-2

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		Diensteanbieter, jeweils unabhängig von der Unternehmensgröße	
412		3. ein mittleres Unternehmen, das Anbieter von Telekommunikationsdiensten oder öffentlich zugänglichen Telekommunikationsnetzen ist,	Umsetzung Art. 3 Abs. 1 lit. c NIS-2 Unter dem Begriff „öffentlich zugängliche Telekommunikationsdienste“ werden solche im Sinne des § 3 Nr.44 des Telekommunikationsgesetzes verstanden: Umsetzung von Art. 6 Ziff. 36 NIS-2 („öffentliches elektronisches Kommunikationsnetz)
413		4. ein Betreiber kritischer Anlagen	
414		5. eine Einrichtung, die gemäß Rechtsverordnung nach § 53 Absatz 1 dem Teilsektor Zentralregierung des Sektors öffentliche Verwaltung angehört,	Umsetzung Art. 3 Abs. 1 lit. d iVm. Art. 2 Abs. 2 lit. f Ziff. i NIS-2 – Unter den NIS-2-Begriff „Zentralregierung“ im Sinne der NIS-2-Richtlinie werden in Anlehnung an die deutsche Definition von „zentrale Regierungsbehörden“ in der Richtlinie 2014/24/EU die Bundesministerien und das Bundeskanzleramt gefasst.
415		ausgenommen Einrichtungen, die gemäß Artikel 2 Absatz 4 der Verordnung (EU) 2022/2554 von deren Anwendungsbereich ausgenommen wurden,	Umsetzung Art. 2 Abs. 10 NIS-2. [*Anm. BMI CI 1 – Ausgestaltung der Ausnahme für DORA mit BMF noch iRd. Ressortabstimmung abzustimmen.*]
416		(4) Eine wichtige Einrichtung ist	
417		1. ein mittleres Unternehmen, das einer der durch Rechtsverordnung nach § 57 53 Absatz 1 bestimmten Einrichtungsarten der Sektoren Energie, Transport und Verkehr, Bankwesen, Finanzmarktinfrastrukturen,	Umsetzung Art. 3 Abs. 2 NIS-2. Im Übrigen werden die bisherigen „Unternehmen im besonderen öffentlichen Interesse“ der neuen Einrichtungskategorie „Wichtige Einrichtungen“ hinzugefügt.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		Gesundheitswesen, Trinkwasser, Abwasser, digitale Infrastruktur, Verwaltung von IKT-Diensten (Business-to-Business) oder Weltraum zuzuordnen ist,	
418		2. ein mittleres Unternehmen oder Großunternehmen, das einer der durch Rechtsverordnung nach § 57 Absatz 1 bestimmten Einrichtungsarten der Sektoren Logistik, Siedlungsabfall, Produktion, Chemie, Ernährung, verarbeitendes Gewerbe, Anbieter digitaler Dienste oder Forschung zuzuordnen ist,	
419		3. Vertrauensanbieter	Umsetzung von Art. 2 Abs. 2 lit. a ii NIS-2. Während qualifizierte Vertrauensanbieter wesentliche Einrichtungen sind, sind Vertrauensdiensteanbieter wichtige Einrichtungen.
420		4. wer Güter im Sinne des Teils B der Kriegswaffenliste herstellt oder entwickelt oder vom Bundesamt zugelassene Produkte mit IT-Sicherheitsfunktionen zur Verarbeitung staatlicher Verschlusssachen oder für die IT-Sicherheitsfunktion wesentliche Komponenten solcher Produkte herstellt,	Die Änderung dient der Korrektur, eines Regelungszustandes, der durch die Verwendung eines dynamischen Verweises im IT-Sicherheitsgesetz 2.0 entstanden ist. Dafür wird anstelle eines Verweises der Wortlaut der früheren Fassung des § 60 Absatz 1 Nummern 1 und 3 AWV unmittelbar in das BSIG übernommen. Die Begründung und alle weiteren Ausführungen zu den Gesetzesfolgen sind im IT-Sicherheitsgesetz 2.0 enthalten. Durch die vorliegende

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			Änderung werden dir dort genannten Angaben künftig wieder zutreffend sein
421		5. wer Betreiber eines Betriebsbereichs der oberen Klasse im Sinne der Störfall-Verordnung in der jeweils geltenden Fassung oder nach § 1 Absatz 2 der Störfall-Verordnung einem solchen gleichgestellt ist,	
422		und keine besonders wichtige Einrichtung ist	
423		sowie ausgenommen Einrichtungen, die gemäß Artikel 2 Absatz 4 der Verordnung (EU) 2022/2554 von deren Anwendungsbereich ausgenommen wurden,	Umsetzung Art. 2 Abs. 10 NIS-2. [*Anm. BMI CI 1 – Ausgestaltung der Ausnahme für DORA mit BMF noch iRd. Ressortabstimmung abzustimmen.*]
424		(5) § 31 und § 32 gelten nicht für	
425		1. Betreiber kritischer Anlagen, besonders wichtige Einrichtungen und wichtige Einrichtungen , soweit sie ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen,	Verschoben von § 8d Abs. 2 Nr. 1; Umsetzung von Erwägungsgrund 92, 95
426		2. die Gesellschaft für Telematik nach § 306 Absatz 1 Satz 3 des Fünften Buches Sozialgesetzbuch, Betreiber von Diensten der Telematikinfrastruktur im Hinblick auf die nach § 311 Absatz 6 und § 325 des Fünften Buches Sozialgesetzbuch zugelassenen Dienste und Betreiber von Diensten, soweit sie die Telematikinfrastruktur für nach § 327 Absatz 2 bis 5 des Fünften Buches Sozialgesetzbuch bestätigte Anwendungen nutzen,	Verschoben von § 8d Abs. 2 Nr. 3 [*Anm. BMI CI 1 – Ob und in wieweit diese bisherige Ausnahme aus dem Anwendungsbereich in Ansehung der NIS-2-Vorgaben bestehen bleiben kann, ist Gegenstand der Abstimmung mit BMG im Rahmen der Ressortabstimmung. Einschlägig in diesem Sinne könnte u.a. die NIS-2-Einrichtungsart „Gesundheitsdienstleister“ des Sektors „Gesundheitswesen“ sein (vgl. NIS-2 Anhang I Ziff. 5 erster Spiegelstrich).*]

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
427		§ 27 Einrichtungen der Bundesverwaltung	In vielen Einrichtungen der Bundesverwaltung besteht ein Defizit bei der Umsetzung von Maßnahmen zum Eigenschutz im Bereich der Informationssicherheit. Die bisherigen Steuerungsinstrumente auf überwiegend untergesetzlicher Basis (z.B. Umsetzungsplan Bund) haben sich als nicht ausreichend effektiv erwiesen, um eine flächendeckende wirksame Steigerung des Sicherheitsniveaus zu erreichen. Vor dem Hintergrund der durch aktuelle geopolitische Entwicklungen („Zeitenwende“) abermals verschärften Bedrohungslage hat sich das Risiko für staatliche Einrichtungen zudem weiter erhöht, durch Gefährdungen aus dem Cyberraum in ihrer Handlungsfähigkeit eingeschränkt zu werden. Die NIS-2-Umsetzung wird deshalb durch diese und weitere Bestimmungen begleitet mit weiteren Regelungen für die Bundesverwaltung, die über die reine Richtlinienumsetzung hinausgehen. Um auf Bundesebene auch vor dem Hintergrund von Verflechtung und Konsolidierung der IT insgesamt ein gemeinsames, kohärentes und handhabbares Regime zu erreichen, werden in nationaler Verantwortung Anforderungen formuliert, die inhaltlich an denjenigen für Wesentliche Einrichtungen der NIS-2-Richtlinie orientiert sind und deren Anwendungsbereich entlang der

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			Mindeststandards nach § 8 BSIG aF. modelliert ist.
428		(1) Ergänzend zu § 28 sind die Pflichten besonders wichtiger Einrichtungen dieses Teils auf Einrichtungen der Bundesverwaltung entsprechend anzuwenden, sofern in Kapitel 3 nichts Abweichendes geregelt ist. Einrichtungen der Bundesverwaltung sind	Die Norm dient als Generalklausel zur grundsätzlichen Erweiterung des Anwendungsbereichs auf Einrichtungen der Bundesverwaltung, die selbst weder besonders wichtige Einrichtungen noch wichtige Einrichtungen sind. Vor dem Hintergrund des Schutzzwecks der Informationssicherheit des Bundes und zum Zwecke der Begriffskonsolidierung ist die Definition orientiert am bisherigen Anwendungsbereich von § 8 Abs. 1 BSIG a.F. sowie dem Geltungsbereich des UP Bund, mit dem der Begriff der Einrichtungen der Bundesverwaltung bereits etabliert worden ist. Damit wird auch dem Umstand begegnet, dass in der Vergangenheit mitunter Unklarheiten bestanden, ob und für welche Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts die Geltung der Mindeststandards angeordnet war. Zur Vermeidung von Unverhältnismäßigkeiten wird die bisherige Anordnungsmöglichkeit für die Mindeststandards und UP Bund mit der Möglichkeit gem. § 43a Abs. 4 ersetzt, dass die Ressorts Ausnahmebescheide für entsprechende Einrichtungen erlassen.
429		1. Stellen des Bundes,	Der Begriff wird inhaltsgleich mit § 8 Absatz 1 Satz 1 Nummer 1 a.F. verwendet.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
430		2. Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie ihre Vereinigungen ungeachtet ihrer Rechtsform auf Bundesebene, sowie	Die Begriffe werden inhaltsgleich mit § 8 Absatz 1 Satz 1 Nummer 2 a.F. verwendet. Auf das Anordnungserfordernis wird auf Basis der Erwägungen in Zeile 434 verzichtet.
431		3. öffentliche Unternehmen, die mehrheitlich im Eigentum des Bundes stehen und die IT-Dienstleistungen für die Bundesverwaltung erbringen	Die Begriffe werden inhaltsgleich mit den bisherigen § 8 Absatz 1 Satz 1 Nummer 3 a.F. verwendet. Auch hier gilt, dass Einrichtungen bei Bedarf teilweise oder ganz von Ressort-ISBs durch Ausnahmebescheid von Verpflichtungen befreit werden können.
432		(2) Kapitel 3 ist auf besonders wichtige Einrichtungen nach § 28 Absatz 3 Nummer 4 vorrangig anzuwenden. Auf andere Einrichtungen der Bundesverwaltung, die zugleich besonders wichtige oder wichtige Einrichtungen sind, findet Kapitel 3 keine Anwendung.	Die Differenzierung erfolgt zwecks klarer Zuordnung: die Zentralregierung wird von Kapitel 3 miterfasst. Falls andere Einrichtungen der Bundesverwaltung zugleich besonders wichtige oder wichtige Einrichtungen wären, dann ist Kapitel 2 vollständig und ausschließlich anzuwenden.
433		(3) Die Ausnahme nach § 7 Absatz 6 gilt entsprechend.	Verweis auf die Ausnahme für den Bereich der Streitkräfte und des Militärischen Abschirmdienstes.
434		Kapitel 2 Risikomanagement, Melde-, Registrierungs-, Nachweis- und Unterrichtungspflichten	Neue Gliederung zur Verbesserung der Übersichtlichkeit

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
435		§ 30 Risikomanagementmaßnahmen	Umsetzung Art. 21 NIS-2
436		(1) Besonders wichtige Einrichtungen und wichtige Einrichtungen nach sind verpflichtet, verhältnismäßige technische und organisatorische Maßnahmen zu ergreifen, um Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen auf ihre oder andere Dienste zu verhindern oder möglichst gering zu halten.	Umsetzung Art. 21 Abs. 1 und 4 NIS-2. Risiken sind das Potenzial für Verluste oder Störungen, die durch einen Sicherheitsvorfall verursacht werden, das als eine Kombination des Ausmaßes eines solchen Verlusts oder einer solchen Störung und der Wahrscheinlichkeit des Eintretens des Sicherheitsvorfalls zum Ausdruck gebracht wird.
437		(2) Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten und unter Berücksichtigung der gegebenenfalls einschlägigen europäischen und internationalen Normen sowie der Umsetzungskosten ein Sicherheitsniveau der informationstechnischen Systeme, Komponenten und Prozesse gewährleisten, das dem bestehenden Risiko angemessen ist. Bei der Bewertung, ob Maßnahmen dem bestehenden Risiko angemessen sind, sind das Ausmaß der Risikoexposition und die Größe der Einrichtung oder des Betreibers sowie die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen, zu berücksichtigen.	Umsetzung Art. 21 Abs. 1 Uabs. 2 NIS-2. Damit keine unverhältnismäßige finanzielle und administrative Belastungen für wesentliche und wichtige Einrichtungen entstehen, sollen die genannten Risikomanagementmaßnahmen in einem angemessenen Verhältnis zu den Risiken stehen, denen das betroffene Netz- und Informationssystem ausgesetzt wird. Hierbei werden u.a. auch den Kosten der Umsetzung sowie der Größe der Einrichtung Rechnung getragen. In die Bewertung der Angemessenheit und Verhältnismäßigkeit kann ebenfalls einfließen, ob wichtige Einrichtungen im Vergleich zu wesentlichen Einrichtungen grundsätzlich einer unterschiedlichen Risikoexposition ausgesetzt sind. „Risiko“ wird als Potenzial für Verluste oder Störungen, die durch einen Sicherheitsvorfall

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			verursacht werden, das als eine Kombination des Ausmaßes eines solchen Verlusts oder einer solchen Störung und der Wahrscheinlichkeit des Eintretens des Sicherheitsvorfalls zum Ausdruck gebracht wird; Umsetzung Art. 6 Ziff. 9 NIS-2, Verwendung in Art. 21 Abs.1 UAbs. 2
438		(3) Für Betreiber kritischer Anlagen gelten für die Bewertung nach Absatz 2, ob Maßnahmen dem bestehenden Risiko angemessen sind, erhöhte Anforderungen für Maßnahmen in Bezug auf das Sicherheitsniveau von informationstechnischen Systemen, Komponenten und Prozessen, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Anlagen maßgeblich sind.	
439		(4) Maßnahmen nach Absatz 1 müssen auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, die informationstechnischen Systeme, Komponenten und Prozesse und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen, und zumindest Folgendes umfassen:	Umsetzung Art. 20 Abs. 2 NIS-2
440		1. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme,	
441		2. Bewältigung von Sicherheitsvorfällen,	Umsetzung von Art. 6 Ziff. 8 NIS 2, Verwendung in Art. 10 Abs. 1, Art. 11 Abs. 5 lit. a, 21 Abs. 2 lit.b
442		3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,	
443		4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern,	
444		5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,	
445		6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit,	
446		7. grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit,	
447		8. Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,	
448		9. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen,	
449		10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.	
450		(5) Der von der Kommission gemäß Artikel 21 Absatz 5 Unterabsatz 1 der NIS-2-Richtlinie erlassene Durchführungsrechtsakt zur Festlegung der	Umsetzung Art. 21 Abs. 5 Uabs. 1 NIS-2

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		technischen und methodischen Anforderungen an die in Absatz 1 genannten Maßnahmen in Bezug auf DNS-Diensteanbieter, TLD-Namenregister, Cloud-Computing-Dienstleister, Anbieter von Rechenzentrumsdiensten, Betreiber von Content Delivery Networks, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter, hat für die vorgenannten Einrichtungsarten Vorrang.	
451		(6) Soweit die Kommission einen Durchführungsrechtsakt gemäß Artikel 21 Absatz 5 Unterabsatz 2 der NIS-2-Richtlinie erlässt, in dem die technischen und methodischen Anforderungen sowie erforderlichenfalls die sektoralen Anforderungen der in Absatz 4 genannten Maßnahmen festgelegt werden, so gehen diese den in Absatz 4 genannten Maßnahmen vor.	Umsetzung Art. 21 Abs. 5 Uabs. 2 NIS-2
452		(7) Soweit die Durchführungsrechtsakte der Kommission nach Artikel 21 Absatz 5 der NIS-2-Richtlinie keine abschließenden Bestimmungen über die technischen und methodischen Anforderungen sowie erforderlichenfalls die sektoralen Anforderungen der in Absatz 4 genannten Maßnahmen in Bezug auf besonders wichtige Einrichtungen und wichtige Einrichtungen enthalten, können diese Bestimmungen vom Bundesministerium des Innern und Heimat im Benehmen mit den jeweils betroffenen Ressorts durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, getroffen werden.	Zur angemessenen Berücksichtigung der Bedrohungslage muss das BSI die Möglichkeit haben, über die ggf. von der KOM veröffentlichten Maßnahmen hinaus, die Umsetzung angemessener Maßnahmen zu fordern.
453		(8) Bei der Erwägung geeigneter Maßnahmen nach Absatz 4 Nummer 4 berücksichtigt die Einrichtung bzw der Betreiber die spezifischen Schwachstellen der einzelnen unmittelbaren Anbieter und Diensteanbieter sowie die Gesamtqualität der Produkte und der	Umsetzung Art. 21 Abs. 3 NIS-2

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		Cybersicherheitspraxis ihrer Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse. Einrichtungen müssen bei der Erwägung geeigneter Maßnahmen nach Satz 1 die Ergebnisse der gemäß Artikel 22 Absatz 1 der NIS-2-Richtlinie durchgeführten koordinierten Risikobewertungen kritischer Lieferketten berücksichtigen.	
454		(9) Verwendet eine besonders wichtige Einrichtung oder eine wichtige Einrichtung ein in einer Rechtsverordnung nach § 57 Absatz 6 bestimmtes IKT-Produkt, einen IKT-Dienst oder IKT-Prozess, so muss dieses oder dieser über eine Cybersicherheitszertifizierung gemäß europäischer Schemata nach Artikel 49 der Verordnung (EU) 2019/881 verfügen.	Umsetzung Art. 24 NIS-2.
455		(9a) Soweit die Kommission einen Durchführungsrechtsakt gemäß Artikel 24 Absatz 2 der NIS-2-Richtlinie erlässt, gehen die darin enthaltenen Vorgaben an den Einsatz zertifizierter IKT-Produkte, IKT-Dienste und IKT-Prozesse denen des Absatz 9 vor	Öffnungsklausel
456		(10) Besonders wichtige Einrichtungen sind ab dem [*Einsetzen: 1 Jahr nach Inkrafttreten*] verpflichtet, am Informationsaustausch nach § 6 teilzunehmen.	Diese Vorschrift geht über die strikte Umsetzung der NIS-2 hinaus. Da die Umsetzung des Art. 29 über die zentrale Austauschplattform des BSI (BISP) umgesetzt wird, soll durch diesen Absatz der bidirektionale Austausch sichergestellt werden.
457		(11) Unbeschadet der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten dürfen der Austausch von Informationen nach § 6 oder die freiwillige Meldung nach § 5 nicht dazu führen, dass der meldenden Einrichtung zusätzliche Verpflichtungen auferlegt werden, die nicht für sie gegolten hätten, wenn sie die Meldung nicht übermittelt hätte.	Umsetzung Art. 30 NIS-2

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
458		(12) Besonders wichtige Einrichtungen nach und ihre Branchenverbände können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach Absatz 1 vorschlagen. Diese müssen Durchführungsrechtsakte der Europäischen Kommission so berücksichtigen. Das Bundesamt stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten. Die Feststellung erfolgt	
459		1. im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe,	
460		2. im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes.	
461			
462		§ 31 Meldepflichten	Umsetzung Art. 23 NIS-2
463			Umsetzung Art. 23 Abs. 1 Uabs. 1 S. 1 NIS-2
464		(1) Besonders wichtige Einrichtungen und wichtige Einrichtungen übermitteln dem Bundesamt über eine vom Bundesamt im Einvernehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete Meldemöglichkeit	Umsetzung Art. 23 Abs. 4 S. 1 NIS-2
465		1. unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, eine frühe Erstmeldung, in der angegeben wird, ob der Verdacht besteht, dass der erhebliche	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte,	
466		2. unverzüglich, spätestens jedoch innerhalb von 72 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, eine Meldung über den Sicherheitsvorfall, in der die in Nummer 1 genannten Informationen bestätigt oder aktualisiert werden und eine erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, sowie gegebenenfalls die Kompromittierungsindikatoren angegeben werden;	
467		3. auf Ersuchen des Bundesamtes eine Zwischenmeldung über relevante Statusaktualisierungen;	
468		4. spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls gemäß Nummer 2, vorbehaltlich Absatz 3, eine Abschlussmeldung, die Folgendes enthält:	
469		a) eine ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen;	
470		b) Angaben zur Art der Bedrohung bzw. zugrunde liegenden Ursache, die	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		wahrscheinlich den Sicherheitsvorfall ausgelöst hat;	
471		c) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen;	
472		d) gegebenenfalls die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls;	
473		(3) Dauert der Sicherheitsvorfall im Zeitpunkt des Absatz 2 Nummer 4 noch an, legt die betreffende Einrichtung statt einer Abschlussmeldung zu diesem Zeitpunkt eine Fortschrittsmeldung und eine Abschlussmeldung innerhalb eines Monats nach Abschluss der Bearbeitung des Sicherheitsvorfalls vor.	Umsetzung Art. 23 Abs. 4 S. 1 lit. e NIS-2
474		(4) Vertrauensdiensteanbieter melden abweichend von Absatz 2 Nummer 2 dem Bundesamt in Bezug auf erhebliche Sicherheitsvorfälle, die sich auf die Erbringung seiner Vertrauensdienste auswirken, unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntniserlangung des erheblichen Sicherheitsvorfalls.	Umsetzung Art. 23 Abs. 4 S. 2
475		(5) Betreiber kritischer Anlagen sind zusätzlich verpflichtet, Angaben zur Art der betroffenen Anlage, der kritischen Dienstleistung und den Auswirkungen des Sicherheitsvorfalls auf diese Dienstleistung zu übermitteln, wenn ein erheblicher Sicherheitsvorfall Auswirkungen auf die von ihnen betriebene kritische Anlage hat oder haben könnte.	
476		(6) Soweit die Kommission einen Durchführungsrechtsakt gemäß Artikel 23 Absatz 11 Unterabsatz 1 der NIS-2-Richtlinie erlässt, in dem die Art der Angaben, das Format oder das Verfahren der Meldungen festgelegt ist, sind diese Vorgaben	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		einzuhalten. Das Bundesamt kann die Einzelheiten zur Ausgestaltung des Meldeverfahrens und zur Konkretisierung der Meldungsinhalte nach Anhörung der betroffenen Betreiber und der betroffenen Wirtschaftsverbände festlegen, soweit sie möglichen Durchführungsrechtsakten der Europäischen Kommission nicht widersprechen.	
477			
478		§ 32 Registrierungspflicht	Umsetzung Art. 3 Abs. 3 NIS-2
479		(1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sowie Domain-Name-Registry-Diensteanbieter sind verpflichtet, spätestens drei Monate nachdem sie erstmals oder erneut als eine der vorgenannten Einrichtungen gelten, dem Bundesamt die folgenden Angaben zu übermitteln:	Umsetzung Art. 3 Abs. 4 Uabs. 2 Satz 1 NIS-2 Gemäß § 27 trifft die Registrierungspflicht entsprechendauch Einrichtungen der Bundesverwaltung im gleichen Umfang. Dies wird in § 41 Absatz 3 Satz 1 klargestellt.
480			Umsetzung Art. 3 Abs. 4 NIS-2
481		1. der Name der Einrichtung, einschließlich der Rechtsform und soweit einschlägig der Handelsregisternummer,	Umsetzung Art. 3 Abs. 4 Uabs. 1 lit. a NIS-2; Erweiterung, da der Name allein in Deutschland nicht eindeutig ist
482		2. die Anschrift und aktuellen Kontaktdaten, einschließlich E-Mail-Adresse, IP-Adressbereiche, Telefonnummern ,	Umsetzung Art. 3 Abs. 4 Uabs. 1 lit. b NIS-2
483		3. der relevante in der Rechtsverordnung nach § 53 Absatz 1 genannte Sektor oder soweit einschlägig Teilsektor,	Umsetzung Art. 3 Abs. 4 Uabs. 1 lit. c NIS-2
484		4. eine Auflistung der Mitgliedstaaten der Europäischen Union, in denen die	Umsetzung Art. 3 Abs. 4 Uabs. 1 lit. d NIS-2

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		Einrichtung Dienste erbringt, die die in der in der Rechtsverordnung nach § 53 Absatz 1 genannten Einrichtungsarten erbringen.	
485		(2) Die Registrierung von besonders wichtigen Einrichtungen, wichtigen Einrichtungen und Domain-Name-Registry-Diensteanbieter kann das Bundesamt auch selbst vornehmen, wenn die Einrichtung oder der Anbieter ihre oder seine Pflicht zur Registrierung nicht erfüllt.	
486	*(3) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens bis zum ersten Werktag, der darauf folgt, dass diese erstmalig oder erneut als Betreiber einer Kritischen Infrastruktur nach der Rechtsverordnung nach § 10 Absatz 1 gelten, die von ihnen betriebenen Kritischen Infrastrukturen beim Bundesamt zu registrieren und eine Kontaktstelle zu benennen. Die Registrierung eines Betreibers einer Kritischen Infrastruktur kann das Bundesamt auch selbst vornehmen, wenn der Betreiber seine Pflicht zur Registrierung nicht erfüllt. Nimmt das Bundesamt eine solche Registrierung selbst vor, informiert es die zuständige Aufsichtsbehörde des Bundes darüber. Die Betreiber haben sicherzustellen, dass sie über die benannte oder durch das Bundesamt festgelegte Kontaktstelle jederzeit erreichbar sind. Die Übermittlung von Informationen durch das Bundesamt nach Absatz 2 Nummer 4 erfolgt an diese Kontaktstelle.*	(3) Betreiber kritischer Anlagen sind verpflichtet, spätestens bis zum ersten Werktag, der darauf folgt, dass diese erstmalig oder erneut als kritische Anlage gelten,	Verschiebung von § 8b Abs. 3; Ergänzung, dass die KRITIS-Betreiber auch die Versorgungskennzahlen ihrer Anlage übermitteln müssen.
487		1. die von ihnen betriebenen kritischen Anlagen beim Bundesamt zu registrieren,	
488		2. die in Absatz 1 genannten Angaben,	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
489		3. Informationen zu einer jederzeit erreichbaren Kontaktstelle und	
490		4 die für die Anlagen gemäß der Rechtsverordnung nach § 53 Absatz 1 ermittelte Anlagenkategorie und Versorgungskennzahlen zu übermitteln.	
491		(4) Die Registrierung einer kritischen Anlage kann das Bundesamt auch selbst vornehmen, wenn der Betreiber seine Pflicht zur Registrierung nicht erfüllt. Nimmt das Bundesamt eine solche Registrierung selbst vor, informiert es die zuständige Aufsichtsbehörde des Bundes darüber. Der Betreiber kritischer Anlagen hat sicherzustellen, dass er über die Angaben nach Absatz 3 Nr. 3 oder durch das Bundesamt festgestellten Kontaktdaten jederzeit erreichbar ist.	
492	*(3a) Rechtfertigen Tatsachen die Annahme, dass ein Betreiber seine Pflicht zur Registrierung nach Absatz 3 nicht erfüllt, so hat der Betreiber dem Bundesamt auf Verlangen die für die Bewertung aus Sicht des Bundesamtes erforderlichen Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorzulegen und Auskunft zu erteilen, soweit nicht Geheimschutzinteressen oder überwiegende Sicherheitsinteressen entgegenstehen.*	(5) Rechtfertigen Tatsachen die Annahme, dass ein Betreiber oder eine Einrichtung ihre Pflicht zur Registrierung nach Absatz 1 oder 2 nicht erfüllt, so hat die Einrichtung dem Bundesamt auf Verlangen die für die Bewertung aus Sicht des Bundesamtes erforderlichen Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorzulegen und Auskunft zu erteilen, soweit nicht Geheimschutzinteressen oder überwiegende Sicherheitsinteressen entgegenstehen.	Verschiebung von § 8b Abs. 3a
493		(6) Bei Änderungen der nach diesem Paragraphen zu übermittelnden Angaben sind diese unverzüglich, spätestens jedoch zwei Wochen ab dem Zeitpunkt der Änderung dem Bundesamt zu übermitteln.	Umsetzung Art. 3 Abs. 4 Uabs. 2 Satz 2 NIS-2
494		(7) Das Bundesamt kann die Einzelheiten zur Ausgestaltung des Registrierungsverfahrens festlegen.	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
495		§ 33 Besondere Registrierungspflicht für bestimmte Einrichtungsarten	Umsetzung Art. 27 Abs. 2-5 NIS-2
496		(1) Eine Einrichtung der in § 63 Absatz 1 Satz 1 genannten Einrichtungsart übermittelt bis zum 17. Januar 2025 dem Bundesamt folgende Angaben:	Umsetzung Art. 27 Abs. 2 NIS-2
497		1. Name der Einrichtung,	Umsetzung Art. 27 Abs. 2 lit. a NIS-2
498		2. einschlägiger Sektor, Teilsektor und Einrichtungsart wie in der in KRITIS-Verordnung weiter bestimmt,	Umsetzung Art. 27 Abs. 2 lit. b NIS-2
499		3. Anschrift der Hauptniederlassung in der Europäischen Union im Sinne des § 63 Absatz 2 und seiner sonstigen Niederlassungen in der Europäischen Union oder, falls er nicht in der Europäischen Union niedergelassen ist, Anschrift seines nach § 63 Absatz 3 benannten Vertreters,	Umsetzung Art. 27 Abs. 2 lit. c NIS-2
500		3. aktuelle Kontaktdaten, einschließlich E-Mail-Adressen und Telefonnummern der Einrichtung und soweit erforderlich, seines nach § 63 Absatz 3 benannten Vertreters,	Umsetzung Art. 27 Abs. 2 lit. d NIS-2
501		4. die Mitgliedstaaten der Europäischen Union, in denen die Einrichtung Dienste erbringt, und	Umsetzung Art. 27 Abs. 2 lit. e NIS-2
502		5. die IP-Adressbereiche der Einrichtung.	Umsetzung Art. 27 Abs. 2 lit. f NIS-2
503		(2) Im Fall einer Änderung der gemäß Absatz 1 übermittelten Angaben unterrichten die Einrichtungen der in Absatz 1 Satz 1 genannten Einrichtungsart das	Umsetzung Art. 27 Abs. 3 NIS-2

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		Bundesamt unverzüglich über diese Änderung, jedoch spätestens innerhalb von drei Monaten ab dem Tag an dem die Änderung eingetreten ist.	
504		(3) Mit Ausnahme der in Absatz 1 Nr. 5 genannten Angaben leitet das Bundesamt die nach diesem Paragraphen übermittelten Angaben an die ENISA weiter.	Umsetzung Art. 27 Abs. 4 NIS-2
505		(4) Das Bundesamt kann für die Übermittlung der Angaben nach Absätzen 1 und 2 eine geeignete Meldemöglichkeit vorsehen.	Umsetzung Art. 27 Abs. 5 NIS-2
506		§ 34 Nachweispflichten für besonders wichtige Einrichtungen	Verschiebungen von § 8a
507		(1) Besonders wichtige Einrichtungen haben die Erfüllung der Anforderungen nach § 30 Absatz 1 spätestens zu einem vom Bundesamt bei der Registrierung festgelegten Zeitpunkt anschließend alle zwei Jahre dem Bundesamt auf geeignete Weise nachzuweisen. Der in Satz 1 genannte Zeitpunkt ist durch das Bundesamt auf einen Zeitpunkt frühestens zwei Jahre und spätestens drei Jahre nach Inkrafttreten dieses Gesetzes festzulegen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Einrichtungen übermitteln dem Bundesamt die Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Das Bundesamt kann die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen. Es kann bei Sicherheitsmängeln die Vorlage eines geeigneten Mängelbeseitigungsplanes und im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		Sicherheitsmängel verlangen. Das Bundesamt kann die Vorlage eines geeigneten Nachweises über die erfolgte Mängelbeseitigung verlangen.	
508		(3) Das Bundesamt kann zur Ausgestaltung des Verfahrens der Prüfungen und Erbringung des Nachweises nach Absatz 1 Anforderungen an die Art und Weise der Durchführung, an die Geeignetheit der zu erbringenden Nachweise sowie fachliche und organisatorische Anforderungen an die Prüfer und die prüfende Stelle nach Anhörung von Vertretern der betroffenen Betreiber und Einrichtungen und der betroffenen Wirtschaftsverbände festlegen.	
509		§ 35 Unterrichtungspflichten	
510		(1) Im Fall eines erheblichen Sicherheitsvorfalls kann das Bundesamt besonders wichtige Einrichtungen und wichtige Einrichtungen anweisen, die Empfänger ihrer Dienste unverzüglich über diese erheblichen Sicherheitsvorfälle zu unterrichten, die die Erbringung des jeweiligen Dienstes beeinträchtigen könnten. Die Unterrichtung nach Satz 1 kann, soweit	Umsetzung Art. 23 Abs. 1 S. 2 NIS-2

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		sinnvoll, auch durch eine Veröffentlichung im Internet erfolgen.	
511	[*Art. 23 Abs. 2: Gegebenenfalls stellen die Mitgliedstaaten sicher, dass wesentliche und wichtige Einrichtungen den potenziell von einer erheblichen Cyberbedrohung betroffenen Empfängern ihrer Dienste unverzüglich alle Maßnahmen oder Abhilfemaßnahmen mitteilen, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können. Die Einrichtungen informieren diese Empfänger gegebenenfalls auch über die erhebliche Cyberbedrohung selbst.*]	(2) Einrichtungen im Sinne des Absatz 1 aus den Sektoren Bankwesen, Digitale Infrastruktur, Verwaltung von IKT-Diensten und Digitale Dienste teilen den potenziell von einer erheblichen Cyberbedrohung betroffenen Empfängern ihrer Dienste unverzüglich alle Maßnahmen oder Abhilfemaßnahmen mit, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können. Die Einrichtungen im Sinne des Absatz 1 informieren diese Empfänger auch über die erhebliche Cyberbedrohung selbst. Die Unterrichtungspflicht nach diesem Absatz gilt nur dann, wenn in Abwägung der Interessen der Einrichtung im Sinne des Absatz 1 und derjenigen des Empfängers letztere überwiegen.	Umsetzung Art. 23 Abs. 2. Nicht in allen Sektoren können die Empfänger von Diensten selbst Maßnahmen gegen Cyberbedrohungen ergreifen. Gerade bei der Versorgung mit Elektrizität oder Waren sind die Empfänger nicht selbst der Cyberbedrohung ausgesetzt, sondern erst deren Folgen. In den Sektoren, in denen die Dienste selbst mit Informationssystemen der Empfänger der Dienste interagieren, ist eine Information der Empfänger oftmals sinnvoll. Die Einrichtungen haben sie daher über die Bedrohung selbst und über mögliche Maßnahmen zu unterrichten, die die Empfänger selbst zu ihrem Schutz ergreifen können.
512		§ 36 Rückmeldungen des Bundesamts gegenüber meldenden Einrichtungen	
513		(1) Im Fall einer Meldung durch einen Betreiber oder eine Einrichtung gemäß § 31 übermittelt das Bundesamt der meldenden Einrichtung unverzüglich und nach Möglichkeit innerhalb von 24 Stunden nach Eingang der Frühwarnung gemäß § 31 eine Antwort, einschließlich einer ersten Rückmeldung zu dem erheblichen Sicherheitsvorfall und, auf Ersuchen der Einrichtung, Orientierungshilfen oder operativer Beratung für die Durchführung möglicher Abhilfemaßnahmen. Das Bundesamt leistet, im Rahmen der zur Verfügung stehenden Kapazitäten und der Priorisierung im Ermessen des Bundesamts, auf Ersuchen der betreffenden Einrichtung zusätzliche	Umsetzung Art. 23 Abs. 5 NIS-2;

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		technische Unterstützung. Wird bei dem erheblichen Sicherheitsvorfall ein krimineller Hintergrund vermutet, gibt das Bundesamt ferner Orientierungshilfen für die Meldung des Sicherheitsvorfalls an die Strafverfolgungsbehörden.	
514		(2) Ist eine Sensibilisierung der Öffentlichkeit erforderlich, um einen erheblichen Sicherheitsvorfall zu verhindern oder einen laufenden erheblichen Sicherheitsvorfall zu bewältigen oder liegt die Offenlegung des erheblichen Sicherheitsvorfalls anderweitig im öffentlichen Interesse, so kann das Bundesamt nach Konsultation des betreffenden Betreibers oder der betreffenden Einrichtung die Öffentlichkeit über den erheblichen Sicherheitsvorfall informieren oder den Betreiber oder die Einrichtung auffordern, dies zu tun.	Umsetzung Art. 23 Abs. 7 NIS-2
515		§ 37 Ausnahmebescheid	Umsetzung Art. 2 Abs. 8 NIS-2. § 35 BSIG n.F. setzt die Möglichkeit der Schaffung einer Ausnahme (s. Art. 2 Abs. 8 RL) um. Der Grund einer teilweisen oder vollständigen Ausnahme von den in Art. 21, 23, 27 der RL (umgesetzt in §§ 30 ff. BSIG n.F.) genannten Pflichten ist die Wahrung des nationalen Sicherheitsinteresses. So ist in den (9) und (10) der Erwägungsgründen der Richtlinie angelegt, dass es zur Wahrung wesentlicher Interessen der nationalen Sicherheit, dem Schutz der öffentlichen Ordnung und der öffentlichen Sicherheit der Mitgliedsstaaten erforderlich sein muss, Einrichtungen von obigen Pflichten auszunehmen, wenn derartige Auskünfte bzw. eine Preisgabe dem nationalen Sicherheitsinteresse

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			zuwiderliefe. Als relevante Bereiche führt Art. 2 Abs. 8 der Richtlinie die Bereiche der nationalen Sicherheit, öffentlichen Sicherheit, der Verteidigung oder Strafverfolgung, einschließlich der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten an. Um dem Sinne einer Ausnahmeregelung, die nicht zu weit greift, gerecht zu werden, ist ein Ausgleich zwischen einem „hohen gemeinsamen Cybersicherheitsniveau“ (s. Erwägungsgrund Nr. 138, 142 der Richtlinie; ausdrückliches Ziel der Richtlinie) und dem Mitgliedsstaatsinteresse der Wahrung nationaler Sicherheitsinteressen zu erbringen.
516		(1) Das Bundesministerium des Innern und für Heimat kann auf Vorschlag des Bundeskanzleramts, des Bundesministeriums für Verteidigung oder auf eigenes Betreiben besonders wichtige Einrichtungen oderwichtige Einrichtungen von Verpflichtungen nach diesem Gesetz nach Maßgabe des Absatzes 2 teilweise (einfacher Ausnahmebescheid) oder des Absatzes 3 insgesamt (erweiterter Ausnahmebescheid) befreien, sofern durch die Einrichtung gleichwertige Vorgaben eingehalten werden.	Umsetzung Art. 2 Abs. 8 NIS-2. Zunächst wird obig genanntem Ziel durch ein begrenztes Vorschlagsrecht, durch Bundeskanzleramt, Bundesverteidigungsministerium und Bundesinnenministerium entsprochen. Ein Eigeninitiativrecht der jeweiligen Einrichtungen würde ausufern. Weiterhin einschränkend sind umfassten Bereiche der Einrichtungen. Hierbei wird insbesondere auf die auch in der Richtlinie explizit genannten, rechtlich anerkannten Kategorien, der öffentlichen Sicherheit und Ordnung verwiesen. Als Begrenzung der Ausnahmeregelung einzubeziehender Erwägungsgrund sollte auf die Wesentlichkeit der Interessen der nationalen Sicherheit abzustellen sein.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			Nicht zuletzt muss andererseits jedoch bei Ausnehmen von den genannten Pflichten das hohe gemeinsame Cybersicherheitsniveau durch Umsetzung gleichwertiger Maßnahmen (s. Erwägungsgründe 13, 137 d. RL) gewährleistet werden. Hierbei wird auf die Erwägungsgründe der Richtlinie in Nr. 137 der Richtlinie verwiesen, die vorsieht, dass ein hohes Maß an Verantwortung für die Risikomanagementmaßnahmen und die Berichtspflichten im Bereich der Cybersicherheit sicherzustellen ist. Dem soll dadurch Rechnung getragen werden, dass § 37 Abs. 1 BSIG n.F. bestimmt, dass bei einer Ausnahme die Einrichtung gleichwertige Vorgaben zu erfüllen hat. Die Kontrolle über die Einhaltung obläge dem vorschlagenden Ressort.
517		(2) Einrichtungen, die	Umsetzung Art. 2 Abs. 8 S. 1 und 2 NIS-2
518		1. in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung, einschließlich der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten (relevante Bereiche) tätig sind oder Dienste erbringen, oder	
519		2. ausschließlich für Behörden, die Aufgaben in relevanten Bereichen erfüllen, tätig sind oder Dienste erbringen,	
520		können für diese Tätigkeiten oder Dienste von den Risikomanagementmaßnahmen nach § 30 und	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		Meldepflichten nach § 31 befreit werden. Die Informationssicherheit dieser Einrichtungen muss in diesen Fällen anderweitig gewährleistet sein und beaufsichtigt werden.	
521		(3) Einrichtungen, die ausschließlich in den relevanten Bereichen tätig sind oder Dienste erbringen, können insgesamt von den in Absatz 2 genannten Pflichten und von den Registrierungspflichten nach § 32 und § 33 befreit werden. Absatz 2 Satz 2 gilt entsprechend.	Umsetzung Art. 2 Abs. 8 S. 3 NIS-2.
522		(4) Diese Vorschrift gilt nicht, wenn die betreffende Einrichtung als Vertrauensdiensteanbieter auftritt.	Umsetzung Art. 2 Abs. 9 NIS-2
523		(5) Ein Ausnahmebescheid nach diesem Gesetz kann zurückgenommen werden. Ein Vermögensnachteilsausgleich entfällt.	Aufnahme einer Rücknahmeregelung: Das Regelungssystem der §§ 48 ff. VwVfG greift, sofern keine spezialgesetzlichen Regelungen zu Rücknahme oder Widerruf getroffen werden. Für die Rücknahme eines rechtswidrigen Verwaltungsakts, hier der Ausnahmebescheid von den Pflichten nach §§ 30 ff. BSIG könnte auf die subsidiären Regelungen des § 48 VwVfG zurückgegriffen werden. Entscheidend ist jedoch, ob die Befreiung als begünstigender oder nicht begünstigender Verwaltungsakt zu verstehen ist. Bei einem rechtswidrigen nicht begünstigenden Verwaltungsakt greift die problemlose Rücknahme nach § 48 I VwVfG. Gem. § 48 I 2 VwVfG bestimmt die Legaldefinition die Begünstigung wie folgt: Ein Verwaltungsakt ist begünstigend, wenn er ein Recht oder einen rechtlich

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			erheblichen Vorteil begründet oder bestätigt. Ein Recht könnte in der Art begründet sein, als dass die der Befreiung unterliegende Einrichtung entweder ganz oder teilweise den Pflichten der §§ 30 ff. BSIG n.F. nicht nachkommen muss. Andererseits entfallen diese Pflichten nicht einfach - und eine Begünstigung ist nach dem objektiven Regelungsgehalt des Verwaltungsakts unter Berücksichtigung des Zwecks der ihm zugrunde liegenden Norm zu beurteilen - nämlich, dass eine Befreiung von obigen Pflichten nicht der Einrichtung, sondern dem nationalen Sicherheitsinteresse zugutekommen sind und dafür gleichwertige Risikomanagementmaßnahmen zu treffen sind. Aus Gründen der Vorsicht wird hier von ersterem, einem begünstigenden Verwaltungsakt ausgegangen, der bei Rücknahme nach § 48 Absatz 3 VwVfG einen Vermögensnachteilsausgleich nach sich ziehen könnte, sodass ein Ausschluss vorgenommen werden muss.
524		(6) Ein Ausnahmebescheid nach diesem Gesetz ist zu widerrufen, wenn nachträglich Tatsachen eintreten, die zur Ablehnung einer Erteilung einer Ausnahme hätten führen müssen. Abweichend von S.1 kann im Falle eines vorübergehenden Wegfalls der Voraussetzungen des Abs. 2 Nr.1 oder Nr.2 aus besonderen Gründen von einem Widerruf abgesehen werden.	Bedarf zur Regelung des Widerrufs einer rechtmäßigen Befreiung: Für den Widerruf einer rechtmäßigen Befreiung sollte von § 49 VwVfG abgewichen werden, um der spezifischen Interessenlage des § 35 Genüge zu tun. Hier ist der Fall der ursprünglich rechtmäßigen Befreiung, deren Voraussetzungen später entfallen zu regeln. Satz 2 soll der

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			vorübergehenden Änderung der Tatsachenlage Rechnung tragen, sodass die Möglichkeit besteht, an einer Befreiung aus besonderen Gründen bei lediglich vorübergehenden Entfallens der Voraussetzungen festzuhalten (Minimierung Verwaltungsaufwand, Unsicherheit welchen Maßnahmen/Melderegimes die betreffende Einrichtung unterliegt)
525		§ 38 Billigungs- und Überwachungspflicht für Leitungsorgane von Wesentlichen Einrichtungen und Wichtigen Einrichtungen; Schulungen	Umsetzung Art. 20 NIS-2
526		(1) Geschäftsleiter besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind verpflichtet, die von diesen Einrichtungen zur Einhaltung von § 30 ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit zu billigen und ihre Umsetzung zu überwachen. Die Beauftragung eines Dritten zu Erfüllung der Verpflichtungen nach Satz 1 ist nicht zulässig.	Umsetzung Art. 20 Abs. 1 NIS-2
527		(2) Geschäftsleiter, welche ihre Pflichten nach Absatz 1 verletzen, haften der Einrichtung für den entstandenen Schaden. Die Amtshaftung bleibt unberührt.	Umsetzung Art. 20 Abs. 1 Uabs.1 aE. NIS-2. Die NIS-2 gibt eine reine Binnenhaftung im Verhältnis Einrichtung-Geschäftsleiter vor. Vom Schadensbegriff sind sowohl Regressansprüche als auch Bußgeldforderungen umfasst. Umsetzung von Art. 20 Abs. 1 Uabs. 2. Die Vorschriften über die Amtshaftung gehen der Haftungsregel in Satz 1vor, eine Ausweitung der bestehenden

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			Haftung von Amtsträgern erfolgt mithin nicht.
528		(3) Ein Verzicht der Einrichtung auf Ersatzansprüche nach Absatz 2 oder ein Vergleich der Einrichtung über diese Ansprüche ist unwirksam. Dies gilt nicht, wenn der Ersatzpflichtige zahlungsunfähig ist und sich zur Abwendung des Insolvenzverfahrens mit seinen Gläubigern vergleicht oder wenn die Ersatzpflicht in einem Insolvenzplan geregelt wird.	Umsetzung Art. 20 Abs. 1 aE. NIS-2. Die Vorsehung einer zwingenden Norm ist zwar nicht ausdrücklich in der umzusetzenden Richtlinienbestimmung enthalten. Jedoch wird hiermit der bestehende Umsetzungsspielraum unionsrechtskonform ausgeübt. Denn soweit eine Richtlinie den Mitgliedsstaaten keine zwingenden Vorgaben macht, sondern Spielräume für die Umsetzung lässt, sind diese durch die Mitgliedsstaaten eigenständig so auszufüllen, dass die Ziele der Richtlinie vollständig erreicht werden. Diesen Zielen würde es widersprechen, wenn es sich hier um eine disponible Haftung handeln würde.
529		(4) Die Geschäftsleiter von Wesentlichen Einrichtungen und Wichtigen Einrichtungen müssen und deren Mitarbeiter sollen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Risikomanagementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.	Umsetzung Art. 20 Abs. 2 NIS-2.
530	§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen	§ 39 Zusätzliche Anforderungen an Betreiber kritischer Anlagen	Kritische Einrichtungen sind Wesentliche Einrichtungen, daher entfällt das Nachweisregime in dieser Bestimmung. Diese Vorschrift ist Gegenstand der Evaluierung gemäß Art. 6 Abs. 1 Nr. 1 Zweites Gesetz zur Erhöhung der

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			Sicherheit informationstechnischer Systeme vom 18. Mai 2021 (BGBl. I S. 1122). Diese Änderung erfolgt vorbehaltlich der Ergebnisse dieser Evaluierung und wird gegebenenfalls noch auf deren Grundlage angepasst.
531	(1) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens bis zum ersten Werktag, der darauf folgt, dass diese erstmalig oder erneut als Betreiber einer Kritischen Infrastruktur nach der Rechtsverordnung nach § 10 Absatz 1 gelten, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.	(1) Betreiber kritischer Anlagen sind verpflichtet, Systeme zur Angriffserkennung einzusetzen. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. Dabei soll der Stand der Technik eingehalten werden. Der hierfür erforderliche Aufwand soll nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage stehen.	Geringfügig modifiziert, da Absatz 1 Satz 1 ja nicht mehr von technischen und organisatorischen Maßnahmen spricht.
532	(1a) Die Verpflichtung nach Absatz 1 Satz 1, angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst ab dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete		

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Beseitigungsmaßnahmen vorzusehen. Absatz 1 Satz 2 und 3 gilt entsprechend.		
533	(2) Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach den Absätzen 1 und 1a vorschlagen. Das Bundesamt stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach den Absätzen 1 und 1a zu gewährleisten. Die Feststellung erfolgt		
534	1. im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe,		
535	2. im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes.		
536	(3) Betreiber Kritischer Infrastrukturen haben die Erfüllung der Anforderungen nach den Absätzen 1 und 1a spätestens zwei Jahre nach dem in Absatz 1 genannten Zeitpunkt und anschließend alle zwei Jahre dem Bundesamt nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt die Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Das Bundesamt kann die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen. Es kann bei Sicherheitsmängeln im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen.	(2) Betreiber kritischer Analgen nach haben die Erfüllung der Anforderungen nach Absatz 1 als zusätzlichen Teil des Nachweises gemäß § 34 dem Bundesamt geeignet nachzuweisen. Betreiber, die gemäß [*§ [●] KRITIS-Dachgesetz*] zum Nachweis der Erfüllung von Anforderungen gegenüber dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe verpflichtet sind, können die in Satz 1 sowie in § 34 Absatz 1 genannten Nachweis zum in [*§ [●] KRITIS-Dachgesetz*] genannten Zeitpunkt einreichen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Einrichtungen übermitteln dem Bundesamt die Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Das Bundesamt kann die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen. Es kann bei Sicherheitsmängeln im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen.	
537	(4) Das Bundesamt kann beim Betreiber Kritischer Infrastrukturen die Einhaltung der Anforderungen nach den Absätzen 1 und 1a überprüfen; es kann sich bei der Durchführung der Überprüfung eines qualifizierten unabhängigen Dritten bedienen. Der Betreiber Kritischer Infrastrukturen hat dem Bundesamt und den in dessen Auftrag handelnden Personen zum Zweck der Überprüfung das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten und auf Verlangen die in Betracht kommenden Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorzulegen, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren. Für die Überprüfung erhebt das Bundesamt Gebühren und Auslagen bei dem jeweiligen Betreiber Kritischer Infrastrukturen nur, sofern das Bundesamt auf Grund von Anhaltspunkten tätig geworden ist, die berechtigte Zweifel an der Einhaltung der Anforderungen nach den Absätzen 1 und 1a begründeten.	(3) Das Bundesamt kann bei Betreibern kritischer Anlagen die Einhaltung der Anforderungen nach dem Absatz 1 überprüfen; es kann sich bei der Durchführung der Überprüfung eines qualifizierten unabhängigen Dritten bedienen. Der Betreiber kritischer Anlagenhat dem Bundesamt und den in dessen Auftrag handelnden Personen zum Zweck der Überprüfung das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten und auf Verlangen die in Betracht kommenden Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorzulegen, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren. Für die Überprüfung erhebt das Bundesamt Gebühren und Auslagen bei dem jeweiligen Betreiber Kritischer Infrastrukturen nur, sofern das Bundesamt auf Grund von Anhaltspunkten tätig geworden ist, die berechtigte Zweifel an der Einhaltung der Anforderungen nach dem Absatz 1 begründeten.	Redaktionelle Änderungen der Absatzzahl und Binnenverweise sowie Umbenennung Einrichtungskategorie
538	(5) Das Bundesamt kann zur Ausgestaltung des Verfahrens der Sicherheitsaudits, Prüfungen und Zertifizierungen nach Absatz 3 Anforderungen an die Art und Weise der Durchführung, an die hierüber auszustellenden Nachweise sowie fachliche und organisatorische Anforderungen an die prüfende Stelle nach Anhörung von Vertretern der betroffenen Betreiber und der betroffenen Wirtschaftsverbände festlegen.	(5) Das Bundesamt kann zur Ausgestaltung des Verfahrens der Sicherheitsaudits, Prüfungen und Zertifizierungen nach Absatz 2 Anforderungen an die Art und Weise der Durchführung, an die hierüber auszustellenden Nachweise sowie fachliche und organisatorische Anforderungen an die Prüfer und die prüfende Stelle nach Anhörung von Vertretern der betroffenen Betreiber und der betroffenen Wirtschaftsverbände festlegen.	Redaktionelle Änderungen der Absatzzahl und Binnenverweise.
539	§ 8b Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen	§ 40 Zentrale Melde- und Anlaufstelle	Umsetzung Art. 8 Abs. 3-5 NIS-2 Diese Vorschrift (§ 8b BSIG aF.) ist Gegenstand der Evaluierung gemäß Art. 6 Abs. 1 Nr. 1 Zweites Gesetz zur Erhöhung der Sicherheit

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			informationstechnischer Systeme vom 18. Mai 2021 (BGBl. I S. 1122). Diese Änderung erfolgt vorbehaltlich der Ergebnisse dieser Evaluierung und wird gegebenenfalls noch auf deren Grundlage angepasst.
540	(1) Das Bundesamt ist die zentrale Meldestelle für Betreiber Kritischer Infrastrukturen in Angelegenheiten der Sicherheit in der Informationstechnik.	(1) Das Bundesamt ist die zentrale Meldestelle für Betreiber kritischer Anlagen, wichtige Einrichtungen und besonders wichtige Einrichtungen in Angelegenheiten der Sicherheit in der Informationstechnik und zentrale Anlaufstelle für die Aufsicht über Betreiber kritischer Anlagen, besonders wichtige Einrichtungen und wichtige Einrichtungen und fungiert dabei als nationale Verbindungsstelle um:	
541		1. die grenzüberschreitende Zusammenarbeit von Behörden der Länder, die diese als zuständige Behörde für die Aufsicht von Einrichtungen der öffentlichen Verwaltung auf regionaler Ebene im Sinne des Artikels 2 Absatz 2 lit. f (ii) der NIS-2-Richtlinie bestimmt haben, Bundesnetzagentur und Bundesanstalt für Finanzdienstleistungsaufsicht mit den für die Überwachung der Anwendung der NIS-2-Richtlinie zuständigen Behörden anderer Mitgliedstaaten und gegebenenfalls mit der Europäischen Kommission und der ENISA	Umsetzung Art. 8 Abs. 3-5 NIS-2
542		2. sowie die sektorübergreifende Zusammenarbeit mit in Nummer 1 genannten Behörden der Länder, , Bundesnetzagentur und Bundesanstalt für Finanzdienstleistungsaufsicht	Umsetzung Art. 8 Abs. 3-5 NIS-2
543		zu gewährleisten.	Umsetzung Art. 8 Abs. 3-5 NIS-2

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
544	(2) Das Bundesamt hat zur Wahrnehmung dieser Aufgabe	(2) Das Bundesamt hat zur Wahrnehmung dieser Aufgabe	
545	1. die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik wesentlichen Informationen zu sammeln und auszuwerten, insbesondere Informationen zu Sicherheitslücken, zu Schadprogrammen, zu erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und zu der dabei beobachteten Vorgehensweise,	1. die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik wesentlichen Informationen zu sammeln und auszuwerten, insbesondere Informationen zu Schwachstellen, zu Schadprogrammen, zu erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und zu der dabei beobachteten Vorgehensweise,	
546	2. deren potentielle Auswirkungen auf die Verfügbarkeit der Kritischen Infrastrukturen in Zusammenarbeit mit den zuständigen Aufsichtsbehörden und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe zu analysieren,	2. deren potentielle Auswirkungen auf die Verfügbarkeit der Kritischen Infrastrukturen in Zusammenarbeit mit den zuständigen Aufsichtsbehörden und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe zu analysieren,	
547	3. das Lagebild bezüglich der Sicherheit in der Informationstechnik der Kritischen Infrastrukturen oder der Unternehmen im besonderen öffentlichen Interesse kontinuierlich zu aktualisieren und	3. das Lagebild bezüglich der Sicherheit in der Informationstechnik der Kritischen Infrastrukturen oder der Unternehmen im besonderen öffentlichen Interesse kontinuierlich zu aktualisieren und	
548	4. unverzüglich	4. unverzüglich	
549	a) die Betreiber Kritischer Infrastrukturen und die Unternehmen im besonderen öffentlichen Interesse über sie betreffende Informationen nach den Nummern 1 bis 3,	a) die Betreiber kritischer Anlagen, besonders wichtigen Einrichtungen und wichtigen Einrichtungen über sie betreffende Informationen nach den Nummern 1 bis 3 durch Übermittlung an die Kontaktdaten nach § 32 Absatz 2 Nummer 2 sowie,	Anpassung an neue Einrichtungskategorien, Verschiebung von Abs. 3 S. 5.
550	b) die zuständigen Aufsichtsbehörden und die sonst zuständigen Behörden des Bundes über die zur Erfüllung		Entfällt. Aufgrund der hohen Sicherheitsrelevanz der Angaben Wesentlicher Einrichtungen, die auch

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	ihrer Aufgaben erforderlichen Informationen nach den Nummern 1 bis 3,		Kritische Einrichtungen miteinschließt, ist eine restriktivere Behandlung angezeigt. Neuregelung in Nr. 5 unten.
551	c) die zuständigen Aufsichtsbehörden der Länder oder die zu diesem Zweck dem Bundesamt von den Ländern als zentrale Kontaktstellen benannten Behörden über die zur Erfüllung ihrer Aufgaben erforderlichen Informationen nach den Nummern 1 bis 3 sowie		s.o.
552	d) die zuständigen Behörden eines anderen Mitgliedstaats der Europäischen Union über nach Absatz 4 oder nach vergleichbaren Regelungen gemeldete erhebliche Störungen, die Auswirkungen in diesem Mitgliedstaat haben,	b) die zuständigen Behörden eines anderen Mitgliedstaats der Europäischen Union über nach Absatz 4 oder nach vergleichbaren Regelungen gemeldete erhebliche Störungen, die Auswirkungen in diesem Mitgliedstaat haben,	Anpassung Nummerierung.
553		5. soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist, im Rahmen vorab abgestimmter Prozesse zur Weitergabe und Wahrung der notwendigen Vertraulichkeit den zuständigen Aufsichtsbehörden und sonst zuständigen Behörden des Bundes Informationen zu Betreibern kritischer Anlagen und in begründeten Fällen zu einer einzelnen kritischen Anlage Informationen nach den Nummern 1 bis 3 zur Verfügung zu stellen.	Aufgrund der hohen Sicherheitsrelevanz der Angaben von Betreibern kritischer Anlagen, ist eine restriktivere Behandlung angezeigt
554	zu unterrichten.	zu unterrichten.	
555		(3) Das Bundesamt hat zur Wahrnehmung seiner Aufgabe als zentrale Anlaufstelle	Umsetzung Art. 8 Abs. 3-5 NIS-2

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
556		1. Anfragen von den in Absatz 1 genannten Stellen anzunehmen oder soweit zutreffend an eine oder mehrere in Absatz 1 genannten Stellen weiterzuleiten,	Umsetzung Art. 8 Abs. 3-5 NIS-2
557		2. Antworten auf die in Absatz 2 Nr. 2 genannten Anfragen zu erstellen und dabei soweit zutreffend die in Absatz 1 genannten Stellen zu beteiligen oder Antworten der in Absatz 1 genannten Stellen an die in Absatz 1 genannten Stellen weiterzuleiten,	Umsetzung Art. 8 Abs. 3-5 NIS-2
558		3. auf eigenes Betreiben nach § 31 eingegangene Meldungen an zentrale Anlaufstellen der anderen betroffenen Mitgliedstaaten der Europäischen Union weiterzuleiten,	Umsetzung Art. 23 Abs. 8 NIS-2
559		4. gegebenenfalls und insbesondere, wenn der erhebliche Sicherheitsvorfall zwei oder mehr Mitgliedstaaten der Europäischen Union betrifft, die anderen betroffenen Mitgliedstaaten und die ENISA über den erheblichen Sicherheitsvorfall zu unterrichten, wobei diese Informationen umfassen die Art der gemäß § 31 Absatz 2 erhaltenen Informationen und das Bundesamt dabei das wirtschaftliche Interesse der Einrichtung sowie die Vertraulichkeit der bereitgestellten Informationen wahrt.	Umsetzung Art. 23 Abs. 6 NIS-2
560	(3) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens bis zum ersten Werktag, der darauf folgt, dass diese erstmalig oder erneut als Betreiber einer Kritischen Infrastruktur nach der Rechtsverordnung nach § 10 Absatz 1 gelten, die von ihnen betriebenen Kritischen Infrastrukturen beim		Verschoben in § 32 Abs. 3 nF.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Bundesamt zu registrieren und eine Kontaktstelle zu benennen. Die Registrierung eines Betreibers einer Kritischen Infrastruktur kann das Bundesamt auch selbst vornehmen, wenn der Betreiber seine Pflicht zur Registrierung nicht erfüllt. Nimmt das Bundesamt eine solche Registrierung selbst vor, informiert es die zuständige Aufsichtsbehörde des Bundes darüber. Die Betreiber haben sicherzustellen, dass sie über die benannte oder durch das Bundesamt festgelegte Kontaktstelle jederzeit erreichbar sind. Die Übermittlung von Informationen durch das Bundesamt nach Absatz 2 Nummer 4 erfolgt an diese Kontaktstelle.		
561	(3a) Rechtfertigen Tatsachen die Annahme, dass ein Betreiber seine Pflicht zur Registrierung nach Absatz 3 nicht erfüllt, so hat der Betreiber dem Bundesamt auf Verlangen die für die Bewertung aus Sicht des Bundesamtes erforderlichen Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorzulegen und Auskunft zu erteilen, soweit nicht Geheimschutzinteressen oder überwiegende Sicherheitsinteressen entgegenstehen.		Verschoben in § 32 Abs. 4 nF.
562	(4) Betreiber Kritischer Infrastrukturen haben die folgenden Störungen unverzüglich über die Kontaktstelle an das Bundesamt zu melden:		Entfällt aufgrund des neuen Melderegimes nach § 31 nF.
563	1. Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen geführt haben,		
564	2. erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit		

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können.		
565	Die Meldung muss Angaben zu der Störung, zu möglichen grenzübergreifenden Auswirkungen sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik, der Art der betroffenen Einrichtung oder Anlage sowie zur erbrachten kritischen Dienstleistung und zu den Auswirkungen der Störung auf diese Dienstleistung enthalten. Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat.		Entfällt. Betreiber kritischer Anlagen müssen zukünftig stets ihren Namen nennen. Die Vorschrift wurde in der heutigen Praxis kaum genutzt.
566	(4a) Während einer erheblichen Störung gemäß Absatz 4 Satz 1 Nummer 2, § 8f Absatz 7 Satz 1 Nummer 2 oder Absatz 8 Satz 1 Nummer 2 kann das Bundesamt im Einvernehmen mit der jeweils zuständigen Aufsichtsbehörde des Bundes von den betroffenen Betreibern Kritischer Infrastrukturen oder den Unternehmen im besonderen öffentlichen Interesse die Herausgabe der zur Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten verlangen. Betreiber Kritischer Infrastrukturen und Unternehmen im besonderen öffentlichen Interesse sind befugt, dem Bundesamt auf Verlangen die zur Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten zu übermitteln, soweit dies zur Bewältigung einer erheblichen Störung gemäß	(4a) Während einer erheblichen Störung gemäß Absatz 4 Satz 1 Nummer 2, kann das Bundesamt im Einvernehmen mit der jeweils zuständigen Aufsichtsbehörde des Bundes von den betroffenen Betreibern kritischer Anlagen die Herausgabe der zur Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten verlangen. Betreiber kritischer Anlagen sind befugt, dem Bundesamt auf Verlangen die zur Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten zu übermitteln, soweit dies zur Bewältigung einer erheblichen Störung gemäß Absatz 4 Satz 1 Nummer 2,erforderlich ist.	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Absatz 4 Satz 1 Nummer 2, § 8f Absatz 7 Satz 1 Nummer 2 oder Absatz 8 Satz 1 Nummer 2 erforderlich ist.		
567	(5) Zusätzlich zu ihrer Kontaktstelle nach Absatz 3 können Betreiber Kritischer Infrastrukturen, die dem gleichen Sektor angehören, eine gemeinsame übergeordnete Ansprechstelle benennen. Wurde eine solche benannt, erfolgt der Informationsaustausch zwischen den Kontaktstellen und dem Bundesamt in der Regel über die gemeinsame Ansprechstelle.		Entfällt. Die Vorschrift hatte keine ersichtliche praktische Relevanz - überwiegend stehen hinter den GÜAS nur Einzelbetreiber. Kaum tatsächliche Nutzung (< 1%) durch die Wirtschaft und führt zu Verzögerungen in den Kommunikationswegen sowie Zusatzaufwand / Sonderfall bei Betreibermanagement.
568	(6) Soweit erforderlich kann das Bundesamt vom Hersteller der betroffenen informationstechnischen Produkte und Systeme die Mitwirkung an der Beseitigung oder Vermeidung einer Störung nach Absatz 4, oder § 8f Absatz 7 oder 8 verlangen. Satz 1 gilt für Störungen bei Betreibern und Genehmigungsinhabern im Sinne von § 8d Absatz 3 entsprechend.		Verschoben nach § 18 nF.
569	(7) Soweit im Rahmen dieser Vorschrift personenbezogene Daten verarbeitet werden, ist eine über die vorstehenden Absätze hinausgehende Verarbeitung zu anderen Zwecken unzulässig. § 5 Absatz 7 Satz 3 bis 8 ist entsprechend anzuwenden.	(7) Soweit im Rahmen dieser Vorschrift personenbezogene Daten verarbeitet werden, ist eine über die vorstehenden Absätze hinausgehende Verarbeitung zu anderen Zwecken unzulässig. § 8 Absatz 7 Satz 3 bis 8 ist entsprechend anzuwenden.	
570	§ 8c Besondere Anforderungen an Anbieter digitaler Dienste		Entfällt. Die Kategorie „Anbieter digitale Dienste“ geht in die neuen Einrichtungskategorien auf.
571	(1) Anbieter digitaler Dienste haben geeignete und verhältnismäßige technische und organisatorische Maßnahmen zu treffen, um Risiken für die Sicherheit der Netz- und Informationssysteme, die sie zur Bereitstellung der digitalen Dienste innerhalb der		s.o.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Europäischen Union nutzen, zu bewältigen. Sie haben Maßnahmen zu treffen, um den Auswirkungen von Sicherheitsvorfällen auf innerhalb der Europäischen Union erbrachte digitale Dienste vorzubeugen oder die Auswirkungen so gering wie möglich zu halten.		
572	(2) Maßnahmen zur Bewältigung von Risiken für die Sicherheit der Netz- und Informationssysteme nach Absatz 1 Satz 1 müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist. Dabei ist folgenden Aspekten Rechnung zu tragen:		s.o.
573	1. der Sicherheit der Systeme und Anlagen,		s.o.
574	2. der Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen,		s.o.
575	3. dem Betriebskontinuitätsmanagement,		s.o.
576	4. der Überwachung, Überprüfung und Erprobung,		s.o.
577	5. der Einhaltung internationaler Normen.		s.o.
578	Die notwendigen Maßnahmen werden durch Durchführungsrechtsakte der Kommission nach Artikel 16 Absatz 8 der Richtlinie (EU) 2016/1148 näher bestimmt.		s.o.
579	(3) Anbieter digitaler Dienste haben jeden Sicherheitsvorfall, der erhebliche Auswirkungen auf die Bereitstellung eines von ihnen innerhalb der Europäischen Union erbrachten digitalen Dienstes hat, unverzüglich dem Bundesamt zu melden. Die Voraussetzungen, nach denen Auswirkungen eines Sicherheitsvorfalls erheblich sind, werden durch Durchführungsakte der Kommission nach Artikel 16		s.o.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Absatz 8 der Richtlinie (EU) 2016/1148 unter Berücksichtigung insbesondere der folgenden Parameter näher bestimmt:		
580	1. die Zahl der von dem Sicherheitsvorfall betroffenen Nutzer, insbesondere der Nutzer, die den Dienst für die Bereitstellung ihrer eigenen Dienste benötigen,		s.o.
581	2. die Dauer des Sicherheitsvorfalls,		s.o.
582	3. das von dem Sicherheitsvorfall betroffene geographische Gebiet,		s.o.
583	4. das Ausmaß der Unterbrechung der Bereitstellung des Dienstes,		s.o.
584	5. das Ausmaß der Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten.		s.o.
585	Die Pflicht zur Meldung eines Sicherheitsvorfalls entfällt, wenn der Anbieter keinen ausreichenden Zugang zu den Informationen hat, die erforderlich sind, um die Auswirkung eines Sicherheitsvorfalls gemessen an den Parametern nach Satz 2 zu bewerten. Für den Inhalt der Meldungen gilt § 8b Absatz 4 entsprechend, soweit nicht Durchführungsakte der Kommission nach Artikel 16 Absatz 9 der Richtlinie (EU) 2016/1148 etwas anderes bestimmen. Über nach Satz 1 gemeldete Sicherheitsvorfälle, die Auswirkungen in einem anderen Mitgliedstaat der Europäischen Union haben, hat das Bundesamt die zuständige Behörde dieses Mitgliedstaats zu unterrichten.		s.o.
586	(4) Liegen Anhaltspunkte dafür vor, dass ein Anbieter digitaler Dienste die Anforderungen des Absatzes 1 in Verbindung mit den		s.o.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Durchführungsrechtsakten der Kommission nach Artikel 16 Absatz 8 der Richtlinie (EU) 2016/1148 und des Absatzes 2 in Verbindung mit den Durchführungsrechtsakten der Kommission nach Artikel 16 Absatz 9 der Richtlinie (EU) 2016/1148 nicht erfüllt, kann das Bundesamt von dem Anbieter digitaler Dienste folgende Maßnahmen verlangen:		
587	1. die Übermittlung der zur Beurteilung der Sicherheit seiner Netz- und Informationssysteme erforderlichen Informationen, einschließlich Nachweisen über ergriffene Sicherheitsmaßnahmen,		s.o.
588	2. die Beseitigung von Mängeln bei der Erfüllung der in den Absätzen 1 und 2 bestimmten Anforderungen.		s.o.
589	Die Anhaltspunkte können sich auch aus Feststellungen ergeben, die dem Bundesamt von den zuständigen Behörden eines anderen Mitgliedstaats der Europäischen Union vorgelegt werden.		s.o.
590	(5) Hat ein Anbieter digitaler Dienste seine Hauptniederlassung, einen Vertreter oder Netz- und Informationssysteme in einem anderen Mitgliedstaat der Europäischen Union, so arbeitet das Bundesamt bei der Erfüllung der Aufgaben nach Absatz 4 mit der zuständigen Behörde dieses Mitgliedstaats zusammen. Diese Zusammenarbeit kann das Ersuchen umfassen, die Maßnahmen in Absatz 4 Satz 1 Nummer 1 und 2 zu ergreifen.		s.o.
591	*§ 9b* *Untersagung des Einsatzes kritischer Komponenten*	§ 41 Untersagung des Einsatzes kritischer Komponenten	Verschiebung von § 9b aF.
592	*(1) Der Betreiber einer Kritischen Infrastruktur hat den geplanten erstmaligen Einsatz einer kritischen*	(1) Ein Betreiber kritischer Anlagen hat den geplanten erstmaligen Einsatz einer kritischen Komponente	Anpassung Bezeichnung neue Einrichtungskategorie; redaktionelle

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Komponente gemäß § 2 Absatz 13 dem Bundesministerium des Innern, für Bau und Heimat vor ihrem Einsatz anzuzeigen. In der Anzeige sind die kritische Komponente und die geplante Art ihres Einsatzes anzugeben. Satz 1 gilt für einen Betreiber einer Kritischen Infrastruktur nicht, wenn dieser den Einsatz einer anderen kritischen Komponente desselben Typs für dieselbe Art des Einsatzes bereits nach Satz 1 angezeigt hat und ihm dieser nicht untersagt wurde.	gemäß § 2 Absatz 1 Nummer 26 dem Bundesministerium des Innern und für Heimat vor ihrem Einsatz anzuzeigen. In der Anzeige sind die kritische Komponente und die geplante Art ihres Einsatzes anzugeben. Satz 1 gilt für einen Betreiber kritischer Anlagen nicht, wenn dieser den Einsatz einer anderen kritischen Komponente desselben Typs für dieselbe Art des Einsatzes bereits nach Satz 1 angezeigt hat und ihm dieser nicht untersagt wurde.	Änderungen und Anpassung des Verweises.
593	*(2) Das Bundesministerium des Innern, für Bau und Heimat kann den geplanten erstmaligen Einsatz einer kritischen Komponente gegenüber dem Betreiber der Kritischen Infrastruktur im Benehmen mit den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt bis zum Ablauf von zwei Monaten nach Eingang der Anzeige nach Absatz 1 untersagen oder Anordnungen erlassen, wenn der Einsatz die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt. Bei der Prüfung einer voraussichtlichen Beeinträchtigung der öffentlichen Ordnung oder Sicherheit kann insbesondere berücksichtigt werden, ob*	(2) Das Bundesministerium des Innern und für Heimat kann den geplanten erstmaligen Einsatz einer kritischen Komponente gegenüber dem Betreiber kritischer Anlagen im Benehmen mit den in § 57 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt bis zum Ablauf von zwei Monaten nach Eingang der Anzeige nach Absatz 1 untersagen oder Anordnungen erlassen, wenn der Einsatz die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt. Bei der Prüfung einer voraussichtlichen Beeinträchtigung der öffentlichen Ordnung oder Sicherheit kann insbesondere berücksichtigt werden, ob	s.o.
594	*1. der Hersteller unmittelbar oder mittelbar von der Regierung, einschließlich sonstiger staatlicher Stellen oder Streitkräfte, eines Drittstaates kontrolliert wird,*	1. der Hersteller unmittelbar oder mittelbar von der Regierung, einschließlich sonstiger staatlicher Stellen oder Streitkräfte, eines Drittstaates kontrolliert wird,	(unverändert)
595	*2. der Hersteller bereits an Aktivitäten beteiligt war oder ist, die nachteilige Auswirkungen auf die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland oder eines anderen Mitgliedstaates der Europäischen Union, der Europäischen Freihandelsassoziation*	2 der Hersteller bereits an Aktivitäten beteiligt war oder ist, die nachteilige Auswirkungen auf die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland oder eines anderen Mitgliedstaates der Europäischen Union, der Europäischen Freihandelsassoziation	(unverändert)

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	oder des Nordatlantikvertrages oder auf deren Einrichtungen hatten, oder	oder des Nordatlantikvertrages oder auf deren Einrichtungen hatten, oder	
596	*3. der Einsatz der kritischen Komponente im Einklang mit den sicherheitspolitischen Zielen der Bundesrepublik Deutschland, der Europäischen Union oder des Nordatlantikvertrages steht.*	3. der Einsatz der kritischen Komponente im Einklang mit den sicherheitspolitischen Zielen der Bundesrepublik Deutschland, der Europäischen Union oder des Nordatlantikvertrages steht.	(unverändert)
597	*Vor Ablauf der Frist von zwei Monaten nach Anzeige nach Absatz 1 ist der Einsatz nicht gestattet. Das Bundesministerium des Innern, für Bau und Heimat kann die Frist gegenüber dem Betreiber um weitere zwei Monate verlängern, wenn die Prüfung besondere Schwierigkeiten tatsächlicher oder rechtlicher Art aufweist.*	Vor Ablauf der Frist von zwei Monaten nach Anzeige nach Absatz 1 ist der Einsatz nicht gestattet. Das Bundesministerium des Innern und für Heimat kann die Frist gegenüber der Einrichtung um weitere zwei Monate verlängern, wenn die Prüfung besondere Schwierigkeiten tatsächlicher oder rechtlicher Art aufweist.	Redaktionelle Änderungen
598	*(3) Kritische Komponenten gemäß § 2 Absatz 13 dürfen nur eingesetzt werden, wenn der Hersteller eine Erklärung über seine Vertrauenswürdigkeit (Garantieerklärung) gegenüber dem Betreiber der Kritischen Infrastruktur abgeben hat. Die Garantieerklärung ist der Anzeige nach Absatz 1 beizufügen. Aus der Garantieerklärung muss hervorgehen, wie der Hersteller sicherstellt, dass die kritische Komponente nicht über technische Eigenschaften verfügt, die spezifisch geeignet sind, missbräuchlich, insbesondere zum Zwecke von Sabotage, Spionage oder Terrorismus auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können. Das Bundesministerium des Innern, für Bau und Heimat legt die Einzelheiten der Mindestanforderungen an die Garantieerklärung im Einvernehmen mit den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt durch Allgemeinverfügung fest, die im Bundesanzeiger bekannt zu machen ist. Die Einzelheiten der Mindestanforderungen an die*	(3) Kritische Komponenten gemäß § 2 Absatz 1 Nummer 26 dürfen nur eingesetzt werden, wenn der Hersteller eine Erklärung über seine Vertrauenswürdigkeit (Garantieerklärung) gegenüber der Kritischen Einrichtung abgeben hat. Die Garantieerklärung ist der Anzeige nach Absatz 1 beizufügen. Aus der Garantieerklärung muss hervorgehen, wie der Hersteller sicherstellt, dass die kritische Komponente nicht über technische Eigenschaften verfügt, die spezifisch geeignet sind, missbräuchlich, insbesondere zum Zwecke von Sabotage, Spionage oder Terrorismus auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können. Das Bundesministerium des Innern und für Heimat legt die Einzelheiten der Mindestanforderungen an die Garantieerklärung im Einvernehmen mit den in § 57 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt durch Allgemeinverfügung fest, die im Bundesanzeiger bekannt zu machen ist. Die Einzelheiten der Mindestanforderungen an die	Redaktionelle Änderungen

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Garantieerklärung müssen aus den Schutzzielen der Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur folgen und die Vermeidung von Gefahren für die öffentliche Sicherheit und Ordnung, insbesondere im Sinne von Absatz 2 Satz 2, adressieren, die aus der Sphäre des Herstellers der kritischen Komponente, insbesondere dessen Organisationsstruktur, stammen. Die Sätze 1 und 2 gelten erst ab der Bekanntmachung der Allgemeinverfügung nach Satz 5 und nicht für bereits vor diesem Zeitpunkt eingesetzte kritische Komponenten. Soweit Änderungen der Allgemeinverfügung erfolgen, sind diese für bereits nach diesem Absatz abgegebene Garantieerklärungen unbeachtlich.	Garantieerklärung müssen aus den Schutzzielen der Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur folgen und die Vermeidung von Gefahren für die öffentliche Sicherheit und Ordnung, insbesondere im Sinne von Absatz 2 Satz 2, adressieren, die aus der Sphäre des Herstellers der kritischen Komponente, insbesondere dessen Organisationsstruktur, stammen. Die Sätze 1 und 2 gelten erst ab der Bekanntmachung der Allgemeinverfügung nach Satz 5 und nicht für bereits vor diesem Zeitpunkt eingesetzte kritische Komponenten. Soweit Änderungen der Allgemeinverfügung erfolgen, sind diese für bereits nach diesem Absatz abgegebene Garantieerklärungen unbeachtlich.	
599	*(4) Das Bundesministerium des Innern, für Bau und Heimat kann den weiteren Einsatz einer kritischen Komponente gegenüber dem Betreiber der Kritischen Infrastruktur im Einvernehmen mit den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt untersagen oder Anordnungen erlassen, wenn der weitere Einsatz die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt, insbesondere, wenn der Hersteller der kritischen Komponente nicht vertrauenswürdig ist. Absatz 2 Satz 2 gilt entsprechend.*	(4) Das Bundesministerium des Innern und für Heimat kann den weiteren Einsatz einer kritischen Komponente gegenüber dem Betreiber kritischer Anlagen im Einvernehmen mit den in § 57 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt untersagen oder Anordnungen erlassen, wenn der weitere Einsatz die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt, insbesondere, wenn der Hersteller der kritischen Komponente nicht vertrauenswürdig ist. Absatz 2 Satz 2 gilt entsprechend.	Redaktionelle Änderungen, Anpassung des Verweises.
600	*(5) Ein Hersteller einer kritischen Komponente kann insbesondere dann nicht vertrauenswürdig sein, wenn hinreichende Anhaltspunkte dafür bestehen, dass*	(5) Ein Hersteller einer kritischen Komponente kann insbesondere dann nicht vertrauenswürdig sein, wenn hinreichende Anhaltspunkte dafür bestehen, dass	(unverändert)
601	*1. er gegen die in der Garantieerklärung eingegangen Verpflichtungen verstoßen hat,*	1. er gegen die in der Garantieerklärung eingegangen Verpflichtungen verstoßen hat,	(unverändert)

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
602	*2. in der Garantieerklärung angegebene Tatsachenbehauptungen unwahr sind,*	2. in der Garantieerklärung angegebene Tatsachenbehauptungen unwahr sind,	(unverändert)
603	*3. er Sicherheitsüberprüfungen und Penetrationsanalysen an seinem Produkt und in der Produktionsumgebung nicht im erforderlichen Umfang in angemessener Weise unterstützt,*	3. er Sicherheitsüberprüfungen und Penetrationsanalysen an seinem Produkt und in der Produktionsumgebung nicht im erforderlichen Umfang in angemessener Weise unterstützt,	(unverändert)
604	*4. Schwachstellen oder Manipulationen nicht unverzüglich, nachdem er davon Kenntnis erlangt, beseitigt und dem Betreiber der Kritischen Infrastruktur meldet,*	4. Schwachstellen oder Manipulationen nicht unverzüglich, nachdem er davon Kenntnis erlangt, beseitigt und der Kritischen Einrichtung meldet,	(unverändert)
605	*5. die kritische Komponente auf Grund von Mängeln ein erhöhtes Gefährdungspotenzial aufweist oder aufgewiesen hat, missbräuchlich auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können oder*	5. die kritische Komponente auf Grund von Mängeln ein erhöhtes Gefährdungspotenzial aufweist oder aufgewiesen hat, missbräuchlich auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können oder	(unverändert)
606	*6. die kritische Komponente über technische Eigenschaften verfügt oder verfügt hat, die spezifisch geeignet sind oder waren, missbräuchlich auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können.*	6. die kritische Komponente über technische Eigenschaften verfügt oder verfügt hat, die spezifisch geeignet sind oder waren, missbräuchlich auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können.	(unverändert)
607	*(6) Wurde nach Absatz 4 der weitere Einsatz einer kritischen Komponente untersagt, kann das Bundesministerium des Innern, für Bau und Heimat im Einvernehmen mit den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt*	(6) Wurde nach Absatz 4 der weitere Einsatz einer kritischen Komponente untersagt, kann das Bundesministerium des Innern und für Heimat im Einvernehmen mit den in § 53 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt	Redaktionelle Änderungen, Anpassung des Verweises.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
608	*1. den geplanten Einsatz weiterer kritischer Komponenten desselben Typs und desselben Herstellers untersagen und*	1. den geplanten Einsatz weiterer kritischer Komponenten desselben Typs und desselben Herstellers untersagen und	(unverändert)
609	*2. den weiteren Einsatz kritischer Komponenten desselben Typs und desselben Herstellers unter Einräumung einer angemessenen Frist untersagen.*	2. den weiteren Einsatz kritischer Komponenten desselben Typs und desselben Herstellers unter Einräumung einer angemessenen Frist untersagen.	(unverändert)
610	*(7) Bei schwerwiegenden Fällen nicht vorliegender Vertrauenswürdigkeit nach Absatz 5 kann das Bundesministerium des Innern, für Bau und Heimat den Einsatz aller kritischen Komponenten des Herstellers im Einvernehmen mit den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt untersagen.*	(7) Bei schwerwiegenden Fällen nicht vorliegender Vertrauenswürdigkeit nach Absatz 5 kann das Bundesministerium des Innern und für Heimat den Einsatz aller kritischen Komponenten des Herstellers im Einvernehmen mit den in § 57 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt untersagen.	Redaktionelle Änderungen, Anpassung des Verweises.
611	§ 8d Anwendungsbereich		Teilweise verschoben, teilweise entfallen. Siehe nachstehende Begründungen. [*Anm. BMI CI 1 – Diese Vorschrift (§ 8d BSIG aF.) ist Gegenstand der Evaluierung gemäß Art. 6 Abs. 1 Nr. 1 Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 18. Mai 2021 (BGBl. I S. 1122). Diese Änderung erfolgt vorbehaltlich der Ergebnisse dieser Evaluierung und wird gegebenenfalls noch auf deren Grundlage angepasst.*]
612	(1) Die §§ 8a und 8b sind nicht anzuwenden auf Kleinstunternehmen im Sinne der Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36). Artikel 3 Absatz 4 des Anhangs der Empfehlung ist nicht anzuwenden.		In Umsetzung von Art. 2 Abs. 2 lit. b-e NIS-2 entfällt eine Mindestunternehmensgröße bei Betreibern kritischer Anlagen.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
613	(1a) § 8f ist nicht anzuwenden auf Kleinstunternehmen und kleine Unternehmen im Sinne der Empfehlung 2003/361/EG. Artikel 3 Absatz 4 des Anhangs zu der Empfehlung ist nicht anzuwenden.		Entfällt in Folge der Streichung von § 8f aF.
614	(2) § 8a ist nicht anzuwenden auf		Teilweise verschoben, teilweise entfallen. Siehe nachstehende Begründungen.
615	1. Betreiber Kritischer Infrastrukturen, soweit sie ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen,		Verschoben nach § 28 Abs. 2 Nr. 1 nF.
616	2. Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 3 des Gesetzes vom 17. Juli 2015 (BGBl. I S. 1324) geändert worden ist, in der jeweils geltenden Fassung, soweit sie den Regelungen des § 11 des Energiewirtschaftsgesetzes unterliegen,		Entfällt. Die Unternehmen sind zukünftig im Anwendungsbereich des BSIG nF.
617	3. die Gesellschaft für Telematik nach § 306 Absatz 1 Satz 3 des Fünften Buches Sozialgesetzbuch, Betreiber von Diensten der Telematikinfrastruktur im Hinblick auf die nach § 311 Absatz 6 und § 325 des Fünften Buches Sozialgesetzbuch zugelassenen Dienste und Betreiber von Diensten, soweit sie die Telematikinfrastruktur für nach § 327 Absatz 2 bis 5 des Fünften Buches Sozialgesetzbuch bestätigte Anwendungen nutzen,		Verschoben nach § 28 Abs. 2 Nr. 2 nF.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
618	4. Genehmigungsinhaber nach § 7 Absatz 1 des Atomgesetzes in der Fassung der Bekanntmachung vom 15. Juli 1985 (BGBl. I S. 1565), das zuletzt durch Artikel 2 des Gesetzes vom 17. Juli 2015 (BGBl. I S. 1324) geändert worden ist, in der jeweils geltenden Fassung für den Geltungsbereich der Genehmigung sowie		Entfällt. Die Regelung erübrigt sich mit dem am 1. April 2023 zu vollziehenden Atomausstieg.
619	5. sonstige Betreiber Kritischer Infrastrukturen, soweit sie auf Grund von Rechtsvorschriften Anforderungen erfüllen müssen, die mit den Anforderungen nach § 8a vergleichbar oder weitergehend sind.		Entfällt. Vorschrift kam in der Praxis nicht ersichtlich zur Anwendung.
620	(3) § 8b Absatz 4 und 4a ist nicht anzuwenden auf		Teilweise verschoben, teilweise entfallen. Siehe nachstehende Begründungen.
621	1. Betreiber Kritischer Infrastrukturen, soweit sie ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen,		Verschoben nach § 28 Abs. 5 Nr. 1 nF.
622	2. Betreiber von Energieversorgungsnetzen oder Energieanlagen, soweit sie den Regelungen des § 11 des Energiewirtschaftsgesetzes unterliegen,		Entfällt. Die Unternehmen sind zukünftig im Anwendungsbereich des BSIG nF.
623	3. die Gesellschaft für Telematik nach § 306 Absatz 1 Satz 3 des Fünften Buches Sozialgesetzbuch, Betreiber von Diensten der Telematikinfrastruktur im Hinblick auf die nach § 311 Absatz 6 und § 325 des Fünften Buches Sozialgesetzbuch zugelassenen Dienste und Betreiber von Diensten, soweit sie die		Verschoben nach § 28 Abs. 5 Nr. 2 nF.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Telematikinfrastruktur für nach § 327 Absatz 2 bis 5 des Fünften Buches Sozialgesetzbuch bestätigte Anwendungen nutzen,		
624	4. Genehmigungsinhaber nach § 7 Absatz 1 des Atomgesetzes für den Geltungsbereich der Genehmigung sowie		Entfällt. Die Regelung erübrigt sich mit dem am 1. April 2023 zu vollziehenden Atomausstieg.
625	5. sonstige Betreiber Kritischer Infrastrukturen, die auf Grund von Rechtsvorschriften Anforderungen erfüllen müssen, die mit den Anforderungen nach § 8b Absatz 4 vergleichbar oder weitergehend sind.		Entfällt. Vorschrift kam in der Praxis nicht ersichtlich zur Anwendung..
626	(4) § 8c Absatz 1 bis 3 gilt nicht für Kleinstunternehmen und kleine Unternehmen im Sinne der Empfehlung 2003/361/EG. § 8c Absatz 3 gilt nicht für Anbieter,		Entfällt in Folge der Streichung von § 8c aF.
627	1. die ihren Hauptsitz in einem anderen Mitgliedstaat der Europäischen Union haben oder		s.o.
628	2. die, soweit sie nicht in einem Mitgliedstaat der Europäischen Union niedergelassen sind, einen Vertreter in einem anderen Mitgliedstaat der Europäischen Union benannt haben, in dem die digitalen Dienste ebenfalls angeboten werden.		s.o.
629	Für Anbieter nach Satz 2 gilt § 8c Absatz 4 nur, soweit sie in der Bundesrepublik Deutschland Netz- und Informationssysteme betreiben, die sie zur Bereitstellung der digitalen Dienste innerhalb der Europäischen Union nutzen.		s.o.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
630	§ 8e Auskunftsverlangen	§ 42 Auskunftsverlangen	Neue Enummerierung [*Anm. BMI CI 1 – Diese Vorschrift (§ 8e BSIG aF.) ist Gegenstand der Evaluierung gemäß Art. 6 Abs. 1 Nr. 1 Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 18. Mai 2021 (BGBl. I S. 1122). Diese Änderung erfolgt vorbehaltlich der Ergebnisse dieser Evaluierung und wird gegebenenfalls noch auf deren Grundlage angepasst.*]
631	(1) Das Bundesamt kann Dritten auf Antrag Auskunft zu den im Rahmen von § 8a Absatz 2 und 3, § 8c Absatz 4 und § 8f erhaltenen Informationen sowie zu den Meldungen nach § 8b Absatz 4, 4a und 4b sowie § 8c Absatz 4 nur erteilen, wenn	(1) Zugang zu den Informationen und Akten in Angelegenheiten nach Teil 2 §§ 4 bis 10 und Teil 3 dieses Gesetzes wird nicht gewährt. Die Akteneinsichtsrechte von Verfahrensbeteiligten bleiben unberührt.	Aufgrund der Tätigkeiten als zuständige Behörde, CSIRT und zentrale Anlaufstelle erhält das Bundesamt nach der NIS-2-RL eine Vielzahl neuer Informationen über Wesentliche und Wichtige Einrichtungen und deren IT-Sicherheitsgefährdungen. Diese können sowohl einzeln als auch in Summe sensibel sein. Das IFG sieht eine Versagung nur dann vor, wenn die herausgegebene Information für sich genommen sensibel ist und lässt daher eine Ausforschung durch Informationszugangsanträge zu, die für sich genommen auf unsensible Informationen gerichtet sind, aber in Summe die Zusammenfügung zu einem sensiblen Bild der Informationssicherheit Wesentlicher und Wichtiger Einrichtungen ermöglichen. Im Hinblick auf die geopolitische Lage und die zunehmende Gefahr von Cyberangriffen auch durch feindlich

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			gesonnene Staaten, müssen diese Informationen daher besonders geschützt werden. Auch Art. 11 Abs. 1 lit. d) NIS-2 schreibt daher die Sicherstellung der Vertraulichkeit für die Cybersicherheitseinrichtungen vor. Die Aktenzugangsrechte von Verfahrensbeteiligten im Rahmen von Widerspruchs- und Gerichtsverfahren gegen Anordnungen o.ä. des Bundesamtes bleiben von dieser Regelung unberührt.
632	1. schutzwürdige Interessen des betroffenen Betreibers einer Kritischen Infrastruktur, des Unternehmens im besonderen öffentlichen Interesse oder des Anbieters digitaler Dienste dem nicht entgegenstehen und		s.o.
633	2. durch die Auskunft keine Beeinträchtigung von Sicherheitsinteressen eintreten kann.		s.o.
634	Zugang zu personenbezogenen Daten wird nicht gewährt.		s.o.
635	(2) Zugang zu den Akten des Bundesamtes in Angelegenheiten nach den §§ 8a bis 8c und 8f wird bei Vorliegen der Voraussetzungen des § 29 des Verwaltungsverfahrensgesetzes nur gewährt, wenn		s.o.
636	1. schutzwürdige Interessen des betroffenen Betreibers einer Kritischen Infrastruktur, des Unternehmens im besonderen öffentlichen Interesse oder des Anbieters digitaler Dienste dem nicht entgegenstehen und		s.o.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
637	2. durch den Zugang zu den Akten keine Beeinträchtigung von Sicherheitsinteressen eintreten kann.		s.o.
638	(3) Für Betreiber nach § 8d Absatz 2 und 3 gelten die Absätze 1 und 2 entsprechend.		s.o.
639	(4) Informationsansprüche nach dem Umweltinformationsgesetz bleiben von dieser Vorschrift unberührt.		s.o.
640	§ 8f Sicherheit in der Informationstechnik bei Unternehmen im besonderen öffentlichen Interesse		Entfällt. Unternehmen im besonderen öffentlichen Interesse („UBI“) gehen in die neue Einrichtungskategorie „Wichtige Einrichtungen“ auf. Sie werden weiterhin erfasst, es gelten nur fortan dieselben Regelungen wie für sonstige Einrichtungen in der neuen Einrichtungskategorie.
641	(1) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 1 und 2 sind verpflichtet, spätestens bis zum ersten Werktag, der darauf folgt, dass diese erstmalig oder erneut als Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 1 oder 2 gelten, und danach mindestens alle zwei Jahre eine Selbsterklärung zur IT-Sicherheit beim Bundesamt vorzulegen, aus der hervorgeht,		s.o.
642	1. welche Zertifizierungen im Bereich der IT-Sicherheit in den letzten zwei Jahren durchgeführt, welche Prüfgrundlage und welcher Geltungsbereich hierfür festgelegt wurden,		s.o.
643	2. welche sonstigen Sicherheitsaudits oder Prüfungen im Bereich der IT-Sicherheit in den letzten zwei Jahren durchgeführt,		s.o.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	welche Prüfgrundlage und welcher Geltungsbereich hierfür festgelegt wurden oder		
644	3. wie sichergestellt wird, dass die für das Unternehmen besonders schützenswerten informationstechnischen Systeme, Komponenten und Prozesse angemessen geschützt werden, und ob dabei der Stand der Technik eingehalten wird.		s.o.
645	(2) Das Bundesamt kann für die Selbsterklärung nach Absatz 1 zu verwendende Formulare einführen.		s.o.
646	(3) Das Bundesamt kann auf Grundlage der Selbsterklärung nach Absatz 1 Hinweise zu angemessenen organisatorischen und technischen Vorkehrungen nach Absatz 1 Nummer 3 zur Einhaltung des Stands der Technik geben.		s.o.
647	(4) Für Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 1 gilt die Pflicht nach Absatz 1 nicht vor dem 1. Mai 2023. Für Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 2 gilt diese Pflicht frühestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 5.		s.o.
648	(5) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 1 und 2 sind verpflichtet, sich gleichzeitig mit der Vorlage der ersten Selbsterklärung zur IT-Sicherheit nach Absatz 1 beim Bundesamt zu registrieren und eine zu den üblichen Geschäftszeiten erreichbare Stelle zu benennen. Die Übermittlung von Informationen durch		s.o.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	das Bundesamt nach § 8b Absatz 2 Nummer 4 erfolgt an diese Stelle.		
649	(6) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 3 können eine freiwillige Registrierung beim Bundesamt und die Benennung einer zu den üblichen Geschäftszeiten erreichbaren Stelle vornehmen. Die Übermittlung von Informationen durch das Bundesamt nach § 8b Absatz 2 Nummer 4 erfolgt an diese Stelle.		s.o.
650	(7) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 1 und 2 haben ab dem Zeitpunkt, zu dem eine Pflicht zur Vorlage der Selbsterklärung zur IT-Sicherheit nach Absatz 1 besteht, die folgenden Störungen unverzüglich über die nach Absatz 5 benannte Stelle an das Bundesamt zu melden:		s.o.
651	1. Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Erbringung der Wertschöpfung geführt haben,		s.o.
652	2. erhebliche Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Erbringung der Wertschöpfung führen können.		s.o.
653	Die Meldung muss Angaben zu der Störung, zu den technischen Rahmenbedingungen, insbesondere zu		s.o.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik und der Art der betroffenen Einrichtung oder Anlage enthalten.		
654	(8) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 3 haben spätestens ab dem 1. November 2021 die folgenden Störungen unverzüglich an das Bundesamt zu melden:		s.o.
655	1. Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Störfall nach der Störfall-Verordnung in der jeweils geltenden Fassung geführt haben,		s.o.
656	2. erhebliche Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Störfall nach der Störfall-Verordnung in der jeweils geltenden Fassung führen können.		s.o.
657	Die Meldung muss Angaben zu der Störung, zu den technischen Rahmenbedingungen, insbesondere zu der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik und der Art der betroffenen Einrichtung oder Anlage enthalten.		s.o.
658	(9) Rechtfertigen Tatsachen die Annahme, dass ein Unternehmen ein Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 2 ist, aber seine Pflichten nach Absatz 5 nicht erfüllt, so kann das Bundesamt verlangen:		s.o.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
659	1. eine rechnerische Darlegung, wie hoch die vom Unternehmen erbrachte inländische Wertschöpfung nach der in der Rechtsverordnung nach § 10 Absatz 5 festgelegten Berechnungsmethode ist, oder		s.o.
660	2. eine Bestätigung einer anerkannten Wirtschaftsprüfungsgesellschaft, dass das Unternehmen nach der in der Rechtsverordnung nach § 10 Absatz 5 festgelegten Berechnungsmethode kein Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 2 ist.		s.o.
661		Kapitel 3 Sicherheit in der Informationstechnik der Einrichtungen der Bundesverwaltung	Neue Gliederung zur Steigerung der Übersichtlichkeit
662		§ 43 Informationssicherheitsmanagement	Neue zentrale Vorschrift zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung
663		(1) Die Einrichtungsleitung ist dafür verantwortlich, unter Berücksichtigung der Belange des IT-Betriebs die Voraussetzungen zur Gewährleistung der Informationssicherheit zu schaffen. Diese Voraussetzungen gelten als erfüllt, wenn die Anforderungen an ein Risikomanagement nach § 30 eingehalten werden und angemessene finanzielle, personelle und Sachmittel eingesetzt werden. Der finanzielle Mitteleinsatz gilt als angemessen, wenn er mindestens 20 Prozent der Ausgaben des IT-Betriebs innerhalb der Einrichtung beträgt. Die Einrichtungsleitung unterrichtet kalenderjährlich jeweils bis zum 31. März des dem Berichtsjahr folgenden Jahres die jeweils zuständige oberste Bundesbehörde	Die Norm dient der grundsätzlichen Verantwortungszuweisung für die Informationssicherheit und macht Vorgaben zu den Pflichten, die damit verbunden sind. Dazu zählen jedenfalls der IT-Grundschutz (inhaltlich kompatibel mit ISO/IEC 27001, der zur von Erwägungsgrund 79 der NIS-2 RL referenzierten Reihe ISO/IEC 27000 gehört) und die BSI-Mindeststandards. Die Verantwortung für die Gewährleistung der

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		über den Einsatz von Mitteln für die Informationssicherheit.	Informationssicherheit trägt die Leitung einer Einrichtung als Teil der allgemeinen Leitungsverantwortung. Sie verantwortet die Einhaltung von gesetzlichen und sonstigen Anforderungen sowie von internen Regelungen, die Übernahme von Restrisiken, das Bereitstellen von Ressourcen für die Informationssicherheit und ist zuständig für übergreifende Entscheidungen hinsichtlich der Informationssicherheitsziele und der Informationssicherheitsstrategie. Die Vorgabe, angemessene finanzielle und personelle Mittel zur Verfügung zu stellen, erlaubt abstrakt-generell auch im Einzelfall ein ausgewogenes Verhältnis zwischen IT-Betrieb und Informationssicherheit herzustellen (und zu diesem Zweck Zusammenarbeit zwischen Verantwortlichen für den IT-Betrieb und ISBs/IT-SiBes aktiv zu fördern). Die Verwendungs-Berichtspflicht als regelmäßige Rechtfertigungspflicht soll die tatsächliche Umsetzung sicherstellen. Die Vermutung, dass der Mitteleinsatz angemessen ist, ist allein auf die Quote bezogen. Die Angemessenheit kann jedoch nur unter zusätzlicher Berücksichtigung des Einsatzzwecks bewertet werden.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
664		(2) Soweit mit dem Betrieb von Informationstechnik des Bundes privatrechtlich organisierte Stellen beauftragt werden, ist vertraglich sicherzustellen, dass diese sich zur Einhaltung der Voraussetzungen zur Gewährleistung der Informationssicherheit verpflichten. Dies gilt auch für den Fall, dass Schnittstellen zur Kommunikationstechnik des Bundes eingerichtet werden. Die Pflichten der Einrichtungsleitung nach Absatz 1 bleiben hiervon unberührt.	Hierbei handelt es sich um eine Generalklausel zum Zweck der Verantwortungszuweisung an Einrichtungsleitungen im Falle der Beauftragung privater Dienstleister (insoweit bereits UP Bund Kap. 7)
665		(3) Die Registrierung von Einrichtungen der Bundesverwaltung nach § 32 obliegt der Einrichtungsleitung. Abweichend von § 34 weisen die Einrichtungen der Bundesverwaltung die Erfüllung der Anforderungen nach Absatz 1 spätestens zwei Jahre nach Inkrafttreten dieses Gesetzes und anschließend regelmäßig dem Bundesamt nach dessen Vorgaben nach.	Satz 1 stellt klar, dass die Registrierungspflicht aus § 32gemäß § 29 auch Einrichtungen der Bundesverwaltung trifft. Die hier vorgesehene Abweichung von § 34 sieht vor, dass Nachweise nicht nur „auf geeignete Weise“ zu erbringen sind, sondern Einrichtungen der Bundesverwaltung hierzu „nach Vorgaben des BSI“ handeln müssen. Zunächst ist dafür die Form einer standardisierten Selbsterklärung vorgesehen, in der die Einrichtungen die Umsetzung des IT-Grundschutzes und der Mindeststandards nachweisen, soweit dem BSI nicht bereits hinreichend aktuelle Ergebnisse eigener Prüfungen nach § 7 für die jeweilige Einrichtung vorliegen. Damit kann innerhalb der Einrichtungen der Bundesverwaltung die erforderliche Nachweisdichte risikobasiert weiter differenziert und der Prüfaufwand im Rahmen von § 7 für überprüfte

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			Einrichtungen und BSI gleichermaßen reduziert werden, wo die Gefährdungslage dies erlaubt.
666	*(3) Werden anderen Bundesbehörden Informationen nach Absatz 2 Nummer 1 bekannt, die für die Erfüllung von Aufgaben oder die Sicherheit der Informationstechnik anderer Behörden von Bedeutung sind, unterrichten diese ab dem 1. Januar 2010 das Bundesamt hierüber unverzüglich, soweit andere Vorschriften dem nicht entgegenstehen.* *(4) Ausgenommen von den Unterrichtungspflichten nach Absatz 2 Nummer 2 und Absatz 3 sind Informationen, die aufgrund von Regelungen zum Geheimschutz oder Vereinbarungen mit Dritten nicht weitergegeben werden dürfen oder deren Weitergabe im Widerspruch zu der verfassungsrechtlichen Stellung eines Abgeordneten des Bundestages oder eines Verfassungsorgans oder der gesetzlich geregelten Unabhängigkeit einzelner Stellen stünde.*	(4) Werden, über die sich aus § 31 ergebenden Meldepflichten hinaus, Einrichtungen der Bundesverwaltung Informationen nach § 4 Absatz 2 Nummer 1 bekannt, die für die Erfüllung von Aufgaben oder die Sicherheit der Kommunikationstechnik des Bundes von Bedeutung sind, unterrichten diese das Bundesamt hierüber unverzüglich, soweit andere Vorschriften dem nicht entgegenstehen. Ausgenommen von den Unterrichtungspflichten nach Satz 1 sind Informationen, die aufgrund von Regelungen zum Geheimschutz oder Vereinbarungen mit Dritten nicht weitergegeben werden dürfen oder deren Weitergabe im Widerspruch zu der verfassungsrechtlichen Stellung eines Abgeordneten des Bundestages oder eines Verfassungsorgans oder der gesetzlich geregelten Unabhängigkeit einzelner Stellen stünde. Die Einrichtungen der Bundesverwaltung melden dem Bundesamt kalenderjährlich jeweils bis zum 31. Januar eines Jahres die Gesamtzahl der nach Satz 2 nicht übermittelten Informationen.	Satz 1 war vormals § 4 Absatz 3. Satz 2 war vormals § 4 Absatz 4 in Bezug auf (dort) Absatz 3. Satz 3 wird neu eingefügt, um mit den betreffenden Informationen („Nullmeldungen“) eine erheblich bessere Gesamtbewertung der Gefährdungslage zu ermöglichen. Die Begrifflichkeiten der Regelungen werden von Bundesbehörden zu Einrichtungen der Bundesverwaltung konsolidiert und von „IT anderer Behörden“ zu „Kommunikationstechnik des Bundes“, womit das Schutzgut in den Vordergrund der Regelung gerückt wird. Mit Blick auf das Schutzgut und vor dem Hintergrund der sich entwickelnden Bedrohungslage ist die Erweiterung des Anwendungsbereichs durch die Erweiterung auf Einrichtungen der Bundesverwaltung sachgerecht.
667	*(6) Das Bundesministerium des Innern, für Bau und Heimat erlässt nach Zustimmung durch den Rat der IT-Beauftragten der Bundesregierung allgemeine Verwaltungsvorschriften zur Durchführung des Absatzes 3.*	(5) Das Bundesministerium des Innern und für Heimat erlässt nach Zustimmung durch die Ressorts allgemeine Verwaltungsvorschriften zur Durchführung des Absatzes 4.	Vormals § 4 Absatz 6 BSIG. Redaktionelle Anpassung des Verweises. Zudem wird der Verweis auf den Rat der IT-Beauftragten der Bundesregierung ersetzt durch „die Ressorts“, um die Durchführung des Gesetzes unabhängig von über die Legislaturperioden hinweg

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			unterschiedlichen politischen Entwicklungen bei der Ausgestaltung der Gremienlandschaft der IT-Steuerung zu halten. Die Zustimmung der Ressorts kann durch Mehrheitsentscheidung in einem geeigneten Gremium erfolgen. (Wie im Umsetzungsplan Bund wird der Begriff „Ressort“ im Zusammenhang mit Regelungen verwendet, die das Bundeskanzleramt oder ein Bundesministerium jeweils inklusive des Geschäftsbereichs betreffen.
668		§ 44 Vorgaben des Bundesamtes	Verschoben, vormals § 8 aF.
669	*(1) Das Bundesamt legt im Benehmen mit den Ressorts Mindeststandards für die Sicherheit der Informationstechnik des Bundes fest, die von*	(1) Das Bundesamt legt durch den IT-Grundschutz und durch Mindeststandards für die Sicherheit der Informationstechnik des Bundes die nach § 43 Absatz 1 zu erfüllenden Anforderungen an das Informationssicherheitsmanagement der Einrichtungen der Bundesverwaltung fest. Die Mindeststandards legt das Bundesamt im Benehmen mit den Ressorts fest. Das Bundesamt berät die Einrichtungen der Bundesverwaltung auf Ersuchen bei der Umsetzung und Einhaltung dieser Anforderungen. Für die in § 2 Absatz 3 Satz 2 genannten Gerichte und Verfassungsorgane haben die Vorschriften nach Satz 1 empfehlenden Charakter.	Der bisherige § 8 Absatz 1 BSIG wird im Anwendungsbereich auf die neu auf gesetzlicher Ebene eingeführte Begrifflichkeit der Einrichtungen der Bundesverwaltung angepasst. Zur näheren Erläuterung des Anwendungsbereichs siehe Begründung zu § 27 Absatz 1 (Zeile 434). Satz 3 aF „Abweichungen von den Mindeststandards sind nur in sachlich gerechtfertigten Fällen zulässig und sind zu dokumentieren und zu begründen.“ wird gestrichen, da er inhaltlich durch die Kompetenz der Ressort-ISBs ersetzt wird, Ausnahmebescheide zu erlassen (§ 42a Abs. 4 nF; Z. 675e).

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			Die Formulierung zielt darauf ab klarzustellen, dass die Vorgaben, die das Bundesamt mit dem IT-Grundschutz und mit den Mindeststandards für die Einrichtungen der Bundesverwaltung festlegt, materiell den Anforderungen an ein Informationssicherheitsmanagement nach § 41 Absatz 1 entsprechen und damit die Voraussetzungen von § 30 erfüllen. Im Einzelnen: Mit der Ergänzung des IT-Grundschutzes in der neuen Regelung über Vorgaben des Bundesamtes wird die bislang durch Kabinettsbeschluss zum Umsetzungsplan Bund für Bundesbehörden bereits geltende Pflicht, den durch das Bundesamt entwickelten IT-Grundschutz umzusetzen, nunmehr gesetzlich verankert. Damit erhalten beide für das Informationssicherheitsmanagement des Bundes maßgeblichen Regelwerke gemeinsam an zentraler Stelle dasselbe Niveau an Verbindlichkeit. Unter Berücksichtigung der Erwägungsgründe der NIS-2-Richtlinie zu den Anforderungen an ein Risikomanagement (insbesondere Erwägungsgründe 78-82) und der Tatsache, dass mit einem ISO 27001-Zertifikat auf der Basis des IT-Grundschutzes eine Institution belegen kann, dass die umgesetzten Maßnahmen zur Informationssicherheit anerkannten internationalen Standards entsprechen, wird festgestellt, dass der

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			IT-Grundschutz in Kombination mit den vom BSI bereitgestellten Mindeststandards die Anforderungen an das Informationssicherheitsmanagement nach § 41 Abs. 1 S. 2 erfüllt und folglich auch bei Vorliegen voneinander abweichender technischer Termini materiell das Schutzniveau erreicht wird, das von § 28 vorgegeben wird. So entsteht den Einrichtungen, die bereits seit langem zur Umsetzung des IT-Grundschutzes und der Mindeststandards verpflichtet sind, keine unverhältnismäßige finanzielle und administrative Belastung durch die Neuregelung. Der IT-Grundschutz liefert ein solides fachliches Fundament und ein umfangreiches Arbeitswerkzeug. Er ist Methode, Anleitung, Empfehlung und in der Praxis als Hilfe zur Selbsthilfe für Behörden, Unternehmen und andere Institutionen etabliert. Zentral ist dabei ein ganzheitlicher Ansatz zur Informationssicherheit: Neben technischen Aspekten werden auch infrastrukturelle, organisatorische und personelle Themen betrachtet. Dies ermöglicht ein systematisches Vorgehen, um notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Die BSI-Standards liefern hierzu bewährte Vorgehensweisen, das IT-Grundschutz-Kompendium zugehörige Anforderungen, um in einer Institution ein Managementsystem für

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			Informationssicherheit (ISMS) zu implementieren. Wegen der generellen Ausnahme für die Streitkräfte und den Militärischen Abschirmdienst in § 27 kann der bisherige Satz 5 entfallen.
670	*1. Stellen des Bundes,*		
671	*2. Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie ihren Vereinigungen ungeachtet ihrer Rechtsform auf Bundesebene, soweit von der jeweils zuständigen obersten Bundesbehörde angeordnet, sowie*		
672	*3. öffentlichen Unternehmen, die mehrheitlich im Eigentum des Bundes stehen und die IT-Dienstleistungen für die Bundesverwaltung erbringen,*		
673	*umzusetzen sind. Abweichungen von den Mindeststandards sind nur in sachlich gerechtfertigten Fällen zulässig und sind zu dokumentieren und zu begründen. Das Bundesamt berät die in Satz 1 genannten Stellen auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards. Für die in § 2 Absatz 3 Satz 2 genannten Gerichte und Verfassungsorgane haben die Vorschriften nach Satz 1 empfehlenden Charakter. Für die Verpflichtung nach Satz 1 gilt die Ausnahme nach § 4a Absatz 6 entsprechend.*		
674	*(1a) Das Bundesministerium des Innern, für Bau und Heimat kann im Benehmen mit der Konferenz der IT-Beauftragten der Ressorts bei bedeutenden*		Verschoben, vormals § 8 Abs. 1a BSIG Regelung gestrichen, da obsolet: Kontrolliert werden nicht

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Mindeststandards die Überwachung und Kontrolle ihrer Einhaltung durch das Bundesamt anordnen. Das Bundesamt teilt das Ergebnis seiner Kontrolle der jeweiligen überprüften Stelle, deren zuständiger Aufsichtsbehörde sowie der Konferenz der IT-Beauftragten der Ressorts mit. Für andere öffentlich-rechtlich oder privatrechtlich organisierte Stellen dürfen nur dann Schnittstellen zur Kommunikationstechnik des Bundes eingerichtet werden, soweit die für die Einrichtung verantwortliche Stelle vertraglich sicherstellt, dass die öffentlich- oder privatrechtlich organisierte Stelle sich zur Einhaltung der Mindeststandards verpflichtet. Das Bundesamt kann im Einvernehmen mit dem Dritten die Einhaltung der Mindeststandards überprüfen und kontrollieren.		Mindeststandards, sondern Einrichtungen, die Kommunikationstechnik des Bundes betreiben. Kontrolle und Überwachung durch das Bundesamt sowie Ergebnismitteilung kann auch ohne Anordnung und Benehmen risikobasiert nach § 7 nF erfolgen, nicht nur hinsichtlich Mindeststandards, auch bei mit Betriebsleistung beauftragten Dritten. Vertragliche Erstreckung von Vorgaben bei der Beauftragung von Privaten sowie der Einrichtung von Schnittstellen ist in § 41 Abs. 2 nF allgemein geregelt.
675	*(2) Das Bundesamt stellt im Rahmen seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 10 technische Richtlinien bereit, die von den Stellen des Bundes als Rahmen für die Entwicklung sachgerechter Anforderungen an Auftragnehmer (Eignung) und IT-Produkte (Spezifikation) für die Durchführung von Vergabeverfahren berücksichtigt werden. Die Vorschriften des Vergaberechts und des Geheimschutzes bleiben unberührt.*	(3) Das Bundesamt stellt im Rahmen seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 10 technische Richtlinien bereit, die von den Stellen des Bundes als Rahmen für die Entwicklung sachgerechter Anforderungen an Auftragnehmer (Eignung) und IT-Produkte (Spezifikation) für die Durchführung von Vergabeverfahren berücksichtigt werden. Die Vorschriften des Vergaberechts und des Geheimschutzes bleiben unberührt.	Verschoben, vorm. § 8 Abs. 2 BSIG Begriffskonsolidierung: Beibehaltung Stellen des Bundes, da Vergaben betroffen.
676		(4) Für den Einsatz von Informationstechnik bei der Verarbeitung von Verschlusssachen nach § 4 Absatz 1 SÜG kann das Bundesamt höhere Anforderungen für die Informationssicherheit vorsehen. Soweit mit Kommunikationstechnik des Bundes sowohl nicht als Verschlusssache eingestufte Daten als auch Verschlusssachen bis zum Einstufungsgrad VS-NUR FÜR DEN DIENSTGEBRAUCH verarbeitet werden, findet darauf ausschließlich dieses Gesetz Anwendung.	Konvergenz von IT-Sicherheit und Geheimschutz, um Zuständigkeitsabgrenzung im Bereich des Geheimschutzes zu erleichtern, soweit offene Informationen gemeinsam mit bis VS-NfD eingestuften Inhalten gemischt verarbeitet werden.
677	*(3) Die Bereitstellung von IT-Sicherheitsprodukten durch das Bundesamt nach § 3 Absatz 1 Satz 2*	(4) Für die Einrichtungen der Bundesverwaltung kann durch den Koordinator oder die Koordinatorin für	Es handelt sich bei diesem Absatz um eine systematische Abspaltung des

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Nummer 11 erfolgt durch Eigenentwicklung oder nach Durchführung von Vergabeverfahren aufgrund einer entsprechenden Bedarfsfeststellung. IT-Sicherheitsprodukte können nur in begründeten Ausnahmefällen durch eine Eigenentwicklung des Bundesamtes zur Verfügung gestellt werden. Die Vorschriften des Vergaberechts bleiben unberührt. Wenn das Bundesamt IT-Sicherheitsprodukte bereitstellt, können die Stellen des Bundes oder von ihnen beauftragte Dritte diese Produkte beim Bundesamt abrufen. Durch Beschluss des Rats der IT-Beauftragten der Bundesregierung kann festgelegt werden, dass die Bundesbehörden verpflichtet sind, diese Produkte beim Bundesamt abzurufen. Eigenbeschaffungen anderer Bundesbehörden sind in diesem Fall nur zulässig, wenn das spezifische Anforderungsprofil den Einsatz abweichender Produkte erfordert. Die Sätze 5 und 6 gelten nicht für die in § 2 Absatz 3 Satz 2 genannten Gerichte und Verfassungsorgane.	Informationssicherheit im Einvernehmen mit den Ressorts festgelegt werden, dass sie verpflichtet sind, nach § 8 bereitgestellte IT-Sicherheitsprodukte beim Bundesamt abzurufen. Eigenbeschaffungen sind in diesem Fall nur zulässig, wenn das spezifische Anforderungsprofil den Einsatz abweichender Produkte erfordert. Dies gilt nicht für die in § 2 Absatz 3 Satz 2 genannten Gerichte und Verfassungsorgane.	vormaligen § 8 Absatz 3 BSIG. Hier enthalten ist die Befugnis, Nutzungsvorgaben für die Einrichtungen der Bundesverwaltung zu machen. Die allgemeine BSI-Befugnis zur Bereitstellung von IT-Sicherheitsprodukten verbleibt mit § 17 in Teil 2 „Bundesamt“. Die Zuständigkeit wird aus sachlichen Gründen auf CISO Bund im Einvernehmen mit den Ressorts (z.B. durch Mehrheitsbeschluss in einem geeigneten Gremium) verlagert. und die Begrifflichkeiten vereinheitlichend erweitert zu Einrichtungen der Bundesverwaltung. Die Erweiterung auf Einrichtungen der Bundesverwaltung erfolgt vor dem Hintergrund, dass eine Abrufverpflichtung über das BSI nur dann erfolgen kann, wenn sachliche Gründe es erfordern, sodass im Ergebnis das Schutzgut der Sicherheit in der Informationstechnik des Bundes schwerer wiegt als Autonomie der Einrichtungen der Bundesverwaltung. Vergaberechtliche Aspekte bleiben unberührt und sind in die Entscheidungsfindung einzubeziehen. In Satz 3 ist eine redaktionelle Folgeänderung erfolgt.
678		§ 45 Informationssicherheitsbeauftragte der Einrichtungen der Bundesverwaltung	Die Regelung führt auf gesetzlicher Ebene Informationssicherheitsbeauftragte (ISBs) in Einrichtungen der Bundesverwaltung als notwendige

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			Funktion ein. Das soll die herausgehobene Bedeutung der Informationssicherheit in allen Bereichen moderner Verwaltungstätigkeit unterstreichen. Eine klare gesetzliche Definition ihrer Aufgaben und Befugnisse erleichtert auch eine verbesserte Zusammenarbeit mit anderen Verantwortungsbereichen und deren Beauftragten (z.B. Datenschutz und Geheimschutz). Im Umsetzungsplan Bund wurde bisher die inzwischen überholte Bezeichnung IT-Sicherheitsbeauftragter (IT-SiBe) verwendet, diese wird hiermit zugunsten des ISB überwunden.
679		(1) Die Einrichtungen der Bundesverwaltung bestellen jeweils eine Informationssicherheitsbeauftragte oder einen Informationssicherheitsbeauftragten sowie eine zur Vertretung berechtigte Person.	Mit der gesetzlichen Festschreibung soll die Bedeutung der Funktion der Informationssicherheitsbeauftragten unterstrichen und gesichert werden.
680		(2) Für die Erfüllung ihrer Aufgaben sind neben Personal- und Sachausstattung in angemessenem Umfang auch finanzielle Mittel zur Verfügung zu stellen, die sie zur Erfüllung ihrer Aufgaben eigenständig verwalten. Die Informationssicherheitsbeauftragen müssen die zur Erfüllung ihrer Aufgaben erforderliche Fachkunde erwerben. Sie unterstehen der Fachaufsicht des oder der jeweils zuständigen Informationssicherheitsbeauftragten des Ressorts.	Personal- und Sachausstattung richten sich nach dem Gesamterfüllungsaufwand in der jeweiligen Einrichtung und nach dem Schadenspotenzial von Sicherheitsvorfällen oder Störungen. Angemessene finanzielle Mittel sind in der Regel ca. 20 % der entsprechenden Ausgaben für den IT-Betrieb (vgl. Erläuterungen zu § 41 Absatz 1, Zeile 657); im Einzelfall bei z.B. IT-Dienstleistern kann diese Quote höher ausfallen. Fachkunde ist nicht Voraussetzung für die Übertragung der Tätigkeit, muss jedoch wenigstens

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			tätigkeitsbegleitend erworben werden. Dadurch wird einerseits die Besetzung entsprechender Funktionen erleichtert. Andererseits müssen auch etablierte Funktionsträger ihre Fachkunde so kontinuierlich an die sich wandelnden Erfordernisse anpassen. Die Fachaufsicht wird zum Zwecke der notwendigen operativen Unabhängigkeit für die effektive Vertretung von Sicherheitsbelangen durch die fachkundigen Ressort-ISBs ausgeübt**.**
681		(3) Die Informationssicherheitsbeauftragten sind für den Aufbau und die Aufrechterhaltung des Informationssicherheitsprozesses der Einrichtung verantwortlich. Sie erstellen ein Informationssicherheitskonzept, welches mindestens die Vorgaben des Bundesamtes nach § 44 Absatz 1 erfüllt. Sie sorgen für die operative Umsetzung des Informationssicherheitskonzepts und kontrollieren diese innerhalb der Einrichtung. Die Informationssicherheitsbeauftragen beraten die Einrichtungsleitung in allen Fragen der Informationssicherheit und unterrichten die Einrichtungsleitung regelmäßig sowie anlassbezogen über ihre Tätigkeit.	Absatz 3 regelt die Aufgaben der Einrichtungs-ISBs, die im Auftrag ihrer Einrichtungsleitung für die operative Umsetzung und Kontrolle von Maßnahmen im Rahmen des Informationssicherheitsmanagements zuständig sind. Indem sie die Anforderungen des Bundesamtes nach § 42 Absatz 1 erfüllen, also die Vorgaben des IT-Grundschutzes und der Mindeststandards, erfüllen sie ihre operative Umsetzungspflicht vollumfänglich. Darüber hinausgehende Sicherheitsmaßnahmen, die ISBs im Einzelfall für erforderlich halten, können sie ergänzend im Informationssicherheitskonzept aufnehmen, ohne dass ein Weglassen solcher Maßnahmen eine Pflichtverletzung im Rahmen ihrer individuellen Verantwortung darstellen würde. Die Verantwortung der Einrichtungsleitung wird hierdurch nicht berührt. Es handelt sich bei der

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			Konzepterstellung nicht um eine höchstpersönliche Aufgabe. Insbesondere kann das Gesamt-Informationssicherheitskonzept für die Einrichtung auch eine Auslagerung bzw. eine Beauftragung Dritter mit der Erstellung von Informationssicherheitskonzepten vorsehen. Die Berichtspflicht soll Compliance erwirken, für deren kontinuierliche Aufrechterhaltung eine mindestens quartalsweise Berichterstattung förderlich ist. Welche Häufigkeit für Regelmäßigkeit konkret angemessen ist, hängt darüber hinaus von den Umständen des jeweiligen Einzelfalls unter Abwägung des Schadenspotenzials im Falle von Sicherheitslücken ab. Aus den Aufgaben ergeben sich zugleich einrichtungsintern entsprechende Befugnisse.
682		(4) Die Informationssicherheitsbeauftragten sind bei allen Maßnahmen zu beteiligen, die die Informationssicherheit der Einrichtung betreffen. Sie haben ein unmittelbares Vortragsrecht bei der jeweiligen Einrichtungsleitung sowie beim Koordinator oder der Koordinatorin für Informationssicherheit des jeweils zuständigen Ressorts.	Die Vortragsrechte gegenüber der Einrichtungsleitung und dem jeweiligen Ressort-ISB dienen dazu, die Position der ISBs fachlich so unabhängig von der Organisation der Einrichtung zu gestalten, wie es für die Aufgabe zur Vermeidung von Interessenskonflikten erforderlich ist.
683		§ 46 Informationssicherheitsbeauftragte der Ressorts	Mit der Norm wird dem Ressort-ISB eine gesetzliche Grundlage gegeben, der schon bisher im Rahmen des Umsetzungsplans Bund angelegt ist. In Umsetzung von Art. 31 Absatz 4 NIS 2 RL bedarf es für die Aufsicht über Einrichtungen öffentlicher Verwaltung

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			der Garantie, dass diese Aufsicht operativ unabhängig von der jeweils beaufsichtigten Einrichtung erfolgen kann. Diese operative Unabhängigkeit wird hier dadurch erreicht, dass Ressort-ISBs a) Fachkunde besitzen müssen, es sich also nicht um politische Funktionen handelt, sondern der Fokus bei der Aufgabenausübung auf der fachlichen Expertise liegt, b) ein eigenes Budgetrecht besitzen, um handlungsfähig zu sein, und c) wird die Unabhängigkeit im Hinblick auf Fragen der Informationssicherheit dadurch sichergestellt, dass sie unmittelbar vor dem CISO Bund vortragen dürfen, der seinerseits Vortragsrechte unmittelbar gegenüber Organen der Legislative besitzt.
684		(1) Die Ressorts bestellen jeweils eine Informationssicherheitsbeauftragte oder einen Informationssicherheitsbeauftragten des Ressorts, denen unter Berücksichtigung der Belange des IT-Betriebs die Steuerung und Überwachung des Informationssicherheitsmanagements in ihrem Ressort obliegt. Sie wirken auf eine angemessene Umsetzung der Informationssicherheit und eine angemessene Verwendung von Mitteln für die Informationssicherheit in ihrem Ressort hin.	Ressort-ISBs tragen die Verantwortung für ein funktionierendes und effektives Informationssicherheitsmanagement in ihrem Ressort, das die jeweilige oberste Bundesbehörde mitsamt ihrem jeweiligen Geschäftsbereich umfasst. Im Fall oberster Bundesbehörden sind die Funktionen von Ressort-ISB und Einrichtungs-ISB zu unterscheiden, können jedoch derselben Person übertragen werden. Die Angemessenheit der Informationssicherheit ist in Bezug auf Wechselwirkung mit den Belangen des IT-Betriebs zu bewerten.
685		(2) Für die Erfüllung seiner oder ihrer Aufgaben sind neben Personal- und Sachausstattung in angemessenem Umfang auch angemessene	Damit Ressort-ISBs die für die Erfüllung ihrer Aufgaben notwendige organisatorische Unabhängigkeit

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		finanzielle Mittel zur Verfügung zu stellen, die der oder die Informationssicherheitsbeauftragte des Ressorts zur Erfüllung seiner oder ihrer Aufgaben eigenständig verwaltet. Der oder die Informationssicherheitsbeauftragte des Ressorts muss die zur Erfüllung seiner oder ihrer Aufgaben erforderliche Fachkunde besitzen.	besitzen, benötigen sie angemessene Ausstattung und Mittel, die nicht auf organisatorischer Ebene anderen Zwecken zufließen können dürfen. Fachkunde ist erforderlich, da die Ressort-ISBs die Fachaufsicht über die ISBs der Einrichtungen in ihrem Zuständigkeitsbereich führen können müssen.
686		(3) Der oder die Informationssicherheitsbeauftragte initiiert und koordiniert jeweils die Fortschreibung von Informationssicherheitsleitlinien für sein oder ihr Ressort. Er oder sie unterrichtet die Ressortleitung über seine oder ihre Tätigkeit und über den Stand der Informationssicherheit innerhalb des Ressorts, über die angemessene Mittelverwendung nach § 43 Absatz 1 Satz 2 sowie über Sicherheitsvorfälle. Er oder sie berichtet über die angemessene Mittelverwendung zudem kalenderjährlich jeweils bis zum 31. März des dem Berichtsjahr folgenden Jahres an den Koordinator oder die Koordinatorin für Informationssicherheit. In begründeten Einzelfällen kann der Informationssicherheitsbeauftragte des Ressorts im Benehmen mit dem oder der jeweiligen IT-Beauftragten des Ressorts den Einsatz bestimmter IT-Produkte in Einrichtungen der Bundesverwaltung innerhalb des jeweiligen Ressorts ganz oder teilweise untersagen.	Absatz 3 normiert die Aufgaben der Ressort-ISBs, aus denen sich zugleich ressortintern die Befugnis zu Kontrolle und Umsetzungsmaßnahmen ergibt. Da die ISBs der Einrichtungen der fachlichen Aufsicht der Ressort-ISBs unterstehen, sind die Ressort-ISBs insoweit weisungsbefugt. Die Berichtspflicht dient als Mittel der Complianceförderung. Das Veto-Recht dient dem Zweck, Informationssicherheitsbelange bei Bedarf durchzusetzen. Die Möglichkeit nur teilweise die Nutzung zu untersagen gestattet zwischen unterschiedlichen Anwendungszwecken zu unterscheiden (soweit etwa Produkte zum Zweck der Überprüfung verwendet werden müssen oder ein Einsatz in bestimmten IT-Umgebungen möglich ist, aber aus Sicherheitsgründen keine Nutzung im allgemeinen Geschäftsbetrieb erfolgen soll).

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
687		(4) Der oder die Informationssicherheitsbeauftragte des Ressorts kann im Benehmen mit dem Koordinator oder der Koordinatorin für Informationssicherheit Einrichtungen der Bundesverwaltung innerhalb des Ressorts, soweit diese nicht besonders wichtige Einrichtungen oder wichtige Einrichtungen nach § 28 sind, von Verpflichtungen nach diesem Teil teilweise oder insgesamt durch Erteilung eines Ausnahmebescheides befreien. Voraussetzung hierfür ist, dass sachliche Gründe für die Erteilung einer Ausnahme vorliegen und durch die Befreiung keine nachteiligen Auswirkungen für die Sicherheit der Informationstechnik des Bundes zu befürchten sind.	Absatz 4 regelt die Möglichkeit für Ressort-ISBs, Ausnahmebescheide für Einrichtungen innerhalb ihres Zuständigkeitsbereichs zu erlassen. Besonders wichtige und wichtige Einrichtungen können hiervon nicht umfasst werden. (Soweit es sich um Einrichtungen der Zentralregierung handelt, schließt die NIS-2-Richtlinie dies bereits aus; für die anderen findet grds. nach § 27 Absatz 2 Satz 2 (Zeile 438) dieses Kapitel ohnehin keine Anwendung; insoweit hat der Einschub hauptsächlich klarstellenden bzw. unterstreichenden Charakter. Die Möglichkeit zu Ausnahmen auch für besonders wichtige und wichtige Einrichtungen ist in § 35 vorgesehen. Anwendungsbeispiele: Für sehr kleine Einrichtungen kann der Ressort-ISB zulassen, dass für die Einrichtung kein eigener ISB bestellt werden muss, wenn ein anderer ISB des Geschäftsbereichs die Rolle für diese Einrichtung wahrnimmt.
688		(5) Der Informationssicherheitsbeauftragte des Ressorts ist bei allen Gesetzes-, Verordnungs- und sonstigen wichtigen Vorhaben innerhalb des Ressorts zu beteiligen, soweit diese Fragen der Informationssicherheit berühren. Er oder sie hat ein unmittelbares Vortragsrecht bei der jeweiligen Ressortleitung sowie beim Beauftragten der Bundesregierung für Informationstechnik und dem Koordinator oder der Koordinatorin für Informationssicherheit.	Allgemeine Beteiligungsrechte und Vortragsrechte der Ressort-ISBs.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
689		§ 47 Wesentliche Digitalisierungsvorhaben des Bundes	
690		(1) Für die Planung und Umsetzung von wesentlichen Digitalisierungsvorhaben und Kommunikationsinfrastrukturen des Bundes sind jeweils eigene Informationssicherheitsbeauftragte nach § 45 zu bestellen. Digitalisierungsvorhaben oder Kommunikationsinfrastrukturen des Bundes sind insbesondere dann wesentlich, wenn dabei Kommunikationstechnik des Bundes ressortübergreifend betrieben wird oder der ressortübergreifenden Kommunikation oder dem ressortübergreifenden Datenaustausch dient.	Wegen der zunehmenden Bedeutung und Größe von Digitalisierungsvorhaben ist fachlich erforderlich, dass Informationssicherheit dort durch eigene ISBs umgesetzt wird. Bei ressortübergreifenden Digitalisierungsvorhaben ist grds. von einer wesentlichen Bedeutung für allgemeine Sicherheitsbelange auszugehen, und die ressortübergreifenden Kommunikationsinfrastrukturen haben für die Regierungskommunikation insgesamt eine herausgehobene Bedeutung.
691	*(4) Zur Gewährleistung der Sicherheit in der Informationstechnik bei der Planung und Umsetzung von wesentlichen Digitalisierungsvorhaben des Bundes soll die jeweils verantwortliche Stelle das Bundesamt frühzeitig beteiligen und dem Bundesamt Gelegenheit zur Stellungnahme geben.*	(2) Zur Gewährleistung der Sicherheit in der Informationstechnik bei der Planung und Umsetzung von wesentlichen Digitalisierungsvorhaben sind angemessene Mittel für die Informationssicherheit einzusetzen. Die jeweils verantwortliche Einrichtung soll das Bundesamt frühzeitig beteiligen und dem Bundesamt Gelegenheit zur Stellungnahme geben.	Verschoben, vormals § 8 Abs. 4 BSIG Die Ergänzung erfolgt, um auch hier angemessene Mittel sicherzustellen.
692		§ 48 Amt des Koordinators für Informationssicherheit	
693		(1) Die Bundesregierung bestellt eine Koordinatorin oder einen Koordinator für Informationssicherheit.	Mit dieser Norm wird die Funktion eines CISO Bund geschaffen. Um Interessenskonflikte zu vermeiden, sollte die Aufgabe möglichst unabhängig organisiert werden.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
694		(2) Für die Erfüllung der Aufgaben sind neben Personal- und Sachausstattung auch finanzielle Mittel in angemessenem Umfang zur Verfügung zu stellen, die der Koordinator oder die Koordinatorin zur Erfüllung seiner oder ihrer Aufgaben eigenständig verwaltet.	Eine Ausübung der Aufgaben und Befugnisse kann nur bei Vorliegen gesicherter Mittel hierfür stattfinden.
695		§ 49 Aufgaben des Koordinators	
696		Dem Koordinator oder der Koordinatorin für Informationssicherheit obliegt die zentrale Koordinierung des Informationssicherheitsmanagements des Bundes. Zu diesem Zweck wirkt er auf ein angemessenes Verhältnis zwischen dem Einsatz von Informationstechnik und Informationssicherheit hin. Er oder sie koordiniert die Erstellung und Aktualisierung von Informationssicherheitsleitlinien des Bundes und unterstützt die Ressorts bei der Umsetzung der Vorgaben zur Informationssicherheit. Er oder sie überwacht die angemessene Mittelverwendung nach § 43 Absatz 1 Satz 2 und unterrichtet hierüber kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres den Haushaltsausschuss des Deutschen Bundestages.	Allgemeine Aufgaben CISO Bund.
697		§ 50 Befugnisse des Koordinators	
698		(1) Zur Wahrnehmung der Aufgaben nach § 49 beteiligen die Ressorts den Koordinator oder die Koordinatorin für Informationssicherheit bei allen Gesetzes-, Verordnungs- und sonstigen wichtigen Vorhaben, soweit sie Fragen der Informationssicherheit berühren. Er oder sie kann der Bundesregierung Vorschläge machen und Stellungnahmen zuleiten. Die Bundesministerien unterstützen den Koordinator oder	Allg. Beteiligungsrechte CISO Bund.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		die Koordinatorin bei der Erfüllung seiner oder ihrer Aufgaben.	
699		(2) Zur Wahrnehmung seiner oder ihrer Aufgaben hat der Koordinator oder die Koordinatorin ein direktes Vortragsrecht vor dem Ausschuss für Inneres und Heimat und dem Haushaltsausschuss des Deutschen Bundestages zu allen Themen der Informationssicherheit in Einrichtungen der Bundesverwaltung,	Vortragsrechte CISO Bund.
700		(3) Der Koordinator oder die Koordinatorin kann im Benehmen mit dem oder der Informationssicherheitsbeauftragten des jeweils zuständigen Ressorts Einrichtungen anweisen, innerhalb von drei Monaten nach der Vorlage der Ergebnisse von Kontrollen gemäß § 7 ein Sofortprogramm vorzulegen, welches die Einhaltung der Anforderungen innerhalb einer angemessenen Umsetzungsfrist sichert.	Konkret operative Umsetzung von Art. 32 Abs. 4 d) NIS 2 im Hinblick auf Zentralregierung zugunsten des CISO Bund. Aus Rücksicht auf das Ressortprinzip bedarf es des Benehmens mit dem oder der jeweiligen Ressort-ISB. Die Möglichkeit, zur Erstellung von Sofortprogrammen anzuweisen, bildet ein wirksames Element für effektive Nachsteuerung, wenn Anlass dafür gegeben ist. Anlässe können sein, wenn sich im Rahmen einer Überprüfung nach § 7 z.B. eine erhebliche Unterschreitung der Anforderungen an das Informationssicherheitsmanagement deutlich wird.
701		Teil 5 Datenbanken der Domain-Name-Registrierungsdaten	Umsetzung Art. 28 NIS-2
702		§ 51 Pflicht zum Führen einer Datenbank	Umsetzung Art. 28 NIS-2

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
703		(1) Um einen Beitrag zur Sicherheit, Stabilität und Resilienz des Domain Name Systems zu leisten, sind Top Level Domain Name Registriesund Domain-Name-Registry-Dienstleister verpflichtet, genaue und vollständige Domain-Namen-Registrierungsdaten in einer eigenen Datenbank im Einklang mit dem Datenschutzrecht in Bezug auf personenbezogene Daten mit der gebotenen Sorgfalt zu sammeln und zu pflegen.	Umsetzung Art. 28 Abs. 1 NIS-2
704		(2) Die Datenbank im Sinne des Absatzes 1 hat die erforderlichen Angaben zu enthalten, anhand derer die Inhaber der Domain-Namen und die Kontaktstellen, die die Domain-Namen im Rahmen der TLD verwalten, identifiziert und kontaktiert werden können. Diese Angaben müssen Folgendes umfassen:	Umsetzung Art. 28 Abs. 2 NIS-2
705		1. den Domain-Namen,	Umsetzung Art. 28 Abs. 2 lit. a NIS-2
706		2. das Datum der Registrierung;	Umsetzung Art. 28 Abs. 2 lit. b NIS-2
707		3. den Namen des Domain-Inhabers, seine E-Mail-Adresse und Telefonnummer;	Umsetzung Art. 28 Abs. 2 lit. c NIS-2
708		4. die Kontakt-E-Mail-Adresse und die Telefonnummer der Anlaufstelle, die den Domain-Namen verwaltet, falls diese sich von denen des Domain-Inhabers unterscheiden.	Umsetzung Art. 28 Abs. 2 lit. d NIS-2
709		(3) Top Level Domain Name Registriesund Domain-Name-Registry-Dienstleister sind verpflichtet über Vorgaben und Verfahren, einschließlich Überprüfungsverfahren, verfügen, mit denen sichergestellt wird, dass die Datenbanken im Sinne des Absatz 1 genaue und vollständige Angaben enthalten. Diese Vorgaben und Verfahren sind öffentlich zugänglich zu machen.	Umsetzung Art. 28 Abs. 3 NIS-2

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
710		(4) Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister sind verpflichtet, unverzüglich nach der Registrierung eines Domain-Namens die nicht personenbezogenen Domain-Namen-Registrierungsdaten öffentlich zugänglich zu machen.	Umsetzung Art. 28 Abs. 4 NIS-2
711		§ 52 Verpflichtung zur Zugangsgewährung	Umsetzung Art. 28 Abs. 5 NIS-2
712		Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister sind verpflichtet, auf rechtmäßige und hinreichend begründete Anträge berechtigten Zugangsnachfragern im Einklang mit dem Datenschutzrecht Zugang zu bestimmten Domain-Namen-Registrierungsdaten zu gewähren. Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister sind verpflichtet, alle Anträge auf Zugang unverzüglich und in jedem Fall innerhalb von 72 Stunden nach Eingang eines Antrags auf Zugang zu beantworten. Diese Vorgaben und Verfahren im Hinblick auf die Offenlegung solcher Daten sind öffentlich zugänglich zu machen.	Umsetzung Art. 28 Abs. 5 NIS-2
713		§ 53 Kooperationspflicht	Umsetzung Art. 28 Abs. 6 NIS-2
714		Um zu vermeiden, dass die Einhaltung der in § 51 und § 52 festgelegten Verpflichtungen zu einer doppelten Erhebung von Domain-Namen-Registrierungsdaten führt, sind TLD-Namenregister und Domain-Name-Registry-Dienstleister insoweit zur Kooperation verpflichtet.	Umsetzung Art. 28 Abs. 6 NIS-2.
715		Teil 5 Zertifizierung und Kennzeichen	Neue Gliederung zur Steigerung der Übersichtlichkeit

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
716	§ 9 Zertifizierung	§ 54 Zertifizierung	
717	(1) Das Bundesamt ist nationale Zertifizierungsstelle der Bundesverwaltung für IT-Sicherheit.	(1) Das Bundesamt ist nationale Zertifizierungsstelle der Bundesverwaltung für IT-Sicherheit.	
718	(2) Für bestimmte Produkte oder Leistungen kann beim Bundesamt eine Sicherheits- oder Personenzertifizierung oder eine Zertifizierung als IT-Sicherheitsdienstleister beantragt werden. Die Anträge werden in der zeitlichen Reihenfolge ihres Eingangs bearbeitet; hiervon kann abgewichen werden, wenn das Bundesamt wegen der Zahl und des Umfangs anhängiger Prüfungsverfahren eine Prüfung in angemessener Zeit nicht durchführen kann und an der Erteilung eines Zertifikats ein öffentliches Interesse besteht. Der Antragsteller hat dem Bundesamt die Unterlagen vorzulegen und die Auskünfte zu erteilen, deren Kenntnis für die Prüfung und Bewertung des Systems oder der Komponente oder der Eignung der Person sowie für die Erteilung des Zertifikats erforderlich ist.	(2) Für bestimmte Produkte oder Leistungen kann beim Bundesamt eine Sicherheits- oder Personenzertifizierung oder eine Zertifizierung als IT-Sicherheitsdienstleister beantragt werden. Die Anträge werden in der zeitlichen Reihenfolge ihres Eingangs bearbeitet; hiervon kann abgewichen werden, wenn das Bundesamt wegen der Zahl und des Umfangs anhängiger Prüfungsverfahren eine Prüfung in angemessener Zeit nicht durchführen kann und an der Erteilung eines Zertifikats ein öffentliches Interesse besteht. Der Antragsteller hat dem Bundesamt die Unterlagen vorzulegen und die Auskünfte zu erteilen, deren Kenntnis für die Prüfung und Bewertung des Systems oder der Komponente oder der Eignung der Person sowie für die Erteilung des Zertifikats erforderlich ist.	
719	(3) Die Prüfung und Bewertung kann durch vom Bundesamt anerkannte sachverständige Stellen erfolgen.	(3) Die Prüfung und Bewertung kann durch vom Bundesamt anerkannte sachverständige Stellen erfolgen.	
720	(4) Das Sicherheitszertifikat wird erteilt, wenn	(4) Das Sicherheitszertifikat wird erteilt, wenn	
721	1. informationstechnische Systeme, Komponenten, Produkte oder Schutzprofile den vom Bundesamt festgelegten Kriterien entsprechen und	1. informationstechnische Systeme, Komponenten, Produkte oder Schutzprofile den vom Bundesamt festgelegten Kriterien entsprechen und	
722	2. das Bundesministerium des Innern, für Bau und Heimat die Erteilung des	2. das Bundesministerium des Innern und für Heimat die Erteilung des Zertifikats nicht nach Absatz 4a untersagt hat.	Redaktionelle Änderung

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Zertifikats nicht nach Absatz 4a untersagt hat.		
723	Vor Erteilung des Sicherheitszertifikats legt das Bundesamt den Vorgang dem Bundesministerium des Innern, für Bau und Heimat zur Prüfung nach Absatz 4a vor.	Vor Erteilung des Sicherheitszertifikats legt das Bundesamt den Vorgang dem Bundesministerium des Innern und für Heimat zur Prüfung nach Absatz 4a vor.	Redaktionelle Änderung
724	(4a) Das Bundesministerium des Innern, für Bau und Heimat kann eine Zertifikatserteilung nach Absatz 4 im Einzelfall untersagen, wenn überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung entgegenstehen.	(4a) Das Bundesministerium des Innern und für Heimat kann eine Zertifikatserteilung nach Absatz 4 im Einzelfall untersagen, wenn überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung entgegenstehen.	Redaktionelle Änderung
725	(5) Für die Zertifizierung von Personen und IT-Sicherheitsdienstleistern gilt Absatz 4 entsprechend.	(5) Für die Zertifizierung von Personen und IT-Sicherheitsdienstleistern gilt Absatz 4 entsprechend.	
726	(6) Eine Anerkennung nach Absatz 3 wird erteilt, wenn	(6) Eine Anerkennung nach Absatz 3 wird erteilt, wenn	
727	1. die sachliche und personelle Ausstattung sowie die fachliche Qualifikation und Zuverlässigkeit der Konformitätsbewertungsstelle den vom Bundesamt festgelegten Kriterien entspricht und	1. die sachliche und personelle Ausstattung sowie die fachliche Qualifikation und Zuverlässigkeit der Konformitätsbewertungsstelle den vom Bundesamt festgelegten Kriterien entspricht und	
728	2. das Bundesministerium des Innern, für Bau und Heimat festgestellt hat, dass überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung nicht entgegenstehen.	2. das Bundesministerium des Innern und für Heimat festgestellt hat, dass überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung nicht entgegenstehen.	Redaktionelle Änderung
729	Das Bundesamt stellt durch die notwendigen Maßnahmen sicher, dass das Fortbestehen der	Das Bundesamt stellt durch die notwendigen Maßnahmen sicher, dass das Fortbestehen der	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Voraussetzungen nach Satz 1 regelmäßig überprüft wird.	Voraussetzungen nach Satz 1 regelmäßig überprüft wird.	
730	(7) Sicherheitszertifikate anderer anerkannter Zertifizierungsstellen aus dem Bereich der Europäischen Union werden vom Bundesamt anerkannt, soweit sie eine den Sicherheitszertifikaten des Bundesamtes gleichwertige Sicherheit ausweisen und die Gleichwertigkeit vom Bundesamt festgestellt worden ist.	(7) Sicherheitszertifikate anderer anerkannter Zertifizierungsstellen aus dem Bereich der Europäischen Union werden vom Bundesamt anerkannt, soweit sie eine den Sicherheitszertifikaten des Bundesamtes gleichwertige Sicherheit ausweisen und die Gleichwertigkeit vom Bundesamt festgestellt worden ist.	
731	§ 9a Nationale Behörde für die Cybersicherheitszertifizierung	§ 55 Nationale Behörde für die Cybersicherheitszertifizierung	
732	(1) Das Bundesamt ist die nationale Behörde für die Cybersicherheitszertifizierung im Sinne des Artikels 58 Absatz 1 der Verordnung (EU) 2019/881.	(1) Das Bundesamt ist die nationale Behörde für die Cybersicherheitszertifizierung im Sinne des Artikels 58 Absatz 1 der Verordnung (EU) 2019/881.	
733	(2) Das Bundesamt kann auf Antrag Konformitätsbewertungsstellen, die im Anwendungsbereich der Verordnung (EU) 2019/881 sowie des § 9 dieses Gesetzes tätig werden, eine Befugnis erteilen, als solche tätig zu werden, wenn die Voraussetzungen des maßgeblichen europäischen Schemas für die Cybersicherheitszertifizierung nach Artikel 54 der Verordnung (EU) 2019/881 oder des § 9 dieses Gesetzes erfüllt sind. Ohne eine Befugniserteilung durch das Bundesamt dürfen Konformitätsbewertungsstellen im Anwendungsbereich der Verordnung (EU) 2019/881 nicht tätig werden.	(2) Das Bundesamt kann auf Antrag Konformitätsbewertungsstellen, die im Anwendungsbereich der Verordnung (EU) 2019/881 sowie des § 54 dieses Gesetzes tätig werden, eine Befugnis erteilen, als solche tätig zu werden, wenn die Voraussetzungen des maßgeblichen europäischen Schemas für die Cybersicherheitszertifizierung nach Artikel 54 der Verordnung (EU) 2019/881 oder des § 54 dieses Gesetzes erfüllt sind. Ohne eine Befugniserteilung durch das Bundesamt dürfen Konformitätsbewertungsstellen im Anwendungsbereich der Verordnung (EU) 2019/881 nicht tätig werden.	
734	(3) Soweit dies zur Erfüllung seiner Aufgaben nach Artikel 58 Absatz 7 der Verordnung (EU) 2019/881 und nach § 9 dieses Gesetzes erforderlich ist, kann das Bundesamt von Konformitätsbewertungsstellen, denen eine Befugnis nach Absatz 2 erteilt wurde, von Inhabern europäischer Cybersicherheitszertifikate und	(3) Soweit dies zur Erfüllung seiner Aufgaben nach Artikel 58 Absatz 7 der Verordnung (EU) 2019/881 und nach § 54 dieses Gesetzes erforderlich ist, kann das Bundesamt von Konformitätsbewertungsstellen, denen eine Befugnis nach Absatz 2 erteilt wurde, von Inhabern europäischer Cybersicherheitszertifikate und	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	von Ausstellern von EU-Konformitätserklärungen im Sinne von Artikel 56 Absatz 8 der Verordnung (EU) 2019/881 die erforderlichen Auskünfte und sonstige Unterstützung, insbesondere die Vorlage von Unterlagen oder Mustern, verlangen. § 3 Absatz 1 Satz 1 und 3 des Akkreditierungsstellengesetzes gilt entsprechend.	von Ausstellern von EU-Konformitätserklärungen im Sinne von Artikel 56 Absatz 8 der Verordnung (EU) 2019/881 die erforderlichen Auskünfte und sonstige Unterstützung, insbesondere die Vorlage von Unterlagen oder Mustern, verlangen. § 3 Absatz 1 Satz 1 und 3 des Akkreditierungsstellengesetzes gilt entsprechend.	
735	(4) Das Bundesamt kann Untersuchungen in Form von Auditierungen nach Artikel 58 Absatz 8 Buchstabe b der Verordnung (EU) 2019/881 bei Konformitätsbewertungsstellen, denen eine Befugnis nach Absatz 2 erteilt wurde, bei Inhabern europäischer Cybersicherheitszertifikate und bei Ausstellern von EU-Konformitätserklärungen im Sinne von Artikel 56 Absatz 8 der Verordnung (EU) 2019/881 durchführen, um die Einhaltung der Bestimmungen des Titels III der Verordnung (EU) 2019/881 zu überprüfen. § 3 Absatz 1 Satz 1 bis 3 des Akkreditierungsstellengesetzes gilt entsprechend.	(4) Das Bundesamt kann Untersuchungen in Form von Auditierungen nach Artikel 58 Absatz 8 Buchstabe b der Verordnung (EU) 2019/881 bei Konformitätsbewertungsstellen, denen eine Befugnis nach Absatz 2 erteilt wurde, bei Inhabern europäischer Cybersicherheitszertifikate und bei Ausstellern von EU-Konformitätserklärungen im Sinne von Artikel 56 Absatz 8 der Verordnung (EU) 2019/881 durchführen, um die Einhaltung der Bestimmungen des Titels III der Verordnung (EU) 2019/881 zu überprüfen. § 3 Absatz 1 Satz 1 bis 3 des Akkreditierungsstellengesetzes gilt entsprechend.	
736	(5) Das Bundesamt ist befugt, Betriebsstätten, Geschäfts- und Betriebsräume von Konformitätsbewertungsstellen, denen eine Befugnis nach Absatz 2 erteilt wurde, und von Inhabern europäischer Cybersicherheitszertifikate im Sinne von Artikel 56 Absatz 8 der Verordnung (EU) 2019/881 in den Zeiten, zu denen die Räume normalerweise für die jeweilige geschäftliche oder betriebliche Nutzung zur Verfügung stehen, zu betreten, zu besichtigen und zu prüfen, soweit dies zur Erfüllung seiner Aufgaben nach Artikel 58 Absatz 7 der Verordnung (EU) 2019/881 sowie nach § 9 dieses Gesetzes erforderlich ist. § 3 Absatz 1 Satz 1 bis 3 des Akkreditierungsstellengesetzes gilt entsprechend.	(5) Das Bundesamt ist befugt, Betriebsstätten, Geschäfts- und Betriebsräume von Konformitätsbewertungsstellen, denen eine Befugnis nach Absatz 2 erteilt wurde, und von Inhabern europäischer Cybersicherheitszertifikate im Sinne von Artikel 56 Absatz 8 der Verordnung (EU) 2019/881 in den Zeiten, zu denen die Räume normalerweise für die jeweilige geschäftliche oder betriebliche Nutzung zur Verfügung stehen, zu betreten, zu besichtigen und zu prüfen, soweit dies zur Erfüllung seiner Aufgaben nach Artikel 58 Absatz 7 der Verordnung (EU) 2019/881 sowie nach § 54 dieses Gesetzes erforderlich ist. § 3 Absatz 1 Satz 1 bis 3 des Akkreditierungsstellengesetzes gilt entsprechend.	
737	(6) Das Bundesamt kann von ihm ausgestellte Cybersicherheitszertifikate oder durch eine Konformitätsbewertungsstelle, der eine Befugnis nach	(6) Das Bundesamt kann von ihm ausgestellte Cybersicherheitszertifikate oder durch eine Konformitätsbewertungsstelle, der eine Befugnis nach	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Absatz 2 erteilt wurde, nach Artikel 56 Absatz 6 der Verordnung (EU) 2019/881 ausgestellte Cybersicherheitszertifikate widerrufen oder EU-Konformitätserklärungen im Sinne der Verordnung (EU) 2019/881 für ungültig erklären,	Absatz 2 erteilt wurde, nach Artikel 56 Absatz 6 der Verordnung (EU) 2019/881 ausgestellte Cybersicherheitszertifikate widerrufen oder EU-Konformitätserklärungen im Sinne der Verordnung (EU) 2019/881 für ungültig erklären,	
738	1. sofern diese Zertifikate oder EU-Konformitätserklärungen die Anforderungen nach der Verordnung (EU) 2019/881 oder eines europäischen Schemas für die Cybersicherheitszertifizierung nach Artikel 54 der Verordnung (EU) 2019/881 nicht erfüllen oder	1. sofern diese Zertifikate oder EU-Konformitätserklärungen die Anforderungen nach der Verordnung (EU) 2019/881 oder eines europäischen Schemas für die Cybersicherheitszertifizierung nach Artikel 54 der Verordnung (EU) 2019/881 nicht erfüllen oder	
739	2. wenn das Bundesamt die Erfüllung nach Nummer 1 nicht feststellen kann, weil der Inhaber des europäischen Cybersicherheitszertifikats oder der Aussteller der EU-Konformitätserklärung seinen Mitwirkungspflichten nach Absatz 3 nicht nachgekommen ist oder weil dieser das Bundesamt bei der Wahrnehmung seiner Befugnisse nach Absatz 4 oder im Falle eines Inhabers eines europäischen Cybersicherheitszertifikats auch nach Absatz 5 behindert hat.	2. wenn das Bundesamt die Erfüllung nach Nummer 1 nicht feststellen kann, weil der Inhaber des europäischen Cybersicherheitszertifikats oder der Aussteller der EU-Konformitätserklärung seinen Mitwirkungspflichten nach Absatz 3 nicht nachgekommen ist oder weil dieser das Bundesamt bei der Wahrnehmung seiner Befugnisse nach Absatz 4 oder im Falle eines Inhabers eines europäischen Cybersicherheitszertifikats auch nach Absatz 5 behindert hat.	
740	(7) Das Bundesamt kann von ihm erteilte Befugnisse nach Absatz 2 widerrufen,	(7) Das Bundesamt kann von ihm erteilte Befugnisse nach Absatz 2 widerrufen,	
741	1. sofern die Voraussetzungen des maßgeblichen europäischen Schemas für die Cybersicherheitszertifizierung nach Artikel 54 Verordnung (EU) 2019/881 oder des § 9 dieses Gesetzes nicht erfüllt sind oder	1. sofern die Voraussetzungen des maßgeblichen europäischen Schemas für die Cybersicherheitszertifizierung nach Artikel 54 Verordnung (EU) 2019/881 oder des § 54 dieses Gesetzes nicht erfüllt sind oder	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
742	2. wenn das Bundesamt die Erfüllung dieser Voraussetzungen nicht feststellen kann, weil die Konformitätsbewertungsstelle ihren Mitwirkungspflichten nach Absatz 3 nicht nachgekommen ist oder weil diese das Bundesamt bei der Wahrnehmung seiner Befugnisse nach den Absätzen 4 und 5 behindert hat.	2. wenn das Bundesamt die Erfüllung dieser Voraussetzungen nicht feststellen kann, weil die Konformitätsbewertungsstelle ihren Mitwirkungspflichten nach Absatz 3 nicht nachgekommen ist oder weil diese das Bundesamt bei der Wahrnehmung seiner Befugnisse nach den Absätzen 4 und 5 behindert hat.	
743	§ 9b Untersagung des Einsatzes kritischer Komponenten		Verschoben nach § 39 nF.
744	(1) Der Betreiber einer Kritischen Infrastruktur hat den geplanten erstmaligen Einsatz einer kritischen Komponente gemäß § 2 Absatz 13 dem Bundesministerium des Innern, für Bau und Heimat vor ihrem Einsatz anzuzeigen. In der Anzeige sind die kritische Komponente und die geplante Art ihres Einsatzes anzugeben. Satz 1 gilt für einen Betreiber einer Kritischen Infrastruktur nicht, wenn dieser den Einsatz einer anderen kritischen Komponente desselben Typs für dieselbe Art des Einsatzes bereits nach Satz 1 angezeigt hat und ihm dieser nicht untersagt wurde.		s.o.
745	(2) Das Bundesministerium des Innern, für Bau und Heimat kann den geplanten erstmaligen Einsatz einer kritischen Komponente gegenüber dem Betreiber der Kritischen Infrastruktur im Benehmen mit den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt bis zum Ablauf von zwei Monaten nach Eingang der Anzeige nach Absatz 1 untersagen oder Anordnungen erlassen, wenn der Einsatz die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt. Bei der Prüfung einer voraussichtlichen Beeinträchtigung der öffentlichen Ordnung oder		s.o.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Sicherheit kann insbesondere berücksichtigt werden, ob		
746	1. der Hersteller unmittelbar oder mittelbar von der Regierung, einschließlich sonstiger staatlicher Stellen oder Streitkräfte, eines Drittstaates kontrolliert wird,		s.o.
747	2. der Hersteller bereits an Aktivitäten beteiligt war oder ist, die nachteilige Auswirkungen auf die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland oder eines anderen Mitgliedstaates der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages oder auf deren Einrichtungen hatten, oder		s.o.
748	3. der Einsatz der kritischen Komponente im Einklang mit den sicherheitspolitischen Zielen der Bundesrepublik Deutschland, der Europäischen Union oder des Nordatlantikvertrages steht.		s.o.
749	Vor Ablauf der Frist von zwei Monaten nach Anzeige nach Absatz 1 ist der Einsatz nicht gestattet. Das Bundesministerium des Innern, für Bau und Heimat kann die Frist gegenüber dem Betreiber um weitere zwei Monate verlängern, wenn die Prüfung besondere Schwierigkeiten tatsächlicher oder rechtlicher Art aufweist.		s.o.
750	(3) Kritische Komponenten gemäß § 2 Absatz 13 dürfen nur eingesetzt werden, wenn der Hersteller eine Erklärung über seine Vertrauenswürdigkeit (Garantieerklärung) gegenüber dem Betreiber der Kritischen Infrastruktur abgeben hat. Die Garantieerklärung ist der Anzeige nach Absatz 1		s.o.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	beizufügen. Aus der Garantieerklärung muss hervorgehen, wie der Hersteller sicherstellt, dass die kritische Komponente nicht über technische Eigenschaften verfügt, die spezifisch geeignet sind, missbräuchlich, insbesondere zum Zwecke von Sabotage, Spionage oder Terrorismus auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können. Das Bundesministerium des Innern, für Bau und Heimat legt die Einzelheiten der Mindestanforderungen an die Garantieerklärung im Einvernehmen mit den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt durch Allgemeinverfügung fest, die im Bundesanzeiger bekannt zu machen ist. Die Einzelheiten der Mindestanforderungen an die Garantieerklärung müssen aus den Schutzzielen der Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur folgen und die Vermeidung von Gefahren für die öffentliche Sicherheit und Ordnung, insbesondere im Sinne von Absatz 2 Satz 2, adressieren, die aus der Sphäre des Herstellers der kritischen Komponente, insbesondere dessen Organisationsstruktur, stammen. Die Sätze 1 und 2 gelten erst ab der Bekanntmachung der Allgemeinverfügung nach Satz 5 und nicht für bereits vor diesem Zeitpunkt eingesetzte kritische Komponenten. Soweit Änderungen der Allgemeinverfügung erfolgen, sind diese für bereits nach diesem Absatz abgegebene Garantieerklärungen unbeachtlich.		
751	(4) Das Bundesministerium des Innern, für Bau und Heimat kann den weiteren Einsatz einer kritischen Komponente gegenüber dem Betreiber der Kritischen Infrastruktur im Einvernehmen mit den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt untersagen oder Anordnungen		s.o.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	erlassen, wenn der weitere Einsatz die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt, insbesondere, wenn der Hersteller der kritischen Komponente nicht vertrauenswürdig ist. Absatz 2 Satz 2 gilt entsprechend.		
752	(5) Ein Hersteller einer kritischen Komponente kann insbesondere dann nicht vertrauenswürdig sein, wenn hinreichende Anhaltspunkte dafür bestehen, dass		s.o.
753	1. er gegen die in der Garantieerklärung eingegangen Verpflichtungen verstoßen hat,		s.o.
754	2. in der Garantieerklärung angegebene Tatsachenbehauptungen unwahr sind,		s.o.
755	3. er Sicherheitsüberprüfungen und Penetrationsanalysen an seinem Produkt und in der Produktionsumgebung nicht im erforderlichen Umfang in angemessener Weise unterstützt,		s.o.
756	4. Schwachstellen oder Manipulationen nicht unverzüglich, nachdem er davon Kenntnis erlangt, beseitigt und dem Betreiber der Kritischen Infrastruktur meldet,		s.o.
757	5. die kritische Komponente auf Grund von Mängeln ein erhöhtes Gefährdungspotenzial aufweist oder aufgewiesen hat, missbräuchlich auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können oder		s.o.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
758	6. die kritische Komponente über technische Eigenschaften verfügt oder verfügt hat, die spezifisch geeignet sind oder waren, missbräuchlich auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können.		s.o.
759	(6) Wurde nach Absatz 4 der weitere Einsatz einer kritischen Komponente untersagt, kann das Bundesministerium des Innern, für Bau und Heimat im Einvernehmen mit den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt		s.o.
760	1. den geplanten Einsatz weiterer kritischer Komponenten desselben Typs und desselben Herstellers untersagen und		s.o.
761	2. den weiteren Einsatz kritischer Komponenten desselben Typs und desselben Herstellers unter Einräumung einer angemessenen Frist untersagen.		s.o.
762	(7) Bei schwerwiegenden Fällen nicht vorliegender Vertrauenswürdigkeit nach Absatz 5 kann das Bundesministerium des Innern, für Bau und Heimat den Einsatz aller kritischen Komponenten des Herstellers im Einvernehmen mit den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt untersagen.		s.o.
763	§ 9c Freiwilliges IT-Sicherheitskennzeichen	§ 56 Freiwilliges IT-Sicherheitskennzeichen	Neue Enummerierung
764	(1) Das Bundesamt führt zur Information von Verbrauchern über die IT-Sicherheit von Produkten bestimmter vom Bundesamt festgelegter	(1) Das Bundesamt führt zur Information von Verbrauchern über die IT-Sicherheit von Produkten bestimmter vom Bundesamt festgelegter	(unverändert)

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Produktkategorien ein einheitliches IT-Sicherheitskennzeichen ein. Das IT-Sicherheitskennzeichen trifft keine Aussage über die den Datenschutz betreffenden Eigenschaften eines Produktes.	Produktkategorien ein einheitliches IT-Sicherheitskennzeichen ein. Das IT-Sicherheitskennzeichen trifft keine Aussage über die den Datenschutz betreffenden Eigenschaften eines Produktes.	
765	(2) Das IT-Sicherheitskennzeichen besteht aus	(2) Das IT-Sicherheitskennzeichen besteht aus	(unverändert)
766	1. einer Zusicherung des Herstellers oder Diensteanbieters, dass das Produkt für eine festgelegte Dauer bestimmte IT-Sicherheitsanforderungen erfüllt (Herstellererklärung), und	1. einer Zusicherung des Herstellers oder Diensteanbieters, dass das Produkt für eine festgelegte Dauer bestimmte IT-Sicherheitsanforderungen erfüllt (Herstellererklärung), und	(unverändert)
767	2. einer Information des Bundesamtes über sicherheitsrelevante IT-Eigenschaften des Produktes (Sicherheitsinformation).	2. einer Information des Bundesamtes über sicherheitsrelevante IT-Eigenschaften des Produktes (Sicherheitsinformation).	(unverändert)
768	(3) Die IT-Sicherheitsanforderungen, auf die sich die Herstellererklärung bezieht, ergeben sich aus einer Norm oder einem Standard oder aus einer branchenabgestimmten IT-Sicherheitsvorgabe, die die jeweilige Produktkategorie umfasst, sofern das Bundesamt in einem Verfahren, das durch Rechtsverordnung nach § 10 Absatz 3 geregelt wird, festgestellt hat, dass die Norm oder der Standard oder die branchenabgestimmte IT-Sicherheitsvorgabe geeignet ist, ausreichende IT-Sicherheitsanforderungen für die Produktkategorie abzubilden. Ein Anspruch auf diese Feststellung besteht nicht. Liegt keine Feststellung nach Satz 1 vor, ergeben sich die IT-Sicherheitsvorgaben aus einer vom Bundesamt veröffentlichten Technischen Richtlinie, die die jeweilige Produktkategorie umfasst, sofern das Bundesamt eine solche Richtlinie bereits veröffentlicht hat. Wird ein Produkt von mehr als einer oder einem bestehenden, als geeignet festgestellten Norm,	(3) Die IT-Sicherheitsanforderungen, auf die sich die Herstellererklärung bezieht, ergeben sich aus einer Norm oder einem Standard oder aus einer branchenabgestimmten IT-Sicherheitsvorgabe, die die jeweilige Produktkategorie umfasst, sofern das Bundesamt in einem Verfahren, das durch Rechtsverordnung nach § 57 Absatz 3 geregelt wird, festgestellt hat, dass die Norm oder der Standard oder die branchenabgestimmte IT-Sicherheitsvorgabe geeignet ist, ausreichende IT-Sicherheitsanforderungen für die Produktkategorie abzubilden. Ein Anspruch auf diese Feststellung besteht nicht. Liegt keine Feststellung nach Satz 1 vor, ergeben sich die IT-Sicherheitsvorgaben aus einer vom Bundesamt veröffentlichten Technischen Richtlinie, die die jeweilige Produktkategorie umfasst, sofern das Bundesamt eine solche Richtlinie bereits veröffentlicht hat. Wird ein Produkt von mehr als einer oder einem bestehenden, als geeignet festgestellten Norm,	Anpassung des Verweises.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Standard, branchenabgestimmten IT-Sicherheitsvorgabe oder Technischen Richtlinie umfasst, richten sich die Anforderungen nach der oder dem jeweils spezielleren bestehenden, als geeignet festgestellten Norm, Standard, branchenabgestimmten IT-Sicherheitsvorgabe oder Technischen Richtlinie.	Standard, branchenabgestimmten IT-Sicherheitsvorgabe oder Technischen Richtlinie umfasst, richten sich die Anforderungen nach der oder dem jeweils spezielleren bestehenden, als geeignet festgestellten Norm, Standard, branchenabgestimmten IT-Sicherheitsvorgabe oder Technischen Richtlinie.	
769	(4) Das IT-Sicherheitskennzeichen darf nur dann für ein Produkt verwendet werden, wenn das Bundesamt das IT-Sicherheitskennzeichen für dieses Produkt freigegeben hat. Das Bundesamt prüft die Freigabe des IT-Sicherheitskennzeichens für ein Produkt auf Antrag des Herstellers oder Diensteanbieters. Dem Antrag sind die Herstellererklärung zu dem Produkt sowie alle Unterlagen beizufügen, die die Angaben in der Herstellererklärung belegen. Das Bundesamt bestätigt den Eingang des Antrags und prüft die Plausibilität der Herstellererklärung anhand der beigefügten Unterlagen. Die Plausibilitätsprüfung kann auch durch einen vom Bundesamt beauftragten qualifizierten Dritten erfolgen. Für die Antragsbearbeitung kann das Bundesamt eine Verwaltungsgebühr erheben.	(4) Das IT-Sicherheitskennzeichen darf nur dann für ein Produkt verwendet werden, wenn das Bundesamt das IT-Sicherheitskennzeichen für dieses Produkt freigegeben hat. Das Bundesamt prüft die Freigabe des IT-Sicherheitskennzeichens für ein Produkt auf Antrag des Herstellers oder Diensteanbieters. Dem Antrag sind die Herstellererklärung zu dem Produkt sowie alle Unterlagen beizufügen, die die Angaben in der Herstellererklärung belegen. Das Bundesamt bestätigt den Eingang des Antrags und prüft die Plausibilität der Herstellererklärung anhand der beigefügten Unterlagen. Die Plausibilitätsprüfung kann auch durch einen vom Bundesamt beauftragten qualifizierten Dritten erfolgen. Für die Antragsbearbeitung kann das Bundesamt eine Verwaltungsgebühr erheben.	(unverändert)
770	(5) Das Bundesamt erteilt die Freigabe des IT-Sicherheitskennzeichens für das jeweilige Produkt, wenn	(5) Das Bundesamt erteilt die Freigabe des IT-Sicherheitskennzeichens für das jeweilige Produkt, wenn	(unverändert)
771	1. das Produkt zu einer der Produktkategorien gehört, die das Bundesamt durch im Bundesanzeiger veröffentlichte Allgemeinverfügung bekannt gegeben hat,	1. das Produkt zu einer der Produktkategorien gehört, die das Bundesamt durch im Bundesanzeiger veröffentlichte Allgemeinverfügung bekannt gegeben hat,	(unverändert)
772	2. die Herstellererklärung plausibel und durch die beigefügten Unterlagen ausreichend belegt ist und	2. die Herstellererklärung plausibel und durch die beigefügten Unterlagen ausreichend belegt ist und	(unverändert)

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
773	3. die gegebenenfalls erhobene Verwaltungsgebühr beglichen wurde.	3. die gegebenenfalls erhobene Verwaltungsgebühr beglichen wurde.	(unverändert)
774	Die Erteilung der Freigabe erfolgt schriftlich und innerhalb einer angemessenen Frist, die in der Rechtsverordnung nach § 10 Absatz 3 bestimmt wird. Den genauen Ablauf des Antragsverfahrens und die beizufügenden Unterlagen regelt die Rechtsverordnung nach § 10 Absatz 3.	Die Erteilung der Freigabe erfolgt schriftlich und innerhalb einer angemessenen Frist, die in der Rechtsverordnung nach § 57 Absatz 3 bestimmt wird. Den genauen Ablauf des Antragsverfahrens und die beizufügenden Unterlagen regelt die Rechtsverordnung nach § 57 Absatz 3.	Anpassung des Verweises.
775	(6) Hat das Bundesamt die Freigabe erteilt, ist das Etikett des IT-Sicherheitskennzeichens auf dem jeweiligen Produkt oder auf dessen Umverpackung anzubringen, sofern dies nach der Beschaffenheit des Produktes möglich ist. Das IT-Sicherheitskennzeichen kann auch elektronisch veröffentlicht werden. Wenn nach der Beschaffenheit des Produktes das Anbringen nicht möglich ist, muss die Veröffentlichung des IT-Sicherheitskennzeichens elektronisch erfolgen. Das Etikett des IT-Sicherheitskennzeichens verweist auf eine Internetseite des Bundesamtes, auf der die Herstellererklärung und die Sicherheitsinformationen abrufbar sind. Das genaue Verfahren und die Gestaltung des Verweises sind in der Rechtsverordnung nach § 10 Absatz 3 festzulegen.	(6) Hat das Bundesamt die Freigabe erteilt, ist das Etikett des IT-Sicherheitskennzeichens auf dem jeweiligen Produkt oder auf dessen Umverpackung anzubringen, sofern dies nach der Beschaffenheit des Produktes möglich ist. Das IT-Sicherheitskennzeichen kann auch elektronisch veröffentlicht werden. Wenn nach der Beschaffenheit des Produktes das Anbringen nicht möglich ist, muss die Veröffentlichung des IT-Sicherheitskennzeichens elektronisch erfolgen. Das Etikett des IT-Sicherheitskennzeichens verweist auf eine Internetseite des Bundesamtes, auf der die Herstellererklärung und die Sicherheitsinformationen abrufbar sind. Das genaue Verfahren und die Gestaltung des Verweises sind in der Rechtsverordnung nach § 57 Absatz 3 festzulegen.	Anpassung des Verweises.
776	(7) Nach Ablauf der festgelegten Dauer nach Absatz 3 Satz 5 oder 6 oder nach Rücknahmeerklärung des Herstellers oder Diensteanbieters gegenüber dem Bundesamt erlischt die Freigabe. Das Bundesamt nimmt einen Hinweis auf das Erlöschen der Freigabe in die Sicherheitsinformation auf.	(7) Nach Ablauf der festgelegten Dauer nach Absatz 3 Satz 5 oder 6 oder nach Rücknahmeerklärung des Herstellers oder Diensteanbieters gegenüber dem Bundesamt erlischt die Freigabe. Das Bundesamt nimmt einen Hinweis auf das Erlöschen der Freigabe in die Sicherheitsinformation auf.	(unverändert)
777	(8) Das Bundesamt kann prüfen, ob die Anforderungen an die Freigabe des IT-Sicherheitskennzeichens für ein Produkt eingehalten werden. Werden bei der Prüfung Abweichungen von der abgegebenen Herstellererklärung oder Sicherheitslücken festgestellt, kann das Bundesamt die	(8) Das Bundesamt kann prüfen, ob die Anforderungen an die Freigabe des IT-Sicherheitskennzeichens für ein Produkt eingehalten werden. Werden bei der Prüfung Abweichungen von der abgegebenen Herstellererklärung oder Schwachstellen festgestellt, kann das Bundesamt die	Redaktionelle Änderung von „Sicherheitslücke“ auf „Schwachstelle“.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	geeigneten Maßnahmen zum Schutz des Vertrauens der Verbraucher in das IT-Sicherheitskennzeichen treffen, insbesondere	geeigneten Maßnahmen zum Schutz des Vertrauens der Verbraucher in das IT-Sicherheitskennzeichen treffen, insbesondere	
778	1. Informationen über die Abweichungen oder Sicherheitslücken in geeigneter Weise in der Sicherheitsinformation veröffentlichen oder	1. Informationen über die Abweichungen oder Schwachstellen in geeigneter Weise in der Sicherheitsinformation veröffentlichen oder	(unverändert)
779	2. die Freigabe des IT-Sicherheitskennzeichens widerrufen.	2. die Freigabe des IT-Sicherheitskennzeichens widerrufen.	(unverändert)
780	Absatz 7 Satz 2 gilt entsprechend.	Absatz 7 Satz 2 gilt entsprechend.	(unverändert)
781	(9) Bevor das Bundesamt eine Maßnahme nach Absatz 8 trifft, räumt es dem Hersteller oder Diensteanbieter Gelegenheit ein, die festgestellten Abweichungen oder Sicherheitslücken innerhalb eines angemessenen Zeitraumes zu beseitigen, es sei denn, gewichtige Gründe der Sicherheit der Produkte erfordern eine sofortige Maßnahme. Die Befugnis des Bundesamtes zur Warnung nach § 7 bleibt davon unberührt.	(9) Bevor das Bundesamt eine Maßnahme nach Absatz 8 trifft, räumt es dem Hersteller oder Diensteanbieter Gelegenheit ein, die festgestellten Abweichungen oder Schwachstellen innerhalb eines angemessenen Zeitraumes zu beseitigen, es sei denn, gewichtige Gründe der Sicherheit der Produkte erfordern eine sofortige Maßnahme. Die Befugnis des Bundesamtes zur Warnung nach § 13 bleibt davon unberührt.	Redaktionelle Änderung von „Sicherheitslücke“ auf „Schwachstelle“; Anpassung des Verweises..
782		Teil 6 Verordnungsermächtigungen, Grundrechtseinschränkungen, Rat der IT Beauftragten und Berichtspflichten	Neue Gliederung zur Steigerung der Übersichtlichkeit
783	§ 10 Ermächtigung zum Erlass von Rechtsverordnungen	§ 57 Ermächtigung zum Erlass von Rechtsverordnungen	
784	(1) Das Bundesministerium des Innern, für Bau und Heimat bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem	(1) Das Bundesministerium des Innern und für Heimat bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber, Einrichtungen und der betroffenen Wirtschaftsverbände im Einvernehmen mit	Die Ermächtigung zum Erlass einer neuen BSI-KritisV wird aufgrund von Artikel 6 und 1b bereits kurz nach Verkündung in Kraft treten. Die wortgleiche Vorschrift in Artikel 1a wird mit Inkrafttreten des Artikels 1 lediglich

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr und digitale Infrastruktur, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit unter Festlegung der in den jeweiligen Sektoren im Hinblick auf § 2 Absatz 10 Satz 1 Nummer 2 wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrads, welche Einrichtungen, Anlagen oder Teile davon als Kritische Infrastrukturen im Sinne dieses Gesetzes gelten. Der nach Satz 1 als bedeutend anzusehende Versorgungsgrad ist anhand von branchenspezifischen Schwellenwerten für jede wegen ihrer Bedeutung als kritisch anzusehende Dienstleistung im jeweiligen Sektor zu bestimmen. Zugang zu Akten, die die Erstellung oder Änderung dieser Verordnung betreffen, wird nicht gewährt.	dem Bundesministerium für Wirtschaft und Klimaschutz, dem Bundesministerium der Justiz, dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Digitales und Verkehr, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz	der neue Absatz 1 und die mit Artikel 1a eingeführten Absätze 1a und 1b entfallen. [*Anm. BMI CI1 – Diese Vorschrift (§ 10 BSIG aF.) ist Gegenstand der Evaluierung gemäß Art. 6 Abs. 1 Nr. 1 Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 18. Mai 2021 (BGBl. I S. 1122). Diese Änderung erfolgt vorbehaltlich der Ergebnisse dieser Evaluierung und wird gegebenenfalls noch auf deren Grundlage angepasst.*]
785		1. unter Festlegung der in den jeweiligen Sektoren Energie, Transport und Verkehr, Bankwesen, Finanzmarktinfrastrukutren, Gesundheitswesen, Trinkwasser, Abwasser, Ernährung, digitale Infrastruktur, sowie Siedlungsabfallentsorgung im Hinblick auf § 28 Absatz 2a wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrads, welche Anlagen oder Teile davon als kritische Anlagen im Sinne dieses Gesetzes gelten,	
786		2. sowie welche Einrichtungsarten in den Sektoren Energie, Transport und Verkehr,	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, digitale Infrastruktur, Verwaltung von IKT-Diensten (Business-to-Business), öffentliche Verwaltung und Weltraum Einrichtungsarten besonders wichtiger Einrichtungen sind, und	
787		3. welche Einrichtungsarten in den Sektoren Energie, Transport und Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, digitale Infrastruktur, Siedlungsabfallentsorgung, Logistik, Produktion, Chemie, Ernährung, verarbeitendes Gewerbe, Anbieter digitaler Dienste oder Forschung Einrichtungsarten wichtiger Einrichtungen sind.	
788		Der nach Satz 1 als bedeutend anzusehende Versorgungsgrad ist anhand von branchenspezifischen Schwellenwerten für jede wegen ihrer Bedeutung als kritisch anzusehende Dienstleistung im jeweiligen Sektor zu bestimmen. Zugang zu Akten, die die Erstellung oder Änderung dieser Verordnung betreffen, wird nicht gewährt.	
789	(2) Das Bundesministerium des Innern, für Bau und Heimat bestimmt nach Anhörung der betroffenen Wirtschaftsverbände und im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, das Nähere über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen nach § 9 und deren Inhalt.	(2) Das Bundesministerium des Innern und für Heimat bestimmt nach Anhörung der betroffenen Wirtschaftsverbände und im Einvernehmen mit dem Bundesministerium für Wirtschaft und Klimaschutz durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, das Nähere über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen nach § 54 und deren Inhalt.	Redaktionelle Änderung
790	(3) Das Bundesministerium des Innern, für Bau und Heimat bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung der betroffenen Wirtschaftsverbände im	(3) Das Bundesministerium des Innern und für Heimat bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung der betroffenen Wirtschaftsverbände im	Redaktionelle Änderung

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie und dem Bundesministerium der Justiz und für Verbraucherschutz die Einzelheiten der Gestaltung, des Inhalts und der Verwendung des IT-Sicherheitskennzeichens nach § 9c, um eine einheitliche Gestaltung des Kennzeichens und eine eindeutige Erkennbarkeit der gekennzeichneten informationstechnischen Produkte zu gewährleisten, sowie die Einzelheiten des Verfahrens zur Feststellung der Eignung branchenabgestimmter IT-Sicherheitsvorgaben und des Antragsverfahrens auf Freigabe einschließlich der diesbezüglichen Fristen und der beizufügenden Unterlagen sowie das Verfahren und die Gestaltung des Verweises auf Sicherheitsinformationen.	Einvernehmen mit dem Bundesministerium für Wirtschaft und Klimaschutz und dem Bundesministerium der Justiz die Einzelheiten der Gestaltung, des Inhalts und der Verwendung des IT-Sicherheitskennzeichens nach § 52, um eine einheitliche Gestaltung des Kennzeichens und eine eindeutige Erkennbarkeit der gekennzeichneten informationstechnischen Produkte zu gewährleisten, sowie die Einzelheiten des Verfahrens zur Feststellung der Eignung branchenabgestimmter IT-Sicherheitsvorgaben und des Antragsverfahrens auf Freigabe einschließlich der diesbezüglichen Fristen und der beizufügenden Unterlagen sowie das Verfahren und die Gestaltung des Verweises auf Sicherheitsinformationen.	
791	(4) Soweit die Durchführungsrechtsakte der Kommission nach Artikel 16 Absatz 8 und 9 der Richtlinie (EU) 2016/1148 keine abschließenden Bestimmungen über die von Anbietern digitaler Dienste nach § 8c Absatz 2 zu treffenden Maßnahmen oder über die Parameter zur Beurteilung der Erheblichkeit der Auswirkungen von Sicherheitsvorfällen nach § 8c Absatz 3 Satz 2 oder über Form und Verfahren der Meldungen nach § 8c Absatz 3 Satz 4 enthalten, werden diese Bestimmungen vom Bundesministerium des Innern, für Bau und Heimat im Einvernehmen mit den jeweils betroffenen Ressorts durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, getroffen.		Entfällt. Die in Umsetzung der (ersten) NIS-Richtlinie eingeführte Vorschrift hatte keine praktische Relevanz.
792	(5) Das Bundesministerium des Innern, für Bau und Heimat bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung von Vertretern der Wissenschaft, der betroffenen Unternehmen und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie, dem		Entfällt. Unternehmen im öffentlichen Interesse (UBI) gehen in die neue Einrichtungskategorie Wichtige Einrichtungen auf.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr und digitale Infrastruktur, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit, welche wirtschaftlichen Kennzahlen bei der Berechnung der inländischen Wertschöpfung heranzuziehen sind, wie die Berechnung mit Hilfe der Methodik der direkten Wertschöpfungsstaffel zu erfolgen hat und welche Schwellenwerte maßgeblich dafür sind, dass ein Unternehmen zu den größten Unternehmen in Deutschland im Sinne des § 2 Absatz 14 Satz 1 Nummer 2 gehört. Unter den Voraussetzungen nach Satz 1 kann das Bundesministerium des Innern, für Bau und Heimat durch Rechtsverordnung bestimmen, welche Alleinstellungsmerkmale maßgeblich dafür sind, dass Zulieferer für Unternehmen, die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören, von wesentlicher Bedeutung im Sinne des § 2 Absatz 14 Satz 1 Nummer 2 sind.		
793		(4) Das Bundesministerium des Innern und Heimat bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung von Vertretern der Wissenschaft, der betroffenen Einrichtungen und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Klimaschutz, dem Bundesministerium der Justiz, dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Digitales und Verkehr, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz, nukleare	Umsetzung Art. 24 NIS-2.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		Sicherheit und Verbraucherschutz welche durch eine besonders wichtige Einrichtung oder wichtige Einrichtung eingesetzten Produkte, Dienste oder Prozesse gemäß § 30 Absatz 9 über eine Cybersicherheitszertifizierung verfügen müssen.	
794	§ 11 Einschränkung von Grundrechten	§ 58 Einschränkung von Grundrechten	Neue Enummerierung
795	Das Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) wird durch die §§ 4a, 5 bis 5c, 7b und 7c eingeschränkt.	Das Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) wird durch die §§ 7, 8, 9, 11, 12 , 15 und 16 eingeschränkt. Die Berufsfreiheit (Artikel 12 des Grundgesetzes) wird durch § 64 eingeschränkt.	[*Anm. CI 1 – Die Prüfung sämtlicher neuer Vorschriften im Hinblick auf das Zitiergebot ist noch nicht abgeschlossen.*]
796	§ 12 Rat der IT-Beauftragten der Bundesregierung		Neue Enummerierung
797	Wird der Rat der IT-Beauftragten der Bundesregierung aufgelöst, tritt an dessen Stelle die von der Bundesregierung bestimmte Nachfolgeorganisation. Die Zustimmung des Rats der IT-Beauftragten kann durch Einvernehmen aller Bundesministerien ersetzt werden. Wird der Rat der IT-Beauftragten ersatzlos aufgelöst, tritt an Stelle seiner Zustimmung das Einvernehmen aller Bundesministerien.		Gestrichen als Folgeänderung: Die Bezugnahmen auf den IT-Rat in § 4 Abs. 6 aF sowie § 5 Abs. 8 aF wurden aus dem Gesetz entfernt, die Gremienstruktur der IT-Steuerung beruht auf untergesetzlichen Festlegungen.
798	§ 13 Berichtspflichten	§ 59Berichtspflichten des Bundesamtes	Neue Enummerierung; klarstellende Ergänzung in der Überschrift, dass Berichtspflichten sich steht auf das Bundesamt beziehen. Im Gegensatz dazu beziehen sich Meldepflichten stets auf Einrichtungen.
799	(1) Das Bundesamt unterrichtet das Bundesministerium des Innern, für Bau und Heimat über seine Tätigkeit.	(1) Das Bundesamt unterrichtet das Bundesministerium des Innern und für Heimat über seine Tätigkeit.	Redaktionelle Änderung

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
800	(2) Die Unterrichtung nach Absatz 1 dient auch der Aufklärung der Öffentlichkeit durch das Bundesministerium des Innern, für Bau und Heimat über Gefahren für die Sicherheit in der Informationstechnik, die mindestens einmal jährlich in einem zusammenfassenden Bericht erfolgt. § 7 Absatz 1a ist entsprechend anzuwenden.	(2) Die Unterrichtung nach Absatz 1 dient auch der Aufklärung der Öffentlichkeit durch das Bundesministerium des Innern und für Heimat über Gefahren für die Sicherheit in der Informationstechnik, die mindestens einmal jährlich in einem zusammenfassenden Bericht erfolgt. § 12 Absatz 1a ist entsprechend anzuwenden.	Redaktionelle Änderung, Anpassung des Verweises.
801	(3) Das Bundesministerium des Innern, für Bau und Heimat unterrichtet kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres den Ausschuss für Inneres und Heimat des Deutschen Bundestages über die Anwendung dieses Gesetzes. Es geht dabei auch auf die Fortentwicklung des maßgeblichen Unionsrechts ein.	(3) Das Bundesministerium des Innern und für Heimat unterrichtet kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres den Ausschuss für Inneres und Heimat des Deutschen Bundestages über die Anwendung dieses Gesetzes. Es geht dabei auch auf die Fortentwicklung des maßgeblichen Unionsrechts ein.	Redaktionelle Änderung
802	(4) Das Bundesamt übermittelt bis zum 9. November 2018 und danach alle zwei Jahre die folgenden Informationen an die Kommission:	(4) Das Bundesamt übermittelt bis zum 9. November 2018 und danach alle zwei Jahre bis zum 17. Oktober 2024 die folgenden Informationen an die Kommission:	
803	1. die nationalen Maßnahmen zur Ermittlung der Betreiber Kritischer Infrastrukturen;	1. die nationalen Maßnahmen zur Ermittlung der Betreiber kritischer Anlagen;	Folgeänderung aufgrund neuer Einrichtungskategorien
804	2. eine Aufstellung der im in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren, die nach § 2 Absatz 10 Satz 1 Nummer 2 wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrad;	2. eine Aufstellung der im in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren, die in der Rechtsverordnung nach § 57 Absatz 1 wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrad;	Anpassung des Verweises.
805	3. eine zahlenmäßige Aufstellung der Betreiber der in Nummer 2 genannten Sektoren, die in den in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren ermittelt werden, einschließlich	3. eine zahlenmäßige Aufstellung der Einrichtungen der in Nummer 2 genannten Sektoren, die in den in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren ermittelt werden,	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	eines Hinweises auf ihre Bedeutung für den jeweiligen Sektor.	einschließlich eines Hinweises auf ihre Bedeutung für den jeweiligen Sektor.	
806	Die Übermittlung darf keine Informationen enthalten, die zu einer Identifizierung einzelner Betreiber führen können. Das Bundesamt übermittelt die nach Satz 1 übermittelten Informationen unverzüglich dem Bundesministerium des Innern, für Bau und Heimat, dem Bundeskanzleramt, dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr und digitale Infrastruktur, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit.	Die Übermittlung darf keine Informationen enthalten, die zu einer Identifizierung einzelner Betreiber führen können. Das Bundesamt übermittelt die nach Satz 1 übermittelten Informationen unverzüglich dem Bundesministerium des Innern und für Heimat, dem Bundeskanzleramt, dem Bundesministerium für Wirtschaft und Klimaschutz, dem Bundesministerium der Justiz, dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Digitales und Verkehr, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit und Verbraucherschutz.	Redaktionelle Änderungen
807	(5) Sobald bekannt wird, dass eine Einrichtung oder Anlage nach § 2 Absatz 10 oder Teile einer Einrichtung oder Anlage eine wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistung in einem der in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren in einem anderen Mitgliedstaat der Europäischen Union bereitstellt, nimmt das Bundesamt zum Zweck der gemeinsamen Ermittlung der Betreiber, die kritische Dienstleistungen in den in Anhang II der Richtlinie (EU) 2016/1148 genannten Teilsektoren erbringen, mit der zuständigen Behörde dieses Mitgliedstaats Konsultationen auf.	(5) Sobald bekannt wird, dass eine Einrichtung oder Anlage nach § 2 Absatz 1 Nummer 19 oder Teile einer Einrichtung oder Anlage eine wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistung in einem der in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren in einem anderen Mitgliedstaat der Europäischen Union bereitstellt, nimmt das Bundesamt zum Zweck der gemeinsamen Ermittlung der Einrichtungen, die kritische Dienstleistungen in den in Anhang II der Richtlinie (EU) 2016/1148 genannten Teilsektoren erbringen, mit der zuständigen Behörde dieses Mitgliedstaats Konsultationen auf.	
808	(6) Das Bundesamt übermittelt bis zum 9. August 2018 und danach jährlich an die Kooperationsgruppe nach Artikel 11 der Richtlinie (EU) 2016/1148 einen zusammenfassenden Bericht zu den Meldungen, die die in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren oder digitale Dienste betreffen.	(6) Das Bundesamt übermittelt bis zum 9. August 2018 und danach jährlich an die Kooperationsgruppe nach Artikel 11 der Richtlinie (EU) 2016/1148 einen zusammenfassenden Bericht zu den Meldungen, die die in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren oder digitale Dienste betreffen.	Folgeänderung aufgrund geänderter Einrichtungskategorien

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Der Bericht enthält auch die Zahl der Meldungen und die Art der gemeldeten Sicherheitsvorfälle sowie die ergriffenen Maßnahmen. Der Bericht darf keine Informationen enthalten, die zu einer Identifizierung einzelner Meldungen oder einzelner Betreiber oder Anbieter führen können.	Der Bericht enthält auch die Zahl der Meldungen und die Art der gemeldeten Sicherheitsvorfälle sowie die ergriffenen Maßnahmen. Der Bericht darf keine Informationen enthalten, die zu einer Identifizierung einzelner Meldungen oder einzelner Einrichtungen führen können.	
809		(7) Das Bundesamt legt der ENISA erstmalig zum [*einfügen: Datum des zweiten Quartalsbeginns nach Inkrafttreten*] und in der Folge alle drei Monate einen zusammenfassenden Bericht vor, der anonymisierte und aggregierte Daten zu erheblichen Sicherheitsvorfällen, erheblichen Cyberbedrohungen und Beinahevorfällen enthält, die gemäß § 31 und § 5 Absatz 2 gemeldet wurden.	Umsetzung Art. 23 Abs. 9 NIS-2. Für die zu übermittelnden Informationen gelten die Ausnahmen des Art. 2 Abs. 11 (nationale, öffentliche Sicherheit oder Verteidigung) und Abs. 13 (Vertraulichkeit von Geschäftsgeheimnissen). [*Anm. BMI CI 1 – Es ist im Übrigen nicht eindeutig, wann der Bericht erstmalig an ENISA zu erstatten ist und ob dann ein Kalendervierteljahr als Zyklus gemeint ist. Diese Auslegung ist jedoch naheliegend und eine diesbezügliche Abstimmung mit der Kommission ist noch nicht abgeschlossen.*]
810		(8) Das Bundesamt übermittelt erstmalig zum 17. April 2025 und in der Folge alle zwei Jahre	Umsetzung Art. 3 Abs. 5 NIS-2.
811		1. der Kommission und der Kooperationsgruppe für jeden Sektor und Teilsektor gemäß Anhang I oder II der NIS-2-Richtlinie die Anzahl der wesentlichen und wichtigen Einrichtungen, die gemäß § 32 Absatz 1 registriert wurden	Umsetzung Art. 3 Abs. 5 lit. a NIS-2.
812		2. der Kommission sachdienliche Informationen über die Zahl der kritischen Einrichtungen, über den Sektor und den Teilsektor gemäß Anhang I oder II der	Umsetzung Art. 3 Abs. 5 lit. b NIS-2.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		NIS-2-Richtlinie, zu dem sie gehören, über die Art der von ihnen erbrachten Dienste und über die Bestimmungen, auf deren Grundlage sie ermittelt wurden.	
813		Teil 7 Bußgeldvorschriften und Aufsicht	Neue Gliederung zur Steigerung der Übersichtlichkeit
814	§ 14 Bußgeldvorschriften	§ 59 Sanktionsvorschriften	Anpassung der Überschrift, da der § 59 nun auch einen Absatz bzgl. Verwaltungszwangs umfasst
815	(1) Ordnungswidrig handelt, wer entgegen § 8a Absatz 3 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 10 Absatz 1 Satz 1 einen Nachweis nicht richtig oder nicht vollständig erbringt.	(1) Ordnungswidrig handelt, wer entgegen § 34 Absatz 1 Satz 1 in Verbindung mit der Rechtsverordnung nach § 57 Absatz 1 Satz 1 einen Nachweis nicht richtig oder nicht vollständig erbringt.	Anpassung der Verweise: § 8a Absatz 3 Satz 1 betraf die früheren Betreiber kritischer Infrastruktur, sodass hier eine Ersetzung mit dem neu eingeführten Einrichtungsäquivalent der besonders wichtigen Einrichtungen erfolgten musste
816	(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig	(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig	Mit § 59 Absatz 2 Nummer 1 lit. a,b und c werden wie zuvor Fälle von Zuwiderhandlungen gegen vollziehbare Anordnungen erfasst. Die getrennte Aufzählung soll, aufgrund unterschiedlicher Schwere der Zuwiderhandlungen, eine entsprechende Bebußung in unterschiedlicher Höhe ermöglichen.
817	1. einer vollziehbaren Anordnung nach	1. einer vollziehbaren Anordnung nach	
818	a) § 5b Absatz 6, § 7c Absatz 1 Satz 1, auch in Verbindung mit § 7c Absatz 3, § 7d, oder § 8a Absatz 3 Satz 5,	a) § 11 Absatz 6, § 16 Absatz 1 Satz 1, auch in Verbindung mit § 16 Absatz 3, § 17, oder § 34 Absatz 1 Satz 5,	Anpassung der Verweise: § 11 Absatz 6: Mitwirkungspflicht bei Wiederherstellung der Sicherheit oder Funktionsfähigkeit des inf. Systems

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			§ 16 Absatz 1 Satz 1: Maßnahmen zur Abwehr konkreter erheblicher Gefahren § 17 : Ergreifung organisatorischer Maßnahmen § 34 Absatz 1 Satz 5: Beseitigung der Sicherheitsmängel und Vorlage eines geeigneten Mängelbeseitigungsplans
819	b) § 7a Absatz 2 Satz 1 oder	b) § 14 Absatz 2 Satz 1 oder	Anpassung des Verweises
820	c) § 8b Absatz 6 Satz 1, auch in Verbindung mit Satz 2, oder § 8c Absatz 4 Satz 1	c) § 40 Absatz 6 Satz 1, auch in Verbindung mit Satz 2,	Anpassung des Verweises § 8c Absatz 4 Satz 1 entfällt, da die Kategorie „Anbieter digitaler Dienste“ in den neuen Einrichtungskategorien aufgeht
821	zuwiderhandelt,	zuwiderhandelt,	
822	2. entgegen § 8a Absatz 1 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 10 Absatz 1 Satz 1 eine dort genannte Vorkehrung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig trifft,	2. entgegen § 30 Absatz 1 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 57 Absatz 1 Satz 1 eine dort genannte Vorkehrung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig trifft,	Anpassung der Verweise und Aktualisierung entsprechend der Anforderungen der NIS 2: Mit der NIS 2 soll eine Bußgeldbewehrung bei Verstoß gegen die sogenannten Risikomanagementmaßnahmen aus Art. 21 NIS 2 (s. § 30 Absatz 1 BSIG nF) erfolgen
823	3. entgegen § 8a Absatz 3 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 10 Absatz 1 Satz 1 einen Nachweis nicht oder nicht rechtzeitig erbringt,	3. entgegen § 34 Absatz 1 Satz 1 oder § 39 Absatz 2 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 57 Absatz 1 Satz 1 einen Nachweis nicht oder nicht rechtzeitig erbringt,	Anpassung der Verweise und Aktualisierung - Nachweispflichten: Aktualisierung der Nachweispflichten entsprechend der neuen Einrichtungskategorien. Hier bestimmt

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			§ 34 Absatz 1 Satz 1 die Anforderungen für besonders wichtige und wichtige Einrichtungen, § 39 Absatz 2 Satz 1 die für kritische Einrichtungen.
824	4. entgegen § 8a Absatz 4 Satz 2 oder § 8b Absatz 3a das Betreten eines dort genannten Raums nicht gestattet, eine dort genannte Unterlage nicht oder nicht rechtzeitig vorlegt, eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder Unterstützung nicht oder nicht rechtzeitig gewährt,	4. entgegen § 64 Absatz 1 Satz 3 oder § 39 Absatz 3 Satz 2 das Betreten eines dort genannten Raums nicht gestattet, eine dort genannte Unterlage nicht oder nicht rechtzeitig vorlegt, eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder Unterstützung nicht oder nicht rechtzeitig gewährt,	Anpassung der Verweise und Aktualisierung – Zutrittsgestattung: § 59 Absatz 2 Nummer 4 soll gewährleisten, dass Auskunftsverlangen bei Vor-Ort-Kontrollen besser durchgesetzt werden können. § 64 Absatz 1 Satz 3 bestimmt hierbei die Anforderungen für besonders wichtige Einrichtungen, § 39 Absatz 3 Satz 2 die für kritische Einrichtungen.
825	5. entgegen § 8b Absatz 3 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 10 Absatz 1 Satz 1 oder entgegen § 8f Absatz 5 Satz 1 eine Registrierung nicht oder nicht rechtzeitig vornimmt oder eine dort genannte Stelle nicht oder nicht rechtzeitig benennt,	5. entgegen § 32 Absatz 1, 2 in Verbindung mit einer Rechtsverordnung nach § 57 Absatz 1 Satz 1 oder entgegen § 33 Absatz 1, 2 eine Registrierung nicht oder nicht rechtzeitig vornimmt oder eine dort genannte Stelle nicht oder nicht rechtzeitig benennt,	Anpassung der Verweise und Aktualisierung – Registrierungspflichten: § 32 Absatz 1 definiert die Registrierungspflichten für wichtige und besonders wichtige Einrichtungen, Absatz 2 die Anforderungen für kritische Einrichtungen. § 8f Absatz 5 Satz 1 entfällt, da dieser in den neuen Einrichtungskategorien aufgeht. Ein Ersatz erfolgt jedoch durch § 33 Absatz 1, 2, der Registrierungen für andere Einrichtungsarten bestimmt
826	6. entgegen § 8b Absatz 3 Satz 4 nicht sicherstellt, dass er erreichbar ist,	6. entgegen § 32 Absatz 4 Satz 3 nicht sicherstellt, dass er erreichbar ist,	Anpassung des Verweises

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
827		7. entgegen § 32 Absatz 6 Änderungen der nach § 32 zu übermittelnden Angaben nicht unverzüglich, spätestens jedoch bis zwei Wochen ab dem Zeitpunkt der Änderung dem Bundesamt übermittelt	Schaffung eines neuen Bußgeldtatbestandes zur umfassenden Ahndung bei Nichtmitteilung von Änderungen zur besseren Durchsetzbarkeit der Nr. 5
828	7. entgegen § 8b Absatz 4 Satz 1, § 8c Absatz 3 Satz 1 oder § 8f Absatz 7 Satz 1 oder Absatz 8 Satz 1 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,	8. entgegen § 31 Absatz 1, § 40 Absatz 4eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,	Anpassung der Verweise und Aktualisierung – Meldepflichten: Umsetzung der NIS 2: § 31 BSIG nF definiert die Meldepflichten für besonders wichtige und wichtige Einrichtungen (Umsetzung des Art. 23 NIS 2) Ergänzung des Verweises auf § 40 Absatz 4 Satz 1, der die besonderen Anforderungen für Meldepflichten bei kritischen Einrichtungen festsetzt. § 8c und 8f entfallen, da die Regelungsadressaten in in den neuen Einrichtungskategorien aufgehen
829	8. entgegen § 8c Absatz 1 Satz 1 eine dort genannte Maßnahme nicht trifft,	9. entgegen § 40 Absatz 4a Satz 1 die zur Bewältigung der Störung notwendigen Informationen nicht herausgibt,	Streichung des § 8c Absatz 1 Satz 1, da Aufgehen in neuen Einrichtungskategorien Schaffung eines neuen Bußgeldtatbestandes für die Herausgabe notwendiger Informationen zur Störungsbeseitigung Zugrundeliegende Erwägungen: Berechtigung die Daten zur Störungsbeseitigung zu verarbeiten. Ein Zwangsgeld wäre hier voraussichtlich sinnlos, da es hier einer

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			rückwirkenden Sanktionierbarkeit bedarf.
830	9. entgegen § 8f Absatz 1 eine Selbsterklärung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vorlegt,	,	Entfällt, da dieser in den neuen Einrichtungskategorien aufgeht
831	10. entgegen § 9a Absatz 2 Satz 2 als Konformitätsbewertungsstelle tätig wird oder	10. entgegen § 55 Absatz 2 Satz 2 als Konformitätsbewertungsstelle tätig wird oder	Anpassung des Verweises
832	11. entgegen § 9c Absatz 4 Satz 1 das IT-Sicherheitskennzeichen verwendet.	11. entgegen § 56 Absastz 4 Satz 1 1 das IT-Sicherheitskennzeichen verwendet.	Anpassung des Verweises
833		12. vorgibt, Inhaber einer Zertifizierung nach § 54 Absatz 2 zu sein, ohne dass diese besteht	Neuer Bußgeldtatbestand: Zugrundeliegende Erwägung ist, dass ein Missbrauchstatbestand für die unbefugte Nutzung oder den sonstigen Missbrauch einer Sicherheitszertifizierung erforderlich ist, da hier keine effektive Verwaltungszwangsmöglichkeit besteht.
834		13. vorgibt, Inhaber eines europäischen Cybersicherheitszertifikats oder Aussteller einer EU-Konformitätserklärung zu sein, obwohl diese nicht besteht, widerrufen oder für ungültig erklärt wurde.	Neuer Bußgeldtatbestand: s. Erläuterung oben
835		14. einer verbindlichen Anweisung nach § 64 Absatz 3 oder § 65 Absatz 1 Nummer 2 nicht nachkommt.	Neuer Bußgeldtatbestand: Umsetzung NIS 2 Art. 32, 33 Abs. 4 lit. f, i sehen eine respektive Bebußung von wichtigen und besonders wichtigen Einrichtungen vor, wenn sie sich einer verbindlichen Anweisung widersetzen.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
836		15. entgegen § 64 Absatz 4 oder § 65 Absatz 3 einer Anweisung nicht oder seinen Mitwirkungspflichten gegenüber einem Überwachungsbeauftragten gemäß § 64 Absatz 5 nicht nachkommt.	Neuer Bußgeldtatbestand: Umsetzung NIS 2 § 64 Absatz 4 und § 65 Absatz 3 sehen respektive für besonders wichtige und wichtige Einrichtungen vor, dass das Bundesamt sie anweisen kann, die natürlichen oder juristischen Personen, für die sie Dienste erbringen oder Tätigkeiten ausüben und die potenziell von einer erheblichen Cyberbedrohung betroffen sind, über die Art der Bedrohung und mögliche Abwehr- oder Abhilfemaßnahmen zu unterrichten, die von diesen natürlichen oder juristischen Personen als Reaktion auf diese Bedrohung ergriffen werden können. Zudem kann es wichtige und wesentliche Einrichtungen anweisen, Informationen zu Verstößen gegen diese Richtlinie nach bestimmten Vorgaben öffentlich bekannt zu machen. Ebenso wird eine Bußgeldbewehrung bei § 60 Absatz 5, der vorsieht, dass das Bundesamt für besonders wichtige Einrichtungen einen Überwachungsbeauftragten benennen, der die Einhaltung der Verpflichtungen aus §§ 30, 31 und 39 überwacht, ergänzt. Art. 32 Abs. 4 lit i in Verbindung mit lit g sieht hier eine Bebußung vor.
837	(3) Ordnungswidrig handelt, wer eine in Absatz 1 bezeichnete Handlung fahrlässig begeht.	(3) Ordnungswidrig handelt, wer eine in Absatz 1 bezeichnete Handlung fahrlässig begeht.	
838	(4) Ordnungswidrig handelt, wer gegen die Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für	(4) Ordnungswidrig handelt, wer gegen die Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15) verstößt, indem er vorsätzlich oder fahrlässig	Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15) verstößt, indem er vorsätzlich oder fahrlässig	
839	1. entgegen Artikel 55 Absatz 1 eine dort genannte Angabe nicht, nicht richtig, nicht vollständig oder nicht binnen eines Monats nach Ausstellung zugänglich macht oder	1. entgegen Artikel 55 Absatz 1 eine dort genannte Angabe nicht, nicht richtig, nicht vollständig oder nicht binnen eines Monats nach Ausstellung zugänglich macht oder	
840	2. entgegen Artikel 56 Absatz 8 Satz 1 eine Information nicht, nicht richtig, nicht vollständig oder nicht unverzüglich nach Feststellung einer Sicherheitslücke oder Unregelmäßigkeit gibt.	2. entgegen Artikel 56 Absatz 8 Satz 1 eine Information nicht, nicht richtig, nicht vollständig oder nicht unverzüglich nach Feststellung einer Schwachstelle oder Unregelmäßigkeit gibt.	Redaktionelle Änderung von „Sicherheitslücke“ auf „Schwachstelle“.
841		(5) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 2 Nummer 1 Buchstabe a mit einer Geldbuße bis zu zwei Millionen Euro, wobei § 30 Absatz 2 Satz 3 des Gesetzes über Ordnungswidrigkeiten anzuwenden ist, sowie in den Fällen des Absatzes 2 Nummer 1 Buchstabe c, Nummern 5, 10, 11, 12 und 13 mit einer Geldbuße bis zu fünfhunderttausend Euro und in den Fällen des Absatzes 2 Nummer 1 Buchstabe b und des Absatzes 3 mit einer Geldbuße bis zu einhunderttausend Euro geahndet werden.	NIS-2 Allgemeiner Bußgeldtatbestand: Das Stufensystem wird beibehalten, wobei die Stufen angepasst wurden. Vorliegend werden die bußgeldbewehrten Tatbestände, die keiner Einrichtungsunterscheidung unterliegen, vorangestellt. a) Stufe 20 Millionen: Zu Absatz 2 Nummer 1 Buchstabe a: Keine Veränderung der Bußgeldhöhe; Übernahme der Anpassung durch § 30 Absatz 2 Satz 3 OWiG b) Stufe 500.000:

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			Zu Absatz 2 Nummer 1 Buchstabe c: Keine Veränderung Zu Absatz 2 Nummer 5: Hier wurden die Registrierungspflichten für andere Einrichtungsarten nach § 32 Absatz 1 s.Domain-Name Registry Diensteanbieter oder Anbieter nach §§ 33 Absatz 1, 64 Absatz 1 aufgenommen (sofern sie nicht unter untenstehende Einrichtungskategorien fallen und damit einer höheren Bebußung unterliegen würden) Zu Absatz 2 Nummer 10: Keine Veränderung der Bußgeldhöhe Zu Absatz 2 Nummer 11: Keine Veränderung der Bußgeldhöhe Zu Absatz 2 Nummer 12: Neuer Bußgeldtatbestand -> Orientierung der Bußgeldhöhe an der Höhe der Nummern 9 und 10 entsprechend Systematik Zu Absatz 2 Nummer 13: Neuer Bußgeldtatbestand; Anpassung der Höhe an Nummern 9 und 10 c) Stufe 100.000 Euro: Keine Veränderungen zum vorherigen Absatz 5

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
842	(5) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 2 Nummer 1 Buchstabe a mit einer Geldbuße bis zu zwei Millionen Euro sowie in den Fällen der Absätze 1, 2 Nummer 2 und 3 mit einer Geldbuße bis zu einer Million Euro geahndet werden. Die Ordnungswidrigkeit kann in den Fällen des Absatzes 2 Nummer 1 Buchstabe c, Nummer 5 und 7 bis 11 und des Absatzes 4 mit einer Geldbuße bis zu fünfhunderttausend Euro sowie in den Fällen des Absatzes 2 Nummer 1 Buchstabe b, Nummer 4 und 6 und des Absatzes 3 mit einer Geldbuße bis zu einhunderttausend Euro geahndet werden. In den Fällen des Satzes 1 ist § 30 Absatz 2 Satz 3 des Gesetzes über Ordnungswidrigkeiten anzuwenden.	(6). Handelt es sich bei dem Betroffenen um eine wichtige Einrichtung kann die Ordnungswidrigkeit in den Fällen der Absätze 2 Nummern 2 und 8 mit einer Geldbuße bis zu 7 Millionen Euro oder mit einem Höchstbetrag von mindestens 1,4 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem der Betroffene angehört, in den Fällen des Absatzes 2 Nummern 3, 5 und 9 mit einer Geldbuße bis zu fünfhunderttausend Euro und in dem Fall des Absatzes 2 Nummern 7, 14 und 15 mit einer Geldbuße bis zu einhunderttausend Euro geahndet werden.	Schaffung eines Bußgeldtatbestandes für wichtige Einrichtungen zur besseren Übersichtlichkeit und Differenzierung der Bußgeldhöhe Zu Absatz 2 Nummer 2: Dieser sieht die Ahndung von Verstößen gegen Risikomanagementmaßnahmen vor. Hier traf Art. 34 Absatz 4 RL dezidierte Vorgaben, die übernommen wurden. Voranstellend zum 4-stufigen bekannten System wurden diese übernommen. Zu Absatz 2 Nummer 8: Dieser sieht die Ahndung von Verstößen gegen die Meldepflichten aus § 31 Absatz 2 BSIG nF vor. Art. 34 Absatz 4 RL traf hier ebenfalls Vorgaben für die Bußgeldhöhe, die hier umgesetzt wurden. Zu Absatz 2 Nummer 3: Anpassung der Bußgeldhöhe im Vergleich zu besonders wichtigen und kritischen Einrichtungen Zu Absatz 2 Nummer 5: Anpassung der Bußgeldhöhe im Vergleich zu besonders wichtigen und kritischen Einrichtungen. Zu Absatz 2 Nummer 7:

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			Anpassung der Bußgeldhöhe im Vergleich zu besonders wichtigen und kritischen Einrichtungen. Zu Absatz 2 Nummer 14: Nichtnachkommen bei einer verbindlichen Anweisung Zu Absatz 2 Nummer 15: Bußgeldrahmen unterste Stufe aufgrund von Öffentlichkeitswirkung
843		(7) Handelt es sich bei dem Betroffenen um einen Betreiber kritischer Anlagen oder eine besonders wichtige Einrichtung, kann die Ordnungswidrigkeit in den Fällen der Absätze 1 und 2 Nummern 2, 3 und 8 mit einer Geldbuße bis zu 10 Millionen Euro oder mit einem Höchstbetrag von mindestens 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem der Betroffene angehört, in den Fällen des Absatzes 2 Nummer 4, 5, 7, 9 und 14 mit einer Geldbuße bis zu fünfhunderttausend Euro und in den Fällen des Absatzes 2 Nummern 6 und 15 mit einer Geldbuße bis zu einhunderttausend Euro geahndet werden	Schaffung eines Bußgeldtatbestandes entsprechend der Kategorien Betreiber kritischer Anlagen und besonders wichtige Einrichtungen zur besseren Übersichtlichkeit Eine Unterscheidung zwischen beiden Kategorien in der Bußgeldhöhe wurde hier nicht vorgenommen wegen marginaler Differenzen im Pflichtenkatalog. Eine entsprechende Differenzierung der Bußgeldhöhe entsprechend des Verhältnismäßigkeitsgrundsatzes kann entsprechend Schwere des Verstoßes und Einrichtungsart durch das Bundesamt vorgenommen werden. So ist bei Betreibern kritischer Anlagen der Bußgeldrahmen am oberen Rande auszuschöpfen. Zu Absatz 1: Keine Veränderung der Bußgeldhöhe, § 30 Absatz 2 Satz 3 OWiG führte vormals zu einer Verzehnfachung, die hier ebenfalls erreicht wird.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			Zu Absatz 2 Nummer 2: Dieser sieht die Ahndung von Verstößen gegen Risikomanagementmaßnahmen iSd § 30 Absatz 1 vor. Hier traf Art. 34 Absatz 4 RL dezidierte Vorgaben, die übernommen wurden. Diese wurden dem bekannten 4-stufigen System vorangestellt. Zu Absatz 2 Nummer 3: Anpassung der Bußgeldhöhe s. Absatz 1, vormals ebenso hoch durch Verweis des § 30 Absatz 2 Satz 3 OWiG Zu Absatz 2 Nummer 8: Dieser sieht die Ahndung von Verstößen gegen die Meldepflichten aus § 31 Absatz 2 BSIG nF vor. Art. 34 Absatz 4 RL traf hier ebenfalls Vorgaben für die Bußgeldhöhe, die hier umgesetzt wurden. zu Absatz 1: Übernahme der bisherigen Höhe, die entsprechend des Verweises auf § 30 Absatz 2 Satz 3 des OWiG verzehnfacht wird. Zu Absatz 2 Nummer 4: Anpassung Bußgeldhöhe 500.000 Euro

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			Zu Absatz 2 Nummer 5: Keine Änderung der Bußgeldhöhe Zu Absatz 2 Nummer 7: Bebußung bei Nichtmitteilung von Änderungen Zu Absatz 2 Nummer 9: Schaffung eines neuen Bußgeldtatbestandes für die Herausgabe wichtiger Informationen; Bußgeldhöhe 500.000 Euro Zu Absatz 2 Nummer 14: Nicht-Nachkommen einer verbindlichen Anweisung Zu Absatz 2 Nummer 6: Übernahme alter Bußgeldhöhe Zu Absatz 2 Nummer 15: Anwendung unterster Stufe des Bußgeldrahmens aufgrund Öffentlichkeitswirkung
844	(6) Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist das Bundesamt.	(8) Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist das Bundesamt.	
845		(9) Verhängen die in Artikel 55 oder 56 der Verordnung (EU) 2016/679 genannten Aufsichtsbehörden gemäß Artikel 58 Absatz 2 Buchstabe i der vorgenannten Verordnung eine Geldbuße, so darf ein weiteres Bußgeld für einen Verstoß nach diesem Gesetz, der sich aus demselben	Umsetzung Art. 35 Absatz 2 NIS-2.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		Verhalten ergibt wie jener Verstoß, nicht verhängt werden.	
846		(10) Soweit das Bundesamt Zwangsgelder verhängt, beträgt deren Höhe abweichend von § 11 Absatz 3 des Verwaltungs-Verfahrensgesetzes bis zu 100.000 Euro.	Umsetzung Art. 34 Absatz 6 NIS 2
847	§ 14a Institutionen der Sozialen Sicherung	§ 61 Institutionen der Sozialen Sicherung	
848	Bei Zuwiderhandlungen gegen eine in § 14 Absatz 1 bis 4 genannte Vorschrift, die von Körperschaften gemäß § 29 des Vierten Buches Sozialgesetzbuch, Arbeitsgemeinschaften gemäß § 94 des Zehnten Buches Sozialgesetzbuch sowie der Deutschen Post AG, soweit sie mit der Berechnung oder Auszahlung von Sozialleistungen betraut ist (Institutionen der Sozialen Sicherung), begangen werden, finden die Sätze 2 bis 4 Anwendung. Bei einer in Satz 1 genannten Zuwiderhandlung von Institutionen der Sozialen Sicherung in Trägerschaft des Bundes stellt das Bundesamt das Einvernehmen über die zu ergreifenden Maßnahmen mit der für die Institution der Sozialen Sicherung zuständigen Aufsichtsbehörde her. Bei einer in Satz 1 genannten Zuwiderhandlung von Institutionen der Sozialen Sicherung in Trägerschaft der Länder informiert das Bundesamt die zuständige Aufsichtsbehörde und schlägt geeignete Maßnahmen vor. Die jeweils zuständige Aufsichtsbehörde informiert das Bundesamt über die Einleitung und Umsetzung von Aufsichtsmitteln und sorgt für deren Durchsetzung.	Bei Zuwiderhandlungen gegen eine in § 60 Absatz 1 bis 4 genannte Vorschrift, die von Körperschaften gemäß § 29 des Vierten Buches Sozialgesetzbuch, Arbeitsgemeinschaften gemäß § 94 des Zehnten Buches Sozialgesetzbuch sowie der Deutschen Post AG, soweit sie mit der Berechnung oder Auszahlung von Sozialleistungen betraut ist (Institutionen der Sozialen Sicherung), begangen werden, finden die Sätze 2 bis 4 Anwendung. Bei einer in Satz 1 genannten Zuwiderhandlung von Institutionen der Sozialen Sicherung in Trägerschaft des Bundes stellt das Bundesamt das Einvernehmen über die zu ergreifenden Maßnahmen mit der für die Institution der Sozialen Sicherung zuständigen Aufsichtsbehörde her. Bei einer in Satz 1 genannten Zuwiderhandlung von Institutionen der Sozialen Sicherung in Trägerschaft der Länder informiert das Bundesamt die zuständige Aufsichtsbehörde und schlägt geeignete Maßnahmen vor. Die jeweils zuständige Aufsichtsbehörde informiert das Bundesamt über die Einleitung und Umsetzung von Aufsichtsmitteln und sorgt für deren Durchsetzung.	
849		§ 62 Zuständigkeit des Bundesamtes	Neue zentrale Zuständigkeitsnorm.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
850		(1) Das Bundesamt ist zuständige Aufsichtsbehörde für die Einhaltung der Vorschriften in Teil 3 durch wichtige und besonders wichtige Einrichtungen, die in der Bundesrepublik Deutschland niedergelassen und nicht Einrichtungen des Sektors öffentliche Verwaltung sind, sowie durch Betreiber kritischer Anlagen, deren kritische Anlagen sich auf dem Hoheitsgebiet der Bundesrepublik Deutschland befinden.	Umsetzung von Art. 8 Abs. 1-2; Art. 26 Abs. 1 NIS-2. Die Zuständigkeit für wichtige und besonders wichtige Einrichtungen bestimmt sich nach dem Niederlassungsprinzip. Die Zuständigkeit für Betreiber kritischer Anlagen bestimmt sich nach Belegenheitsprinzip hinsichtlich der jeweiligen kritischen Anlagen. Die Zuständigkeit des Bundesamtes für Einrichtungen der Bundesverwaltung richtet sich nach den Befugnissen des Bundesamtes in Teil 2 Kapitel 1.
851		(2) Abweichend von Absatz 1 ist die Bundesnetzagentur für Betreiber von Kommunikationsnetzen oder Anbieter von Telekommunikationsdiensten zuständig, die ihre Dienste in der Bundesrepublik Deutschland erbringen.	Umsetzung von Art. 26 Abs. 1 lit. a NIS-2.
852		(3) Abweichend von Absatz 1 ist das Bundesamt im Sektor öffentliche Verwaltung nur für solche wichtige und besonders wichtige Einrichtungen zuständig, die von der Bundesrepublik Deutschland eingerichtet wurden.	Umsetzung von Art. 26 Abs. 1 lit. c NIS-2.
853		§ 63 Zentrale Zuständigkeit in der Europäischen Union für bestimmte Einrichtungsarten	Umsetzung von Art. 26 Abs. 1 lit. b, Abs. 2-5 NIS-2.
854		(1) Abweichend von § 62 ist das Bundesamt für DNS-Diensteanbieter, Top Level Domain Name Registries, Domain-Name-Registry-Dienstleister, Anbieter von Cloud Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Content Delivery Networks, Managed Service Provider, Managed Security Service Provider sowie Anbieter von	Umsetzung von Art. 26 Abs. 1 lit. b NIS-2.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		Online-Marktplätzen, Online-Suchmaschinen oder Plattformen für Dienste sozialer Netzwerke nur dann zuständig, wenn diese ihre Hauptniederlassung in der Europäischen Union in der Bundesrepublik Deutschland hat. Ist dies der Fall, so ist das Bundesamt für die Einrichtung in der gesamten Europäischen Union zentral zuständig.	
855		(2) Als Hauptniederlassung in der Europäischen Union im Sinne von Absatz 1 gilt derjenige Mitgliedstaat der Europäischen Union, in dem die Entscheidungen der Einrichtung im Zusammenhang mit den Maßnahmen zum Cybersicherheitsrisikomanagement vorwiegend getroffen werden. Kann ein solcher Mitgliedstaat nicht bestimmt werden oder werden solche Entscheidungen nicht in der Europäischen Union getroffen, so gilt als Hauptniederlassung der Mitgliedstaat, in dem die Cybersicherheitsmaßnahmen durchgeführt werden. Kann ein solcher Mitgliedstaat nicht bestimmt werden, so gilt als Hauptniederlassung der Mitgliedstaat, in dem die betreffende Einrichtung die Niederlassung mit der höchsten Beschäftigtenzahl in der Europäischen Union hat.	Umsetzung von Art. 26 Abs. 2 NIS-2.
856		(3) Hat eine Einrichtung der in Absatz 1 Satz 1 genannten Einrichtungsart keine Niederlassung in der Europäischen Union, bietet aber Dienste innerhalb der Europäischen Union an, ist sie verpflichtet einen Vertreter zu benennen. Der Vertreter muss in einem Mitgliedstaat der Europäischen Union niedergelassen sein, in der die betreffende Einrichtung die Dienste anbietet. Ist der Vertreter in der Bundesrepublik Deutschland niedergelassen, ist das Bundesamt für die Einrichtung zuständig. Wurde durch eine Einrichtung der in Absatz 1 Satz 1 genannten Einrichtungsart in der Europäischen Union kein Vertreter im Sinne dieses Absatzes benannt, kann das Bundesamt sich für die betreffende Einrichtung zuständig erklären.	Umsetzung von Art. 26 Abs. 3 NIS-2. Vertreter kann eine in der Europäischen Union niedergelassene natürliche oder juristische Person sein, die ausdrücklich benannt wurde, um im Auftrag einer Einrichtung, die nicht in der Europäischen Union niedergelassen ist, zu handeln, und an die sich das Bundesamt in Fragen der der Pflichten der benennenden Einrichtung nach diesem Gesetz wenden kann.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
857		(4) Die Benennung eines Vertreters durch eine Einrichtung der in Absatz 1 Satz 1 genannten Einrichtungsart lässt rechtliche Schritte, die gegen die Einrichtung selbst eingeleitet werden könnten, unberührt.	Umsetzung von Art. 26 Abs. 4 NIS-2.
858		(5) Das Bundesamt ist befugt, wenn und soweit es ein Rechtshilfeersuchen eines anderen Mitgliedsstaats der Europäischen Union zu einer Einrichtung der in Absatz 1 Satz 1 genannten Einrichtungsart erhalten hat, innerhalb der Grenzen dieses Ersuchens geeignete Aufsichts- und Durchsetzungsmaßnahmen in Bezug auf die betreffende Einrichtung zu ergreifen, die in der Bundesrepublik Deutschland Dienste anbietet oder eine informationstechnisches System, Komponente oder Prozess betreibt.	Umsetzung von Art. 26 Abs. 5 NIS-2.
859		§ 64 Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtige Einrichtungen	Umsetzung von Art. 32 NIS-2.
860		(1) Das Bundesamt kann bei besonders wichtigen Einrichtungen die Einhaltung der Anforderungen nach diesem Gesetz überprüfen. Es kann sich bei der Durchführung der Überprüfung eines qualifizierten unabhängigen Dritten bedienen. Die Besonders wichtige Einrichtung hat dem Bundesamt und den in dessen Auftrag handelnden Personen zum Zweck der Überprüfung das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten und auf Verlangen die in Betracht kommenden Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorzulegen, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren. Für die Überprüfung erhebt das Bundesamt Gebühren und Auslagen bei der jeweiligen Wesentlichen Einrichtung nur, sofern das Bundesamt auf Grund von Anhaltspunkten tätig	Umsetzung Art. 32 NIS-2.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		geworden ist, die berechtigte Zweifel an der Einhaltung der Anforderungen nach § 30 Absatz 1 begründeten.	
861		(2) Das Bundesamt kann gegenüber besonders wichtigen Einrichtungen Anweisungen in Bezug auf Maßnahmen erlassen, die zur Verhütung oder Behebung eines Sicherheitsvorfalls erforderlich sind. Ferner kann das Bundesamt die Einrichtungen zur Berichterstattung zu den nach Satz 1 angeordneten Maßnahmen auffordern.	Umsetzung Art. 32 Abs. 4 lit. b NIS-2.
862		(3) Das Bundesamt kann gegenüber besonders wichtigen Einrichtungen verbindliche Anweisungen zur Umsetzung der Verpflichtungen nach diesem Gesetz erlassen.	Umsetzung von Art. 32 Abs. 4 lit. c, d und f NIS-2.
863		(4) Das Bundesamt kann besonders wichtige Einrichtungen anweisen, die natürlichen oder juristischen Personen, für die sie Dienste erbringen oder Tätigkeiten ausüben und die potenziell von einer erheblichen Cyberbedrohung betroffen sind, über die Art der Bedrohung und mögliche Abwehr- oder Abhilfemaßnahmen zu unterrichten, die von diesen natürlichen oder juristischen Personen als Reaktion auf diese Bedrohung ergriffen werden können. Zudem kann es besonders wichtige Einrichtungen anweisen, Informationen zu Verstößen gegen diese Richtlinie nach bestimmten Vorgaben öffentlich bekannt zu machen.	Umsetzung von Art. 32 Abs. 4 lit. e (S. 1) und lit. h (S. 2) NIS-2.
864		(5) Das Bundesamt kann für besonders wichtige Einrichtungen einen Überwachungsbeauftragten benennen, der die Einhaltung der Verpflichtungen aus §§ 28, 29 und 37 überwacht. Die Benennung erfolgt für einen bestimmten Zeitraum und muss die Aufgaben des Überwachungsbeauftragten genau festlegen.	Umsetzung Art. 32 Abs. 4 lit. g NIS-2.
865		(6) Sofern besonders wichtige Einrichtungen den Anordnungen des Bundesamtes nach diesem Gesetz	Umsetzung Art. 32 Abs. 5 Uabs. 1 NIS-2.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		trotz Fristsetzung nicht nachkommen, kann das Bundesamt	
866		1. die Zertifizierung für einen Teil oder alle Dienste oder Tätigkeiten dieser Einrichtung aussetzen	Umsetzung Art. 32 Abs. 5 Uabs. 1 lit. a NIS-2.
867		2. den natürlichen Personen, die als Geschäftsführung oder gesetzliche Vertreter für Leitungsaufgaben in der Wesentlichen Einrichtung zuständig sind, die Wahrnehmung der Leitungsaufgaben vorübergehend untersagen.	Umsetzung Art. 32 Abs. 5 Uabs. 1 lit. b NIS-2.
868		Die Aussetzung nach Buchstabe a und die Untersagung nach Buchstabe b sind nur solange zulässig, bis die Besonders wichtige Einrichtung den Anordnungen des Bundesamtes nachkommt, wegen deren Nichtbefolgung sie verhängt ausgesprochen wurden.	Umsetzung Art. 32 Abs. 5 Uabs. 2 NIS-2.
869		(7) Soweit das Bundesamt Aufsichtsmaßnahmen gegenüber besonders wichtigen Einrichtungen [*die in Umsetzung der CER-Richtlinie als kritische Einrichtungen im Sinne der CER-Richtlinie identifiziert wurden*], informiert es die für die Aufsicht über diese Einrichtungen nach dem [*KRITIS-Dachgesetz*] zuständige Behörde des Bundes darüber.	Umsetzung Art. 32 Abs. 9 NIS-2. [*Anm. BMI CI1 – Verweis in das KRITIS-Dachgesetz noch nachzutragen.*]
870		(8) Stellt das Bundesamt im Zuge der Beaufsichtigung oder Durchsetzung fest, dass der Verstoß einer besonders wichtigen Einrichtung gegen Verpflichtungen aus § 30 oder § 31 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 der vorgenannten Verordnung zu melden ist, unterrichtet das Bundesamt unverzüglich die in Artikel 55 oder 56	Umsetzung Art. 35 Abs. 1 NIS-2.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		der vorgenannten Verordnung genannten Aufsichtsbehörden.	
871		§ 65 Aufsichts- und Durchsetzungsmaßnahmen für wichtige Einrichtungen	Umsetzung Art. 33 NIS-2
872		(1) Erlangt das Bundesamt Kenntnis über Hinweise oder Informationen, wonach eine wichtige Einrichtung die Anforderungen aus § 30 Absatz 1 oder § 29 nicht oder nicht richtig umsetzt, so kann es folgende Maßnahmen durchführen:	s.o.
873		1. Überprüfung der Einhaltung der Anforderungen nach § 30 Absatz 1. § 64 Sätze 2 bis 4 gelten entsprechend.	s.o.
874		2. Verbindliche Anweisungen zur Umsetzung der Verpflichtungen für wichtige Einrichtungen nach diesem Gesetz erlassen.	Umsetzung Art. 33 Abs. 4 lit. b, c, d und f NIS-2.
875		(2) Das Bundesamt kann Informationen anfordern, um die Einhaltung der Verpflichtungen zur Übermittlung von Informationen an die zuständigen Behörden nach diesem Gesetz zu überprüfen.	Umsetzung Art. 33 Abs. 2 lit. d NIS-2.
876		(3) Das Bundesamt kann wichtige Einrichtungen anweisen, die natürlichen oder juristischen Personen, für die sie Dienste erbringen oder Tätigkeiten ausüben und die potenziell von einer erheblichen Cyberbedrohung betroffen sind, über die Art der Bedrohung und mögliche Abwehr- oder Abhilfemaßnahmen zu unterrichten, die von diesen natürlichen oder juristischen Personen als Reaktion auf diese Bedrohung ergriffen werden können. Zudem kann es wichtige Einrichtungen anweisen, Informationen zu Verstößen gegen diese Richtlinie	Umsetzung Art. 33 Abs. 4 lit. e und lit. g NIS-2.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		nach bestimmten Vorgaben öffentlich bekannt zu machen,	
877		(4) § 64 Abs. 8 gilt entsprechend für einen Verstoß einer wichtige Einrichtung.	Umsetzung Art. 35 Abs. 1 NIS-2.
878	§ 15 Anwendbarkeit der Vorschriften für Anbieter digitaler Dienste		Die Vorschrift hat sich durch Zeitablauf erledigt. Im Übrigen geht die Kategorie der Anbieter digitaler Dienste in die neuen Einrichtungskategorien auf.
879	Die Vorschriften, die Anbieter digitaler Dienste betreffen, sind ab dem 10. Mai 2018 anwendbar.		s.o.
880		**Artikel 2** **Änderung des BSI-Gesetzes**	
881	§ 10 Ermächtigung zum Erlass von Rechtsverordnungen	§ 10 Ermächtigung zum Erlass von Rechtsverordnungen	
882	(1) Das Bundesministerium des Innern, für Bau und Heimat bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr und digitale Infrastruktur, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit unter Festlegung der in den jeweiligen Sektoren im Hinblick auf § 2 Absatz 10 Satz 1 Nummer 2 wegen ihrer Bedeutung als	(1) Das Bundesministerium des Innern, für Bau und Heimat bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr und digitale Infrastruktur, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit unter Festlegung der in den jeweiligen Sektoren im Hinblick auf § 2 Absatz 10 Satz 1 Nummer 2 wegen ihrer Bedeutung als	(unverändert)

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrads, welche Einrichtungen, Anlagen oder Teile davon als Kritische Infrastrukturen im Sinne dieses Gesetzes gelten. Der nach Satz 1 als bedeutend anzusehende Versorgungsgrad ist anhand von branchenspezifischen Schwellenwerten für jede wegen ihrer Bedeutung als kritisch anzusehende Dienstleistung im jeweiligen Sektor zu bestimmen. Zugang zu Akten, die die Erstellung oder Änderung dieser Verordnung betreffen, wird nicht gewährt.	kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrads, welche Einrichtungen, Anlagen oder Teile davon als Kritische Infrastrukturen im Sinne dieses Gesetzes gelten. Der nach Satz 1 als bedeutend anzusehende Versorgungsgrad ist anhand von branchenspezifischen Schwellenwerten für jede wegen ihrer Bedeutung als kritisch anzusehende Dienstleistung im jeweiligen Sektor zu bestimmen. Zugang zu Akten, die die Erstellung oder Änderung dieser Verordnung betreffen, wird nicht gewährt.	
883		(1a) Die Ermächtigung zum Erlass einer Rechtsverordnung nach Absatz 1 entfällt, sobald von der Ermächtigung zum Erlass einer Rechtsverordnung nach Absatz 1b Gebrauch gemacht wurde.	Die neue BSI-KritisV soll auf Grundlage der neuen Ermächtigung nach Absatz 1a nF. erlassen werden. Damit die bisherige BSI-KritisV bis zum Erlass der neuen BSI-KritisV ihre Geltung behält, entfällt die Ermächtigung nach Absatz 1 bedingt auf den Gebrauch der Ermächtigung nach Absatz 1b.
884		(1b) Das Bundesministerium des Innern und für Heimat bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber, Einrichtungen und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Klimaschutz, dem Bundesministerium der Justiz, dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Digitales und Verkehr, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz	Damit die neue BSI-KritisV noch vor Inkrafttreten des Gesetzes im Übrigen erlassen werden kann, tritt dieser Artikel vor den Übrigen in Kraft. [*Anm. BMI CI1 – Diese Vorschrift (§ 10 BSIG aF.) ist Gegenstand der Evaluierung gemäß Art. 6 Abs. 1 Nr. 1 Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 18. Mai 2021 (BGBl. I S. 1122). Diese Änderung erfolgt vorbehaltlich der Ergebnisse dieser Evaluierung und wird gegebenenfalls noch auf deren Grundlage angepasst.*]

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
885		1. unter Festlegung der in den jeweiligen Sektoren Energie, Transport und Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, Ernährung, digitale Infrastruktur, sowie Siedlungsabfallentsorgung im Hinblick auf § 30 Absatz 2a wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrads, welche Anlagen oder Teile davon als kritische Anlagen im Sinne dieses Gesetzes gelten,	
886		2. sowie welche Einrichtungsarten in den Sektoren Energie, Transport und Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, digitale Infrastruktur, Verwaltung von IKT-Diensten (Business-to-Business), und Weltraum Einrichtungsarten besonders wichtiger Einrichtungen sind, und	
887		3. welche Einrichtungsarten in den Sektoren Energie, Transport und Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, digitale Infrastruktur, Siedlungsabfallentsorgung, Logistik, Produktion, Chemie, Ernährung, verarbeitendes Gewerbe, Anbieter digitaler Dienste oder Forschung Einrichtungsarten wichtiger Einrichtungen sind.	
888		Der nach Satz 1 als bedeutend anzusehende Versorgungsgrad ist anhand von branchenspezifischen	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		Schwellenwerten für jede wegen ihrer Bedeutung als kritisch anzusehende Dienstleistung im jeweiligen Sektor zu bestimmen. Zugang zu Akten, die die Erstellung oder Änderung dieser Verordnung betreffen, wird nicht gewährt.	
889		**Artikel 3** **Telekommunikationsgesetz (TKG)**	
890	§ 165 Technische und organisatorische Schutzmaßnahmen	§ 165 Technische und organisatorische Schutzmaßnahmen	
891	(1) Wer Telekommunikationsdienste erbringt oder daran mitwirkt, hat angemessene technische Vorkehrungen und sonstige Maßnahmen zu treffen	(1) Wer Telekommunikationsdienste erbringt oder daran mitwirkt, hat angemessene technische Vorkehrungen und sonstige Maßnahmen zu treffen	
892	1. zum Schutz des Fernmeldegeheimnisses und	1. zum Schutz des Fernmeldegeheimnisses und	
893	2. gegen die Verletzung des Schutzes personenbezogener Daten.	2. gegen die Verletzung des Schutzes personenbezogener Daten.	
894	Dabei ist der Stand der Technik zu berücksichtigen.	Dabei ist der Stand der Technik zu berücksichtigen.	
895	(2) Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat bei den hierfür betriebenen Telekommunikations- und Datenverarbeitungssystemen angemessene technische und organisatorische Vorkehrungen und sonstige Maßnahmen zu treffen	(2) Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat bei den hierfür betriebenen Telekommunikations- und Datenverarbeitungssystemen angemessene technische und organisatorische Vorkehrungen und sonstige Maßnahmen zu treffen	
896	1. zum Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und -diensten führen, auch, sofern diese Störungen durch äußere Angriffe und	1. zum Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und -diensten führen, auch, sofern diese Störungen durch äußere Angriffe und Einwirkungen	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Einwirkungen von Katastrophen bedingt sein können, und	von Katastrophen bedingt sein können, und	
897	2. zur Beherrschung der Risiken für die Sicherheit von Telekommunikationsnetzen und -diensten.	2. zur Beherrschung der Risiken für die Sicherheit von Telekommunikationsnetzen und -diensten.	
898	Insbesondere sind Maßnahmen, einschließlich gegebenenfalls Maßnahmen in Form von Verschlüsselung, zu treffen, um Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu sichern und Auswirkungen von Sicherheitsverletzungen für Nutzer, andere Telekommunikationsnetze und Dienste so gering wie möglich zu halten. Bei diesen Maßnahmen ist der Stand der Technik zu berücksichtigen.	Insbesondere sind Maßnahmen, einschließlich gegebenenfalls Maßnahmen in Form von Verschlüsselung, zu treffen, um Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu sichern und Auswirkungen von Sicherheitsverletzungen für Nutzer, andere Telekommunikationsnetze und Dienste so gering wie möglich zu halten. Bei diesen Maßnahmen ist der Stand der Technik zu berücksichtigen.	
899	(3) Als eine angemessene Maßnahme im Sinne des Absatzes 2 können Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher Telekommunikationsdienste Systeme zur Angriffserkennung im Sinne des § 2 Absatz 9b des BSI-Gesetzes einsetzen. Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher Telekommunikationsdienste mit erhöhtem Gefährdungspotenzial haben entsprechende Systeme zur Angriffserkennung einzusetzen. Die eingesetzten Systeme zur Angriffserkennung müssen in der Lage sein, durch kontinuierliche und automatische Erfassung und Auswertung Gefahren oder Bedrohungen zu erkennen. Sie sollen zudem in der Lage sein, erkannte Gefahren oder Bedrohungen abzuwenden und für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen. Weitere Einzelheiten kann die Bundesnetzagentur im Katalog von Sicherheitsanforderungen nach § 167 festlegen.	(3) Als eine angemessene Maßnahme im Sinne des Absatzes 2 können Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher Telekommunikationsdienste Systeme zur Angriffserkennung im Sinne des § 2 Absatz 1 Nummer 52 des BSI-Gesetzes einsetzen. Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher Telekommunikationsdienste mit erhöhtem Gefährdungspotenzial haben entsprechende Systeme zur Angriffserkennung einzusetzen. Die eingesetzten Systeme zur Angriffserkennung müssen in der Lage sein, durch kontinuierliche und automatische Erfassung und Auswertung Gefahren oder Bedrohungen zu erkennen. Sie sollen zudem in der Lage sein, erkannte Gefahren oder Bedrohungen abzuwenden und für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen. Weitere Einzelheiten kann die Bundesnetzagentur im Katalog von Sicherheitsanforderungen nach § 167 festlegen.	Anpassung des Verweises auf das BSIG nF.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
900	(4) Kritische Komponenten im Sinne von § 2 Absatz 13 des BSI-Gesetzes dürfen von einem Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial nur eingesetzt werden, wenn sie vor dem erstmaligen Einsatz von einer anerkannten Zertifizierungsstelle überprüft und zertifiziert wurden.	(4) Kritische Komponenten im Sinne von § 2 Absatz 1 Nummer 26 des BSI-Gesetzes dürfen von einem Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial nur eingesetzt werden, wenn sie vor dem erstmaligen Einsatz von einer anerkannten Zertifizierungsstelle überprüft und zertifiziert wurden.	Anpassung des Verweises auf das BSIG nF.
901	§ 167 Katalog von Sicherheitsanforderungen	§ 167 Katalog von Sicherheitsanforderungen	
902	(1) Die Bundesnetzagentur legt im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit durch Allgemeinverfügung in einem Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikationsund Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten fest:	(1) Die Bundesnetzagentur legt im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit durch Allgemeinverfügung in einem Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten fest:	
903	1. Einzelheiten der nach § 165 Absatz 1 bis 7 zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen unter Beachtung der verschiedenen Gefährdungspotenziale der öffentlich	1. Einzelheiten der nach § 165 Absatz 1 bis 7 zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen unter Beachtung der verschiedenen Gefährdungspotenziale der öffentlich	[*Anm. BMI CI3 – Hier ist in Folge der NIS-2-Richtlinie noch sicherzustellen, dass die Sicherheitsanforderungen im Katalog die Mindestanforderungen von NIS-2 nicht unterschreiten. Ggf. sind die in Art. 21 NIS-2 explizit genannten Maßnahmen auch hier explizit zu nennen.*]
904	2. welche Funktionen kritische Funktionen im Sinne von § 2 Absatz 13 Satz 1 Nummer 3 Buchstabe b des BSI-Gesetzes sind, die von kritischen Komponenten im Sinne von § 2 Absatz 13 des BSI-Gesetzes realisiert werden, und	2. welche Funktionen kritische Funktionen im Sinne von § 2 Absatz 1 Nummer 20 Buchstabe c Doppelbuchstabe bb des BSI-Gesetzes sind, die von kritischen Komponenten im Sinne von § 2 Absatz 1 Nummer 20 des BSI-Gesetzesrealisiert werden, und	Anpassung der Verweise auf das BSIG nF.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
905	3. wer als Betreiber öffentlicher Telekommunikationsnetze und als Anbieter öffentlich zugänglicher Telekommunikationsdienste mit erhöhtem Gefährdungspotenzial einzustufen ist.	3. wer als Betreiber öffentlicher Telekommunikationsnetze und als Anbieter öffentlich zugänglicher Telekommunikationsdienste mit erhöhtem Gefährdungspotenzial einzustufen ist.	
906	Der Katalog von Sicherheitsanforderungen nach Satz 1 kann auch Anforderungen zur Offenlegung und Interoperabilität von Schnittstellen von Netzkomponenten einschließlich einzuhaltender technischer Standards enthalten. Die Bundesnetzagentur gibt den Herstellern, den Verbänden der Betreiber öffentlicher Telekommunikationsnetze und den Verbänden der Anbieter öffentlich zugänglicher Telekommunikationsdienste Gelegenheit zur Stellungnahme.	Der Katalog von Sicherheitsanforderungen nach Satz 1 kann auch Anforderungen zur Offenlegung und Interoperabilität von Schnittstellen von Netzkomponenten einschließlich einzuhaltender technischer Standards enthalten. Die Bundesnetzagentur gibt den Herstellern, den Verbänden der Betreiber öffentlicher Telekommunikationsnetze und den Verbänden der Anbieter öffentlich zugänglicher Telekommunikationsdienste Gelegenheit zur Stellungnahme.	
907	§ 168 Mitteilung eines Sicherheitsvorfalls	§ 168 Mitteilung eines Sicherheitsvorfalls	
908	(1) Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat der Bundesnetzagentur und dem Bundesamt für Sicherheit in der Informationstechnik einen Sicherheitsvorfall mit beträchtlichen Auswirkungen auf den Betrieb der Netze oder die Erbringung der Dienste unverzüglich mitzuteilen. § 42 Absatz 4 und § 43 Absatz 4 des Bundesdatenschutzgesetzes gelten entsprechend.	(1) Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat der Bundesnetzagentur und dem Bundesamt für Sicherheit in der Informationstechnik einen Sicherheitsvorfall mit beträchtlichen Auswirkungen auf den Betrieb der Netze oder die Erbringung der Dienste unverzüglich mitzuteilen. § 42 Absatz 4 und § 43 Absatz 4 des Bundesdatenschutzgesetzes gelten entsprechend.	[*Anm. BMI CI3 - Hier ist in Folge der NIS-2-Richtlinie noch sicherzustellen, dass die Meldevorschrift die Mindestanforderungen von NIS-2 nicht unterschreitet.*]
909	(2) Das Ausmaß der Auswirkungen eines Sicherheitsvorfalls ist – sofern verfügbar – insbesondere anhand folgender Kriterien zu bewerten:	(2) Das Ausmaß der Auswirkungen eines Sicherheitsvorfalls ist – sofern verfügbar – insbesondere anhand folgender Kriterien zu bewerten:	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
910	1. die Zahl der von dem Sicherheitsvorfall betroffenen Nutzer,	1. die Zahl der von dem Sicherheitsvorfall betroffenen Nutzer,	
911	2. die Dauer des Sicherheitsvorfalls,	2. die Dauer des Sicherheitsvorfalls,	
912	3. die geographische Ausdehnung des von dem Sicherheitsvorfall betroffenen Gebiets,	3. die geographische Ausdehnung des von dem Sicherheitsvorfall betroffenen Gebiets,	
913	4. das Ausmaß der Beeinträchtigung des Telekommunikationsnetzes oder des Dienstes,	4. das Ausmaß der Beeinträchtigung des Telekommunikationsnetzes oder des Dienstes,	
914	5. das Ausmaß der Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten.	5. das Ausmaß der Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten.	
915	(3) Die Mitteilung nach Absatz 1 Satz 1 muss die folgenden Angaben enthalten:	(3) Die Mitteilung nach Absatz 1 Satz 1 muss die folgenden Angaben enthalten:	
916	1. Angaben zu dem Sicherheitsvorfall,	1. Angaben zu dem Sicherheitsvorfall,	
917	2. Angaben zu den Kriterien nach Absatz 2,	2. Angaben zu den Kriterien nach Absatz 2,	
918	3. Angaben zu den betroffenen Systemen sowie	3. Angaben zu den betroffenen Systemen sowie	
919	4. Angaben zu der vermuteten oder tatsächlichen Ursache.	4. Angaben zu der vermuteten oder tatsächlichen Ursache.	
920	(4) Die Bundesnetzagentur legt Einzelheiten des Mitteilungsverfahrens fest. Die Bundesnetzagentur kann einen detaillierten Bericht über den Sicherheitsvorfall und die ergriffenen Abhilfemaßnahmen verlangen.	(4) Die Bundesnetzagentur legt Einzelheiten des Mitteilungsverfahrens fest. Die Bundesnetzagentur kann einen detaillierten Bericht über den Sicherheitsvorfall und die ergriffenen Abhilfemaßnahmen verlangen.	
921	(5) Erforderlichenfalls unterrichtet die Bundesnetzagentur die nationalen Regulierungsbehörden der anderen Mitgliedstaaten der Europäischen Union und die Agentur der	(5) Erforderlichenfalls unterrichtet die Bundesnetzagentur die nationalen Regulierungsbehörden der anderen Mitgliedstaaten der Europäischen Union und die Agentur der	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Europäischen Union für Cybersicherheit über den Sicherheitsvorfall. Die Bundesnetzagentur kann die Öffentlichkeit unterrichten oder die nach Absatz 1 Satz 1 Verpflichteten zu dieser Unterrichtung verpflichten, wenn sie zu dem Schluss gelangt, dass die Bekanntgabe des Sicherheitsvorfalls im öffentlichen Interesse liegt.	Europäischen Union für Cybersicherheit über den Sicherheitsvorfall. Die Bundesnetzagentur kann die Öffentlichkeit unterrichten oder die nach Absatz 1 Satz 1 Verpflichteten zu dieser Unterrichtung verpflichten, wenn sie zu dem Schluss gelangt, dass die Bekanntgabe des Sicherheitsvorfalls im öffentlichen Interesse liegt.	
922	(6) Im Falle einer besonderen und erheblichen Gefahr eines Sicherheitsvorfalls informieren die nach Absatz 1 Satz 1 Verpflichteten die von dieser Gefahr potenziell betroffenen Nutzer über alle möglichen Schutz- oder Abhilfemaßnahmen, die von den Nutzern ergriffen werden können sowie gegebenenfalls auch über die Gefahr selbst. § 8e des BSI-Gesetzes gilt entsprechend.	(6) Im Falle einer besonderen und erheblichen Gefahr eines Sicherheitsvorfalls informieren die nach Absatz 1 Satz 1 Verpflichteten die von dieser Gefahr potenziell betroffenen Nutzer über alle möglichen Schutz- oder Abhilfemaßnahmen, die von den Nutzern ergriffen werden können sowie gegebenenfalls auch über die Gefahr selbst. § 42 des BSI-Gesetzes gilt entsprechend.	
923	§ 174 Manuelles Auskunftsverfahren	§ 174 Manuelles Auskunftsverfahren	
924	(1) Wer Telekommunikationsdienste erbringt oder daran mitwirkt, darf von ihm erhobene Bestandsdaten sowie die nach § 172 erhobenen Daten nach Maßgabe dieser Vorschrift zur Erfüllung von Auskunftspflichten gegenüber den in Absatz 3 genannten Stellen verwenden. Dies gilt auch für Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird. Die in eine Auskunft aufzunehmenden Daten dürfen auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse bestimmt werden; hierfür dürfen Verkehrsdaten auch automatisiert ausgewertet werden. Für die Auskunftserteilung nach Satz 3 sind sämtliche unternehmensinternen Datenquellen zu berücksichtigen. Der Verpflichtete hat die in seinem Verantwortungsbereich für die Auskunftserteilung	(1) Wer Telekommunikationsdienste erbringt oder daran mitwirkt, darf von ihm erhobene Bestandsdaten sowie die nach § 172 erhobenen Daten nach Maßgabe dieser Vorschrift zur Erfüllung von Auskunftspflichten gegenüber den in Absatz 3 genannten Stellen verwenden. Dies gilt auch für Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird. Die in eine Auskunft aufzunehmenden Daten dürfen auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse bestimmt werden; hierfür dürfen Verkehrsdaten auch automatisiert ausgewertet werden. Für die Auskunftserteilung nach Satz 3 sind sämtliche unternehmensinternen Datenquellen zu berücksichtigen. Der Verpflichtete hat die in seinem Verantwortungsbereich für die Auskunftserteilung	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	erforderlichen Vorkehrungen auf eigene Kosten zu treffen.	erforderlichen Vorkehrungen auf eigene Kosten zu treffen.	
925	(3) Die Auskunft nach Absatz 1 Satz 1 darf nur erteilt werden	(3) Die Auskunft nach Absatz 1 Satz 1 darf nur erteilt werden	
926	8. an das Bundesamt für Sicherheit in der Informationstechnik zum Schutz der Versorgung der Bevölkerung in den Bereichen des § 2 Absatz 10 Satz 1 Nummer 1 des BSI-Gesetzes oder der öffentlichen Sicherheit, um damit eine Beeinträchtigung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme einer Kritischen Infrastruktur oder eines Unternehmens im besonderen öffentlichen Interesse abzuwenden, wenn Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, das auf die informationstechnischen Systeme bestimmbarer Infrastrukturen oder Unternehmen abzielen wird, und die in die Auskunft aufzunehmenden Daten im Einzelfall erforderlich sind, um den Betreiber der betroffenen Kritischen Infrastruktur oder das betroffene Unternehmen im besonderen öffentlichen Interesse vor dieser Beeinträchtigung zu warnen, über diese zu informieren oder bei deren Beseitigung zu beraten oder zu unterstützen.	8. an das Bundesamt für Sicherheit in der Informationstechnik zum Schutz der Versorgung der Bevölkerung in den Bereichen des § 57 Absatz 1 Satz 1 Nummer 1des BSI-Gesetzes oder der öffentlichen Sicherheit, um damit eine Beeinträchtigung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme einer Kritischen Infrastruktur oder eines Unternehmens im besonderen öffentlichen Interesse abzuwenden, wenn Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, das auf die informationstechnischen Systeme bestimmbarer Infrastrukturen oder Unternehmen abzielen wird, und die in die Auskunft aufzunehmenden Daten im Einzelfall erforderlich sind, um den Betreiber der betroffenen Kritischen Infrastruktur oder das betroffene Unternehmen im besonderen öffentlichen Interesse vor dieser Beeinträchtigung zu warnen, über diese zu informieren oder bei deren Beseitigung zu beraten oder zu unterstützen.	
927	(5) Die Auskunft nach Absatz 1 Satz 3 darf nur erteilt werden an	(5) Die Auskunft nach Absatz 1 Satz 3 darf nur erteilt werden an	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
928	8. an das Bundesamt für Sicherheit in der Informationstechnik zum Schutz der Versorgung der Bevölkerung in den Bereichen des § 2 Absatz 10 Satz 1 Nummer 1 des BSI-Gesetzes oder der öffentlichen Sicherheit, um damit eine Beeinträchtigung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme einer Kritischen Infrastruktur oder eines Unternehmens im besonderen öffentlichen Interesse abzuwenden, wenn Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, das auf die informationstechnischen Systeme bestimmbarer Infrastrukturen oder Unternehmen abzielen wird, und die in die Auskunft aufzunehmenden Daten im Einzelfall erforderlich sind, um den Betreiber der betroffenen Kritischen Infrastruktur oder das betroffene Unternehmen im besonderen öffentlichen Interesse vor dieser Beeinträchtigung zu warnen, über diese zu informieren oder bei deren Beseitigung zu beraten oder zu unterstützen.	8. an das Bundesamt für Sicherheit in der Informationstechnik zum Schutz der Versorgung der Bevölkerung in den Bereichen des § 57 Absatz 1 Satz 1 Nummer 1 des BSI-Gesetzes oder der öffentlichen Sicherheit, um damit eine Beeinträchtigung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme einer Kritischen Infrastruktur oder eines Unternehmens im besonderen öffentlichen Interesse abzuwenden, wenn Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, das auf die informationstechnischen Systeme bestimmbarer Infrastrukturen oder Unternehmen abzielen wird, und die in die Auskunft aufzunehmenden Daten im Einzelfall erforderlich sind, um den Betreiber der betroffenen Kritischen Infrastruktur oder das betroffene Unternehmen im besonderen öffentlichen Interesse vor dieser Beeinträchtigung zu warnen, über diese zu informieren oder bei deren Beseitigung zu beraten oder zu unterstützen.	Anpassung des Verweises auf das BSIG nF.
929	§ 214 Verfahren der nationalen Streitbeilegung	§ 214 Verfahren der nationalen Streitbeilegung	
930	(3) Sind bei Streitigkeiten über das Vorliegen eines Ablehnungsgrundes nach § 136 Absatz 4 Nummer 3, § 137 Absatz 3 Nummer 3, § 141 Absatz 2 Nummer 4, § 142 Absatz 4 Nummer 4, § 143 Absatz 4 Nummer 1, § 153 Absatz 4 Nummer 3 oder § 154 Absatz 4 Satz 2	(3) Sind bei Streitigkeiten über das Vorliegen eines Ablehnungsgrundes nach § 136 Absatz 4 Nummer 3, § 137 Absatz 3 Nummer 3, § 141 Absatz 2 Nummer 4, § 142 Absatz 4 Nummer 4, § 143 Absatz 4 Nummer 1, § 153 Absatz 4 Nummer 3 oder § 154 Absatz 4 Satz 2	Anpassung des Verweises auf das BSIG nF.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Nummer 4 Kritische Infrastrukturen im Sinne des § 2 Absatz 10 des BSI-Gesetzes betroffen, so entscheidet die Bundesnetzagentur im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik.	Nummer 4 kritische Anlagen im Sinne des § 2 Absatz 1 Nummer 19 des BSI-Gesetzes betroffen, so entscheidet die Bundesnetzagentur im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik.	
931		**Artikel 4** **Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz - EnWG)[3]**	
932	§ 11 Betrieb von Energieversorgungsnetzen	§ 11 Betrieb von Energieversorgungsnetzen	
933	(1) Betreiber von Energieversorgungsnetzen sind verpflichtet, ein sicheres, zuverlässiges und leistungsfähiges Energieversorgungsnetz diskriminierungsfrei zu betreiben, zu warten und bedarfsgerecht zu optimieren, zu verstärken und auszubauen, soweit es wirtschaftlich zumutbar ist. Sie haben insbesondere die Aufgaben nach den §§ 12 bis 16a zu erfüllen. Sie nehmen diese Aufgaben für ihr Energieversorgungsnetz in eigener Verantwortung wahr. Sie kooperieren und unterstützen sich bei der Wahrnehmung dieser Aufgaben; dies ist insbesondere für Maßnahmen anzuwenden, die sich auf das Netz eines anderen Betreibers von Energieversorgungsnetzen auswirken können. Die Verpflichtungen sind auch anzuwenden im Rahmen der Wahrnehmung der wirtschaftlichen Befugnisse der Leitung des vertikal integrierten Unternehmens und seiner Aufsichtsrechte nach § 7a Absatz 4 Satz 3. Der Ausbau eines L-Gasversorgungsnetzes ist nicht bedarfsgerecht im Sinne von Satz 1, wenn er auf Grund von Netzanschlüssen erfolgen muss, zu deren Einräumung der Betreiber des L-	(1) Betreiber von Energieversorgungsnetzen sind verpflichtet, ein sicheres, zuverlässiges und leistungsfähiges Energieversorgungsnetz diskriminierungsfrei zu betreiben, zu warten und bedarfsgerecht zu optimieren, zu verstärken und auszubauen, soweit es wirtschaftlich zumutbar ist. Sie haben insbesondere die Aufgaben nach den §§ 12 bis 16a zu erfüllen. Sie nehmen diese Aufgaben für ihr Energieversorgungsnetz in eigener Verantwortung wahr. Sie kooperieren und unterstützen sich bei der Wahrnehmung dieser Aufgaben; dies ist insbesondere für Maßnahmen anzuwenden, die sich auf das Netz eines anderen Betreibers von Energieversorgungsnetzen auswirken können. Die Verpflichtungen sind auch anzuwenden im Rahmen der Wahrnehmung der wirtschaftlichen Befugnisse der Leitung des vertikal integrierten Unternehmens und seiner Aufsichtsrechte nach § 7a Absatz 4 Satz 3. Der Ausbau eines L-Gasversorgungsnetzes ist nicht bedarfsgerecht im Sinne von Satz 1, wenn er auf Grund von Netzanschlüssen erfolgen muss, zu deren Einräumung der Betreiber des L-	

[3] Energiewirtschaftsgesetz vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 3 des Gesetzes vom 4. Januar 2023 (BGBl. 2023 I Nr. 9) geändert worden ist.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Gasversorgungsnetzes nicht nach den §§ 17 und 18 verpflichtet war.	Gasversorgungsnetzes nicht nach den §§ 17 und 18 verpflichtet war.	
934	(1a) Der Betrieb eines sicheren Energieversorgungsnetzes umfasst insbesondere auch einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind. Die Regulierungsbehörde erstellt hierzu im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik einen Katalog von Sicherheitsanforderungen und veröffentlicht diesen. Der Katalog der Sicherheitsanforderungen enthält auch Regelungen zur regelmäßigen Überprüfung der Erfüllung der Sicherheitsanforderungen. Ein angemessener Schutz des Betriebs eines Energieversorgungsnetzes liegt vor, wenn dieser Katalog der Sicherheitsanforderungen eingehalten und dies vom Betreiber dokumentiert worden ist. Die Einhaltung kann von der Regulierungsbehörde überprüft werden. Zu diesem Zwecke kann die Regulierungsbehörde nähere Bestimmungen zu Format, Inhalt und Gestaltung der Dokumentation nach Satz 4 treffen.	(1a) Das Bundesamt für Sicherheit in der Informationstechnik leitet die Meldungen nach § 31 Absatz 1 des BSI-Gesetzes von Betreibern von Energieversorgungsnetzen oder Energieanlagen sowie solche Meldungen über Sicherheitsvorfälle nach § 5 Absatz 2 und § 31 Absatz 1 des BSI-Gesetzes, bei welchen das Bundesamt für Sicherheit in der Informationstechnik Kenntnis von einer Relevanz für die Energieversorgungssicherheit und Erfüllung der Ziele nach § 1 erlangt, unverzüglich an die Bundesnetzagentur weiter. Die Bundesnetzagentur führt unverzüglich eine Bewertung der Auswirkungen der zugrundeliegenden Störungen auf die Energieversorgungssicherheit durch und übermittelt diese an das Bundesamt für Sicherheit in der Informationstechnik. Die Bundesnetzagentur kann von dem betroffenen Unternehmen die Herausgabe der zur Bewertung der Auswirkungen des Sicherheitsvorfalls auf die Energieversorgungssicherheit notwendigen Informationen, einschließlich personenbezogener Daten, verlangen. Das betroffene Unternehmen ist befugt, der Bundesnetzagentur die zur Bewertung der Auswirkungen des Sicherheitsvorfalls auf die Energieversorgungssicherheit notwendigen Informationen, einschließlich personenbezogener Daten zu übermitteln. Die Bundesnetzagentur kann bei der Durchführung der Bewertung nach Satz 2 die Betreiber von Übertragungs- und Fernleitungsnetzen einbeziehen. Das Bundesamt für Sicherheit in der Informationstechnik berücksichtigt die Bewertung der Bundesnetzagentur bei der Erfüllung der Aufgaben nach § 5 Absatz 2 und § 40 Absatz 2 des BSI-Gesetzes. Das Bundesamt für Sicherheit in der Informationstechnik und die Bundesnetzagentur haben sicherzustellen, dass die unbefugte Offenbarung der	Die Vorschrift entfällt, da die Verpflichtungen für Betreiber und Einrichtungen im Energiesektor zukünftig einheitlich im BSIG geregelt werden und die Aufsicht im Energiesektor durch das BSI erfolgt.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		ihnen nach diesem Absatz zur Kenntnis gelangten Informationen ausgeschlossen wird. Zugang zu den Akten des Bundesamtes für Sicherheit in der Informationstechnik sowie zu den Akten der Bundesnetzagentur in Angelegenheiten nach Absatz 1a bis Absatz 1b wird nicht gewährt. § 29 des Verwaltungsverfahrensgesetzes bleibt unberührt. § 42 des BSI-Gesetzes ist entsprechend anzuwenden.	
935	(1b) Betreiber von Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 8 des Gesetzes vom 17. Juli 2015 (BGBl. I S. 1324) geändert worden ist, in der jeweils geltenden Fassung als Kritische Infrastruktur bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind, haben innerhalb einer von der Regulierungsbehörde festzulegenden Frist einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme zu gewährleisten, die für einen sicheren Anlagenbetrieb notwendig sind. Die Regulierungsbehörde erstellt hierzu im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik einen Katalog von Sicherheitsanforderungen, in den auch die Bestimmung der Frist nach Satz 1 aufzunehmen ist, und veröffentlicht diesen. Für Telekommunikations- und elektronische Datenverarbeitungssysteme von Anlagen nach § 7 Absatz 1 des Atomgesetzes haben Vorgaben auf Grund des Atomgesetzes Vorrang. Die für die nukleare Sicherheit zuständigen Genehmigungs- und Aufsichtsbehörden des Bundes und der Länder sind bei der Erarbeitung des Katalogs von Sicherheitsanforderungen zu beteiligen. Der Katalog von Sicherheitsanforderungen enthält auch Regelungen zur regelmäßigen Überprüfung der		s.o.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Erfüllung der Sicherheitsanforderungen. Ein angemessener Schutz des Betriebs von Energieanlagen im Sinne von Satz 1 liegt vor, wenn dieser Katalog eingehalten und dies vom Betreiber dokumentiert worden ist. Die Einhaltung kann von der Bundesnetzagentur überprüft werden. Zu diesem Zwecke kann die Regulierungsbehörde nähere Bestimmungen zu Format, Inhalt und Gestaltung der Dokumentation nach Satz 6 treffen.		
936	(1c) Betreiber von Energieversorgungsnetzen und von solchen Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt wurden, haben		s.o.
937	1. Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer erheblichen Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage geführt haben,		s.o.
938	2. erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer erheblichen Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage führen können,		s.o.
939	über die Kontaktstelle unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik zu melden.		s.o.
940	Die Meldung muss Angaben zu der Störung, zu möglichen grenzübergreifenden Auswirkungen sowie zu den technischen Rahmenbedingungen,		s.o.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	insbesondere der vermuteten oder tatsächlichen Ursache und der betroffenen Informationstechnik, enthalten. Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat. Das Bundesamt für Sicherheit in der Informationstechnik hat die Meldungen unverzüglich an die Bundesnetzagentur weiterzuleiten. Das Bundesamt für Sicherheit in der Informationstechnik und die Bundesnetzagentur haben sicherzustellen, dass die unbefugte Offenbarung der ihnen nach Satz 1 zur Kenntnis gelangten Angaben ausgeschlossen wird. Zugang zu den Akten des Bundesamtes für Sicherheit in der Informationstechnik sowie zu den Akten der Bundesnetzagentur in Angelegenheiten nach § 11 Absatz 1a bis Absatz 1c wird nicht gewährt. § 29 des Verwaltungsverfahrensgesetzes bleibt unberührt. § 8e Absatz 1 des BSI-Gesetzes ist entsprechend anzuwenden.		
941	(1d) Betreiber von Energieversorgungsnetzen und von solchen Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt wurden, sind verpflichtet, spätestens bis zum 1. April jeden Jahres, die von ihnen betriebene Anlage beim Bundesamt für Sicherheit in der Informationstechnik zu registrieren und eine Kontaktstelle zu benennen. Das Bundesamt für Sicherheit in der Informationstechnik übermittelt die Registrierungen einschließlich der damit verbundenen Kontaktdaten an die Bundesnetzagentur. Die Registrierung eines Betreibers eines Energieversorgungsnetzes oder von solchen Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt wurden, kann das Bundesamt für Sicherheit in der		s.o.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Informationstechnik auch selbst vornehmen, wenn der Betreiber seine Pflicht zur Registrierung nicht erfüllt. Nimmt das Bundesamt für Sicherheit in der Informationstechnik eine solche Registrierung selbst vor, informiert es die Bundesnetzagentur darüber und übermittelt die damit verbundenen Kontaktdaten. Die Betreiber haben sicherzustellen, dass sie über die benannte oder durch das Bundesamt für Sicherheit in der Informationstechnik festgelegte Kontaktstelle jederzeit erreichbar sind. Die Übermittlung von Informationen durch das Bundesamt für Sicherheit in der Informationstechnik nach § 8b Absatz 2 Nummer 4 Buchstabe a des BSI-Gesetzes erfolgt an diese Kontaktstelle.		
942	(1e) Betreiber von Energieversorgungsnetzen und von solchen Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt wurden, haben spätestens ab dem 1. Mai 2023 in ihren informationstechnischen Systemen, Komponenten oder Prozessen, die für die Funktionsfähigkeit der von ihnen betriebenen Energieversorgungsnetze oder Energieanlagen maßgeblich sind, in angemessener Weise Systeme zur Angriffserkennung einzusetzen. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen. Dabei soll der Stand der Technik eingehalten werden. Der Einsatz von Systemen zur Angriffserkennung ist angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den möglichen Folgen eines Ausfalls oder einer Beeinträchtigung des betroffenen		s.o.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	Energieversorgungsnetzes oder der betroffenen Energieanlage steht.		
943	(1f) Betreiber von Energieversorgungsnetzen und von solchen Energieanlagen, die nach der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur gelten, haben dem Bundesamt für Sicherheit in der Informationstechnik erstmalig am 1. Mai 2023 und danach alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1d nachzuweisen. Das Bundesamt für Sicherheit in der Informationstechnik hat die hierfür eingereichten Nachweisdokumente unverzüglich an die Bundesnetzagentur weiterzuleiten. Das Bundesamt für Sicherheit in der Informationstechnik und die Bundesnetzagentur haben sicherzustellen, dass die unbefugte Offenbarung der ihnen nach Satz 1 zur Kenntnis gelangten Angaben ausgeschlossen wird. Das Bundesamt für Sicherheit in der Informationstechnik kann bei Mängeln in der Umsetzung der Anforderungen nach Absatz 1d oder in den Nachweisdokumenten nach Satz 1 im Einvernehmen mit der Bundesnetzagentur die Beseitigung der Mängel verlangen.		s.o.
944	(1g) Die Bundesnetzagentur legt bis zum 22. Mai 2023 im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik durch Allgemeinverfügung im Wege einer Festlegung nach § 29 Absatz 1 in einem Katalog von Sicherheitsanforderungen für das Betreiben von Energieversorgungsnetzen und Energieanlagen fest,	(1b) Die Bundesnetzagentur legt bis zum 22. Mai 2023 im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik durch Allgemeinverfügung im Wege einer Festlegung nach § 29 Absatz 1 in einem Katalog von Sicherheitsanforderungen für das Betreiben von Energieversorgungsnetzen und Energieanlagen fest,	
945	1. welche Komponenten kritische Komponenten im Sinne des § 2 Absatz 13 Satz 1 Nummer 3 Buchstabe a des BSI-Gesetzes sind oder	1. welche Komponenten kritische Komponenten im Sinne des § 2 Absatz 1 Nummer 20 Buchstabe c Doppelbuchstabe aa des BSI-Gesetzes sind oder	Anpassung des Verweises auf das BSIG nF.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
946	2. welche Funktionen kritisch bestimmte Funktionen im Sinne des § 2 Absatz 13 Satz 1 Nummer 3 Buchstabe b des BSI-Gesetzes sind.	2. welche Funktionen kritisch bestimmte Funktionen im Sinne des § 2 Absatz 1 Nummer 20 Buchstabe c Doppelbuchstabe bb des BSI-Gesetzes sind.	Anpassung des Verweises auf das BSIG nF.
947	Die Betreiber von Energieversorgungsnetzen und Energieanlagen, die durch Rechtsverordnung gemäß § 10 Absatz 1 Satz 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt wurden, haben die Vorgaben des Katalogs spätestens sechs Monate nach dessen Inkrafttreten zu erfüllen, es sei denn, in dem Katalog ist eine davon abweichende Umsetzungsfrist festgelegt worden. Der Katalog wird mit den Katalogen der Sicherheitsanforderungen nach § 11 Absatz 1a und 1b verbunden.		Die Vorschrift entfällt, da die Verpflichtungen für Betreiber und Einrichtungen im Energiesektor zukünftig einheitlich im BSIG geregelt werden und die Aufsicht im Energiesektor durch das BSI erfolgt.
948		(1c) Das Bundesamt für Sicherheit in der Informationstechnik kann im Einvernehmen mit der Bundesnetzagentur einen Katalog von Sicherheitsanforderungen erstellen und veröffentlicht diesen. Der Katalog der Sicherheitsanforderungen beschreibt geeignete Risikomanagementmaßnahmen nach § 30 Absatz 1 des BSI-Gesetzes. Dabei beteiligen die Bundesnetzagentur und das Bundesamt die Betreiber und deren Branchenverbände sowie die nukleare Sicherheit zuständigen Genehmigungs- und Aufsichtsbehörden des Bundes und der Länder. Der Katalog von Sicherheitsanforderungen enthält auch Regelungen zur regelmäßigen Überprüfung der Erfüllung seiner Sicherheitsanforderungen.	Die Verpflichtungen für Betreiber und Einrichtungen im Energiesektor werden durch die Neuerungen zentral im BSI-Gesetz geregelt. Da die Betreiber nach den bisherigen Regelungen des EnWG von der Bundesnetzagentur zu erstellende Sicherheitskataloge zu erfüllen hatten, wird mit dieser Vorschrift die Möglichkeit eingeführt, dass das BSI ähnliche Sicherheitskataloge mit der Bundesnetzagentur erstellt, um Mehraufwände für die Unternehmen im Nachweis der Anforderungen zu vermeiden.
949		**Artikel 5**	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		Gesetz über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren (Atomgesetz)[4]	
950	§ 44b Meldewesen für die Sicherheit in der Informationstechnik	§ 44b Meldewesen für die Sicherheit in der Informationstechnik	
951	Genehmigungsinhaber nach den §§ 6, 7 und 9 haben Beeinträchtigungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einer Gefährdung oder Störung der nuklearen Sicherheit der betroffenen kerntechnischen Anlage oder Tätigkeit führen können oder bereits geführt haben, unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik als zentrale Meldestelle zu melden. § 8b Absatz 1, 2 Nummer 1 bis 3, Nummer 4 Buchstabe a bis c und Absatz 7 des BSI-Gesetzes sind entsprechend anzuwenden. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, und der betroffenen Informationstechnik enthalten. Das Bundesamt für Sicherheit in der Informationstechnik leitet diese Meldungen unverzüglich an die für die nukleare Sicherheit und Sicherung zuständigen Genehmigungs- und Aufsichtsbehörden des Bundes und der Länder und an die von diesen bestimmten Sachverständigen nach § 20 weiter.	Genehmigungsinhaber nach den §§ 6, 7 und 9 haben Beeinträchtigungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einer Gefährdung oder Störung der nuklearen Sicherheit der betroffenen kerntechnischen Anlage oder Tätigkeit führen können oder bereits geführt haben, unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik als zentrale Meldestelle zu melden. § 40 Absatz 1, 2 Nummer 1 bis 3, Nummer 4 Buchstabe a bis c und Absatz 7 des BSI-Gesetzes sind entsprechend anzuwenden. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, und der betroffenen Informationstechnik enthalten. Das Bundesamt für Sicherheit in der Informationstechnik leitet diese Meldungen unverzüglich an die für die nukleare Sicherheit und Sicherung zuständigen Genehmigungs- und Aufsichtsbehörden des Bundes und der Länder und an die von diesen bestimmten Sachverständigen nach § 20 weiter.	[*Anm. BMI CI1 – In der Ressortabstimmung mit BMUV zu klären, ob nach dem 1. April 2023 (Automaustieg) noch Genehmigungsinhaber nach §§ 6, 7 und 9 AtomG existieren und weiterhin zur Meldung verpflichtet sein sollen (ggf. Zwischen-/Endlager).*]
952		**Artikel 6**	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
		Vertrauensdienstegesetz (VDG)[5]	
953		[*Anm. BMI CI1 – Änderungsbedarf durch DV I 2 im Rahmen dortiger Zuständigkeit zu ergänzen.*]	
954		**Artikel 7** **Gesetz zur Sicherung der Energieversorgung (Energiesicherungsgesetz – EnSiG)**[6]	
955	§ 17 Treuhandverwaltung von Unternehmen der kritischen Infrastruktur	§ 17 Treuhandverwaltung von Unternehmen der kritischen Infrastruktur	
956	(1) Ein Unternehmen, das selbst oder durch verbundene Unternehmen im Sinne von § 15 des Aktiengesetzes Kritische Infrastrukturen im Sinne von § 2 Absatz 10 des BSI-Gesetzes im Sektor Energie betreibt, kann unter Treuhandverwaltung gestellt werden, wenn die konkrete Gefahr besteht, dass ohne eine Treuhandverwaltung das Unternehmen seine dem Funktionieren des Gemeinwesens im Sektor Energie dienenden Aufgaben nicht erfüllen wird, und eine Beeinträchtigung der Versorgungssicherheit droht.	(1) Ein Unternehmen, das selbst oder durch verbundene Unternehmen im Sinne von § 15 des Aktiengesetzes kritische Anlagen im Sinne von § 2 Absatz 1 Nummer 19 des BSI-Gesetzes im Sektor Energie betreibt, kann unter Treuhandverwaltung gestellt werden, wenn die konkrete Gefahr besteht, dass ohne eine Treuhandverwaltung das Unternehmen seine dem Funktionieren des Gemeinwesens im Sektor Energie dienenden Aufgaben nicht erfüllen wird, und eine Beeinträchtigung der Versorgungssicherheit droht.	Anpassung des Verweises auf das BSIG nF.
957	§ 18 Enteignung zur Sicherung der Energieversorgung im Bereich der Kritischen Infrastruktur	§ 18 Enteignung zur Sicherung der Energieversorgung im Bereich der Kritischen Infrastruktur	
958	(2) Zulässige Gegenstände einer Enteignung zur Sicherung der Energieversorgung können sein:	(2) Zulässige Gegenstände einer Enteignung zur Sicherung der Energieversorgung können sein:	
959	1. Anteile an Unternehmen, die selbst oder durch verbundene Unternehmen im Sinne	1. Anteile an Unternehmen, die selbst oder durch verbundene Unternehmen im Sinne	Anpassung des Verweises auf das BSIG nF.

[5] Vertrauensdienstegesetz vom 18. Juli 2017 (BGBl. I S. 2745), das durch Artikel 2 des Gesetzes vom 18. Juli 2017 (BGBl. I S. 2745) geändert worden ist.

[6] Energiesicherungsgesetz vom 20. Dezember 1974 (BGBl. I S. 3681), das zuletzt durch Artikel 7 des Gesetzes vom 20. Dezember 2012 (BGBl. I S. 2560) geändert worden ist.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	von § 15 des Aktiengesetzes Kritische Infrastrukturen im Sinne von § 2 Absatz 10 des BSI-Gesetzes im Sektor Energie betreiben,	von § 15 des Aktiengesetzes kritische Anlagen im Sinne von § 2 Absatz 1 Nummer 19 des BSI-Gesetzes im Sektor Energie betreiben,	
960	Als Anteile im Sinne von Satz 1 Nummer 1 gelten auch Anteile an Personengesellschaften. Entsprechendes gilt, wenn abhängige Unternehmen im Sinne des Satzes 1 Nummer 3 in der Rechtsform einer Personengesellschaft geführt werden. Satz 1 gilt nicht für Unternehmen, die in der Rechtsform einer inländischen juristischen Person des öffentlichen Rechts geführt werden oder an denen ausschließlich inländische juristische Personen des öffentlichen Rechts unmittelbar oder mittelbar beteiligt sind. Inländischen juristischen Personen des öffentlichen Rechts stehen juristische Personen des öffentlichen Rechts aus einem Mitgliedstaat der Europäischen Union oder des Europäischen Wirtschaftsraums gleich.	Als Anteile im Sinne von Satz 1 Nummer 1 gelten auch Anteile an Personengesellschaften. Entsprechendes gilt, wenn abhängige Unternehmen im Sinne des Satzes 1 Nummer 3 in der Rechtsform einer Personengesellschaft geführt werden. Satz 1 gilt nicht für Unternehmen, die in der Rechtsform einer inländischen juristischen Person des öffentlichen Rechts geführt werden oder an denen ausschließlich inländische juristische Personen des öffentlichen Rechts unmittelbar oder mittelbar beteiligt sind. Inländischen juristischen Personen des öffentlichen Rechts stehen juristische Personen des öffentlichen Rechts aus einem Mitgliedstaat der Europäischen Union oder des Europäischen Wirtschaftsraums gleich.	
961	§ 29 Erleichterungen durch Durchführung von Stabilisierungsmaßnahmen	§ 29 Erleichterungen durch Durchführung von Stabilisierungsmaßnahmen	
962	(1) Beantragt ein Unternehmen, das selbst oder durch verbundene Unternehmen im Sinne von § 15 des Aktiengesetzes Kritische Infrastrukturen im Sinne von § 2 Absatz 10 des BSI-Gesetzes im Sektor Energie betreibt, beim Bund Stabilisierungsmaßnahmen, gelten für die Durchführung der Stabilisierungsmaßnahmen die nachfolgenden Regelungen. Stabilisierungsmaßnahmen im Sinne dieses Gesetzes sind alle Maßnahmen, die der Sicherung oder Wiederherstellung einer positiven Fortbestehensprognose nach § 19 Absatz 2 der Insolvenzordnung oder der Durchfinanzierung der Abwicklung des Unternehmens dienen. Ein Rechtsanspruch auf Stabilisierungsmaßnahmen	(1) Beantragt ein Unternehmen, das selbst oder durch verbundene Unternehmen im Sinne von § 15 des Aktiengesetzes kritische Anlagen im Sinne von § 2 Absatz 1 Nummer 19 des BSI-Gesetzes im Sektor Energie betreibt, beim Bund Stabilisierungsmaßnahmen, gelten für die Durchführung der Stabilisierungsmaßnahmen die nachfolgenden Regelungen. Stabilisierungsmaßnahmen im Sinne dieses Gesetzes sind alle Maßnahmen, die der Sicherung oder Wiederherstellung einer positiven Fortbestehensprognose nach § 19 Absatz 2 der Insolvenzordnung oder der Durchfinanzierung der Abwicklung des Unternehmens dienen. Ein	Anpassung des Verweises auf das BSIG nF.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	besteht nicht. Das Bundesministerium für Wirtschaft und Klimaschutz ist die zuständige Behörde für die Verhandlungen über Stabilisierungsmaßnahmen mit den in Satz 1 genannten Unternehmen. Anträge sind bei dem Bundesministerium für Wirtschaft und Klimaschutz zu stellen, das im Einvernehmen mit dem Bundesministerium der Finanzen und dem Bundeskanzleramt über die Anträge entscheidet.	Rechtsanspruch auf Stabilisierungsmaßnahmen besteht nicht. Das Bundesministerium für Wirtschaft und Klimaschutz ist die zuständige Behörde für die Verhandlungen über Stabilisierungsmaßnahmen mit den in Satz 1 genannten Unternehmen. Anträge sind bei dem Bundesministerium für Wirtschaft und Klimaschutz zu stellen, das im Einvernehmen mit dem Bundesministerium der Finanzen und dem Bundeskanzleramt über die Anträge entscheidet.	
963		**Artikel 8** **Gesetz über den Bundesnachrichtendienst (BND-Gesetz)**[7]	
964	§ 24 Eignungsprüfung	§ 24 Eignungsprüfung	
965	(5) Die im Rahmen einer Eignungsprüfung erhobenen personenbezogenen Daten dürfen nur zum Zweck der Eignungsprüfung verwendet werden. § 5 Absatz 7 Satz 2 bis 8 des BSI-Gesetzes gilt entsprechend. Der Bundesnachrichtendienst darf die erhobenen personenbezogenen Daten speichern, soweit dies zur Durchführung der Eignungsprüfung erforderlich ist. Die Auswertung ist unverzüglich nach der Erhebung durchzuführen.	(5) Die im Rahmen einer Eignungsprüfung erhobenen personenbezogenen Daten dürfen nur zum Zweck der Eignungsprüfung verwendet werden. § 8 Absatz 7 Satz 2 bis 8 des BSI-Gesetzes gilt entsprechend. Der Bundesnachrichtendienst darf die erhobenen personenbezogenen Daten speichern, soweit dies zur Durchführung der Eignungsprüfung erforderlich ist. Die Auswertung ist unverzüglich nach der Erhebung durchzuführen.	Anpassung des Verweises auf das BSIG nF.
966		**Artikel 9** **Gesetz über den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation und bei Telemedien (Telekommunikation-Telemedien-Datenschutz-Gesetz – TTDSG)**[8]	

[7] BND-Gesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2979), das zuletzt durch Artikel 3 des Gesetzes vom 5. Juli 2021 (BGBl. I S. 2274) geändert worden ist.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
967	§ 19 Technische und organisatorische Vorkehrungen	§ 19 Technische und organisatorische Vorkehrungen	
968	(4) Anbieter von Telemedien haben, soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass	(4) Anbieter von Telemedien haben, soweit dies technisch möglich und wirtschaftlich zumutbar ist, im Rahmen ihrer jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass	
969	1. kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und	1. kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und	
970	2. diese gesichert sind gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind.	2. diese gesichert sind gegen Störungen, auch soweit sie durch äußere Angriffe bedingt sind.	
971	Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen. Eine Vorkehrung nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens. Anordnungen des Bundesamtes für Sicherheit in der Informationstechnik nach § 7d Satz 1 BSI-Gesetz bleiben unberührt.	Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen. Eine Vorkehrung nach Satz 1 ist insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens. Anordnungen des Bundesamtes für Sicherheit in der Informationstechnik nach § 17 Satz 1 des BSI-Gesetzes bleiben unberührt.	Anpassung des Verweises auf das BSIG nF.
972		**Artikel 10** **Sozialgesetzbuch Fünftes Buch - Gesetzliche Krankenversicherung (SGB V)**[9]	

[9] Sozialgesetzbuch Fünftes Buch vom 20. Dezember 1988 (BGBl. I S. 2477, 2482), das zuletzt durch Artikel 1 des Gesetzes vom 7. November 2022 (BGBl. I S. 1990) geändert worden ist.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
973	§ 75b Richtlinie zur IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung	§ 75b Richtlinie zur IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung	
974	(4) Die Richtlinie ist für die an der vertragsärztlichen und vertragszahnärztlichen Versorgung teilnehmenden Leistungserbringer verbindlich. Die Richtlinie ist nicht anzuwenden für die vertragsärztliche und vertragszahnärztliche Versorgung im Krankenhaus, soweit dort bereits angemessene Vorkehrungen getroffen werden. Angemessene Vorkehrungen im Sinne von Satz 2 gelten als getroffen, wenn die organisatorischen und technischen Vorkehrungen nach § 8a Absatz 1 des BSI-Gesetzes oder entsprechende branchenspezifische Sicherheitsstandards umgesetzt wurden.	(4) Die Richtlinie ist für die an der vertragsärztlichen und vertragszahnärztlichen Versorgung teilnehmenden Leistungserbringer verbindlich. Die Richtlinie ist nicht anzuwenden für die vertragsärztliche und vertragszahnärztliche Versorgung im Krankenhaus, soweit dort bereits angemessene Vorkehrungen getroffen werden. Angemessene Vorkehrungen im Sinne von Satz 2 gelten als getroffen, wenn die organisatorischen und technischen Vorkehrungen nach § 39 Absatz 1 des BSI-Gesetzes oder entsprechende branchenspezifische Sicherheitsstandards umgesetzt wurden.	Anpassung des Verweises auf das BSIG nF.
975	§ 75c IT-Sicherheit in Krankenhäusern	§ 75c IT-Sicherheit in Krankenhäusern	
976	(1) Ab dem 1. Januar 2022 sind Krankenhäuser verpflichtet, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung des Krankenhauses oder der Sicherheit der verarbeiteten Patienteninformationen steht. Die informationstechnischen Systeme sind spätestens alle	(1) Ab dem 1. Januar 2022 sind Krankenhäuser verpflichtet, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung des Krankenhauses oder der Sicherheit der verarbeiteten Patienteninformationen steht. Die informationstechnischen Systeme sind spätestens alle	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	zwei Jahre an den aktuellen Stand der Technik anzupassen.	zwei Jahre an den aktuellen Stand der Technik anzupassen.	
977	(2) Die Krankenhäuser können die Verpflichtungen nach Absatz 1 insbesondere erfüllen, indem sie einen branchenspezifischen Sicherheitsstandard für die informationstechnische Sicherheit der Gesundheitsversorgung im Krankenhaus in der jeweils gültigen Fassung anwenden, dessen Eignung vom Bundesamt für Sicherheit in der Informationstechnik nach § 8a Absatz 2 des BSI-Gesetzes festgestellt wurde.	(2) Die Krankenhäuser können die Verpflichtungen nach Absatz 1 insbesondere erfüllen, indem sie einen branchenspezifischen Sicherheitsstandard für die informationstechnische Sicherheit der Gesundheitsversorgung im Krankenhaus in der jeweils gültigen Fassung anwenden, dessen Eignung vom Bundesamt für Sicherheit in der Informationstechnik nach § 30 Absatz 12 des BSI-Gesetzes festgestellt wurde.	Anpassung des Verweises auf das BSIG nF.
978	(3) Die Verpflichtung nach Absatz 1 gilt für alle Krankenhäuser, soweit sie nicht ohnehin als Betreiber Kritischer Infrastrukturen gemäß § 8a des BSI-Gesetzes angemessene technische Vorkehrungen zu treffen haben.	(3) Die Verpflichtung nach Absatz 1 gilt für alle Krankenhäuser, soweit sie nicht ohnehin als Betreiber kritischer Anlagen gemäß §§ 30 und 39 des BSI-Gesetzes Risikomanagementmaßnahmen und angemessene technische Vorkehrungen zu treffen haben.	Anpassung des Verweises auf das BSIG nF.
979		**Artikel 11** **Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (Messstellenbetriebsgesetz – MsbG)**[10]	
980	§ 24 Zertifizierung des Smart-Meter-Gateway	§ 24 Zertifizierung des Smart-Meter-Gateway	
981	(2) Für die Zertifizierung sind § 9 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821) sowie die BSI-Zertifizierungs- und Anerkennungsverordnung vom 17. Dezember 2014 (BGBl. I S. 2231) in der jeweils geltenden Fassung anzuwenden.	(2) Für die Zertifizierung sind § 54 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821) sowie die BSI-Zertifizierungs- und Anerkennungsverordnung vom 17. Dezember 2014 (BGBl. I S. 2231) in der jeweils geltenden Fassung anzuwenden.	Anpassung des Verweises auf das BSIG nF.

[10] Messstellenbetriebsgesetz vom 29. August 2016 (BGBl. I S. 2034), das zuletzt durch Artikel 11 des Gesetzes vom 20. Juli 2022 (BGBl. I S. 1237) geändert worden ist.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
982		**Artikel 12** **De-Mail-Gesetz (De-Mail-G)**	
983	§ 18 Voraussetzungen der Akkreditierung; Nachweis	§ 18 Voraussetzungen der Akkreditierung; Nachweis	
984	(1) Als Diensteanbieter kann nur akkreditiert werden, wer	(1) Als Diensteanbieter kann nur akkreditiert werden, wer	
985	1. die für den Betrieb von De-Mail-Diensten erforderliche Zuverlässigkeit und Fachkunde besitzt,	1. die für den Betrieb von De-Mail-Diensten erforderliche Zuverlässigkeit und Fachkunde besitzt,	
986	2. eine geeignete Deckungsvorsorge trifft, um seinen gesetzlichen Verpflichtungen zum Ersatz von Schäden nachzukommen,	2. eine geeignete Deckungsvorsorge trifft, um seinen gesetzlichen Verpflichtungen zum Ersatz von Schäden nachzukommen,	
987	3. die technischen und organisatorischen Anforderungen an die Pflichten nach den §§ 3 bis 13 sowie nach § 16 in der Weise erfüllt, dass er die Dienste zuverlässig und sicher erbringt, er mit den anderen akkreditierten Diensteanbietern zusammenwirkt und für die Erbringung der Dienste ausschließlich technische Geräte verwendet, die sich im Gebiet der Mitgliedstaaten der Europäischen Union oder eines anderen Vertragsstaates des Abkommens über den Europäischen Wirtschaftsraum befinden,	3. die technischen und organisatorischen Anforderungen an die Pflichten nach den §§ 3 bis 13 sowie nach § 16 in der Weise erfüllt, dass er die Dienste zuverlässig und sicher erbringt, er mit den anderen akkreditierten Diensteanbietern zusammenwirkt und für die Erbringung der Dienste ausschließlich technische Geräte verwendet, die sich im Gebiet der Mitgliedstaaten der Europäischen Union oder eines anderen Vertragsstaates des Abkommens über den Europäischen Wirtschaftsraum befinden,	
988	4. bei der Gestaltung und dem Betrieb der De-Mail-Dienste die datenschutzrechtlichen Anforderungen erfüllt.	4. bei der Gestaltung und dem Betrieb der De-Mail-Dienste die datenschutzrechtlichen Anforderungen erfüllt.	

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
989	(3) Die Voraussetzungen nach Absatz 1 werden wie folgt nachgewiesen:	(3) Die Voraussetzungen nach Absatz 1 werden wie folgt nachgewiesen:	
990	3. die Erfüllung der technischen und organisatorischen Anforderungen an die Pflichten im Sinne des Absatzes 1 Nummer 3 durch vom Bundesamt für Sicherheit in der Informationstechnik nach § 9 Absatz 2 Satz 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik zertifizierten IT-Sicherheitsdienstleistern erteilte Testate; das Zusammenwirken mit den anderen akkreditierten Diensteanbietern kann nur nach ausreichenden Prüfungen bestätigt werden; die Sicherheit der Dienste kann nur nach einer umfassenden im Rahmen der Vergabe der Testate stattfindenden Prüfung des Sicherheitskonzepts und der eingesetzten IT-Infrastrukturen bestätigt werden; zum Zeitpunkt des Inkrafttretens des Gesetzes erteilte Zertifikate können berücksichtigt werden;	3. die Erfüllung der technischen und organisatorischen Anforderungen an die Pflichten im Sinne des Absatzes 1 Nummer 3 durch vom Bundesamt für Sicherheit in der Informationstechnik nach § 54 Absatz 2 Satz 1 des BSI-Gesetzes zertifizierten IT-Sicherheitsdienstleistern erteilte Testate; das Zusammenwirken mit den anderen akkreditierten Diensteanbietern kann nur nach ausreichenden Prüfungen bestätigt werden; die Sicherheit der Dienste kann nur nach einer umfassenden im Rahmen der Vergabe der Testate stattfindenden Prüfung des Sicherheitskonzepts und der eingesetzten IT-Infrastrukturen bestätigt werden; zum Zeitpunkt des Inkrafttretens des Gesetzes erteilte Zertifikate können berücksichtigt werden;	Anpassung des Verweises auf das BSIG nF.
991		**Artikel 13** **Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz – EGovG)**[11]	
992	§ 10 Umsetzung von Standardisierungsbeschlüssen des IT-Planungsrates	§ 10 Umsetzung von Standardisierungsbeschlüssen des IT-Planungsrates	
993	Fasst der Planungsrat für die IT-Zusammenarbeit der öffentlichen Verwaltung zwischen Bund und Ländern (IT-Planungsrat) einen Beschluss über	Fasst der Planungsrat für die IT-Zusammenarbeit der öffentlichen Verwaltung zwischen Bund und Ländern (IT-Planungsrat) einen Beschluss über	Löschung des Verweises auf das BSIG wegen Entfernung IT-Rat als Entscheidungsgremium, welches auf

[11] E-Government-Gesetz vom 25. Juli 2013 (BGBl. I S. 2749), das zuletzt durch Artikel 1 des Gesetzes vom 16. Juli 2021 (BGBl. I S. 2941) geändert worden ist.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
	fachunabhängige und fachübergreifende IT-Interoperabilitäts- oder IT-Sicherheitsstandards gemäß § 1 Absatz 1 Satz 1 Nummer 2 und § 3 des Vertrages über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Artikel 91c GG (BGBl. 2010 I S. 662, 663), so beschließt der Rat der IT-Beauftragten der Bundesregierung (IT-Rat) die Umsetzung dieses Beschlusses innerhalb der Bundesverwaltung. § 12 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik gilt entsprechend.	fachunabhängige und fachübergreifende IT-Interoperabilitäts- oder IT-Sicherheitsstandards gemäß § 1 Absatz 1 Satz 1 Nummer 2 und § 3 des Vertrages über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Artikel 91c GG (BGBl. 2010 I S. 662, 663), so beschließen die Ressorts in einem geeigneten Gremium oder durch Einvernehmen aller Bundesministerien die Umsetzung dieses Beschlusses innerhalb der Bundesverwaltung.	untergesetzlicher Ebene eingerichtet wird.
994		**Artikel 14** **Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0)[12]**	
995	Art. 6 Evaluierung	Art. 6 Evaluierung	
996	(1) Das Bundesministerium des Innern, für Bau und Heimat berichtet dem Deutschen Bundestag unter Einbeziehung von wissenschaftlichem Sachverstand über die Wirksamkeit der in diesem Gesetz enthaltenen Maßnahmen für die Erreichung der mit diesem Gesetz verfolgten Ziele	(1) Das Bundesministerium des Innern, für Bau und Heimat berichtet dem Deutschen Bundestag unter Einbeziehung von wissenschaftlichem Sachverstand über die Wirksamkeit der in diesem Gesetz enthaltenen Maßnahmen für die Erreichung der mit diesem Gesetz verfolgten Ziele	
997	1. bis zum 1. Mai 2023 hinsichtlich des § 2 Absatz 10, der §§ 8a, 8b, 8d und 8e sowie § 10 Absatz 1 des BSI-Gesetzes (Artikel 1) und	bis zum 1. Mai 2023 hinsichtlich des § 2 Absatz 10, der §§ 8a, 8b, 8d und 8e sowie § 10 Absatz 1 des BSI-Gesetzes (Artikel 1).	
998	2. bis zum 1. Mai 2025 hinsichtlich des Gesetzes im Übrigen.		Die bis zum 1. Mai 2025 durchzuführende Evaluierung der übrigen Vorschriften des IT-SiG 2.0 erübrigt sich da diese in weiten Teilen im Zuge der NIS-2-Umsetzung

[12] Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (BGBl. S. 1122) vom 18. Mai 2021.

Zeile	aktuelle Fassung	NIS2UmsuCG	Begründung
			geändert werden. Die unveränderten Vorschriften sind bereits durch dieses Gesetz bestätigt. Da die NIS-2-Richtlinie bereits einer Evaluierung durch die Kommission unterliegt (Art. 40 NIS-2) ist eine (auf den Mitgliedstaat Deutschland isolierte) Evaluierung der Umsetzung nicht zielführend.
999		**Artikel 15** **Inkrafttreten**	
1000		(1) Dieses Gesetz tritt vorbehaltlich des Absatzes 2 am 1. Oktober 2024 in Kraft.	Bei einer Verkündung im März 2024 stehen den Einrichtungen noch sechs Monate für die Umsetzung der in diesem Gesetz enthaltenen Verpflichtungen zur Verfügung. Der hier genannte Zeitpunkt ist der letzte Quartalsbeginn vor Ablauf der Umsetzungsfrist des Artikel 41 NIS-2-Richtlinie am 17. Oktober 2024. Im Übrigen sind die für die Verpflichtungen von wesentlichen und wichtigen Einrichtungen maßgeblichen Inhalte der NIS-2-Richtlinie bereits seit dem Kommissionsentwurf aus Dezember 2020 bekannt.
1001		(2) Artikel 2 tritt am Tag nach der Verkündung in Kraft.	Die überarbeitete Ermächtigung zum Erlass einer Rechtsverordnung nach § 10 Abs. 1b BSIG muss bereits zuvor in Kraft treten, damit diese zum Tag des Inkrafttretens des Gesetzes im Übrigen bereits erlassen sein kann.

* * *

Begründung

A. Allgemeiner Teil

I. Zielsetzung und Notwendigkeit der Regelungen

Bereits in der vergangenen Legislaturperiode wurden Vorhaben zur Erhöhung der IT-Sicherheit umgesetzt. Hervorzuhaben ist das zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0), das im Jahr 2021 verkündet wurde.

Die Umsetzung der Vorgaben der NIS-2-Richtlinie wird mit einer Neugliederung des BSIG verbunden. Entsprechend dem Auftrag aus dem Koalitionsvertrag für die 20. Legislaturperiode, Zeile 438, wird daher das IT-Sicherheitsrecht weiterentwickelt.

II. Wesentlicher Inhalt des Entwurfs

Die unionsrechtlichen Vorgaben der NIS-2-Richtlinie werden im Rahmen einer Anpassung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) sowie einzelner Fachgesetze umgesetzt. Des Weiteren wird das Informationssicherheitsmanagement in der Bundesverwaltung gestärkt. Im Einzelnen

- Einführung der vorgegebenen Einrichtungskategorien besonders wichtige und wichtige Einrichtungen, die eine signifikante Ausweitung des bisher auf Betreiber Kritischer Infrastrukturen, Anbieter digitaler Dienste und Unternehmen im besonderen öffentlichen Interesse beschränkten Anwendungsbereichs, vorsieht.
- Weiterführung der Einrichtungskategorie KRITIS als zusätzliche Kategorie für Unternehmen, die besonders schützenswert sind, mit entsprechenden Anforderungen.
- Der Katalog der Mindestsicherheitsanforderungen des Art. 21 Abs. 2 NIS-2-Richtlinie wird in das BSIG übernommen, wobei in der Intensität der jeweiligen Maßnahme aus Gründen der Verhältnismäßigkeit zwischen den Kategorien ausdifferenziert wird.
- Gesetzliche Verankerung wesentlicher nationaler Anforderungen an das Informationssicherheitsmanagement des Bundes und Abbildung der zugehörigen Rollen und Verantwortlichkeiten.
- Harmonisierung der Anforderungen an Einrichtungen der Bundesverwaltung aus nationalen und unionsrechtlichen Vorgaben, um ein insgesamt kohärentes und handhabbares Regelungsregime zu gewährleisten.
- Einführung eines dreistufigen Melderegimes, wodurch der bürokratische Aufwand für die Einrich-tungen im Rahmen des Umsetzungsspielraums minimiert und mögliche Synergien mit weiteren Meldepflichten – insbesondere zum Störungs-Monitoring des geplanten KRITIS-Dachgesetzes – gesucht und genutzt werden.
- Ergänzung des Instrumentariums des BSI bei der Aufsicht: Es wird ein der EU-Datenschutzgrundverordnung nachempfundener Bußgeldrahmen, der zwischen KRITIS und besonders wichtigen Einrichtungen sowie andererseits wichtigen Einrichtungen unterscheidet, umgesetzt.
- Umsetzung einer Ausschlussklausel für Unternehmen, die einen besonderen Bezug zum Sicherheits- und Verteidigungsbereich aufweisen. Für solche Einrichtungen gelten dann die jeweils einschlägigen Vorgaben für den Sicherheits- bzw. Verteidigungsbereich.
- Etablierung eines CISO Bund als zentralem Koordinator für Maßnahmen zur Informationssicherheit in Einrichtungen der Bundesverwaltung und zur Unterstützung der Ressorts bei der Umsetzung der Vorgaben für das Informationssicherheitsmanagement.

- Weiterentwicklung der BSI KRITIS VO, sodass eine Erfassung von Einrichtungen unterhalb der Size-Cap-Rule, für die die NIS-2-Richtlinie als Sonderfall eine Identifizierung anhand von Kritikalitätskriterien vorsieht, erfolgen kann.

III. Alternativen

Keine.

IV. Gesetzgebungskompetenz

Für die Änderungen des BSIG (Artikel 1), die den rein technischen Schutz der Informationstechnik von und für Einrichtungen betreffen, folgt die Gesetzgebungskompetenz des Bundes aus Artikel 73 Absatz 1 Nummer 7 (Telekommunikation) Grundgesetz (GG) sowie aus Artikel 74 Absatz 1 Nummer 11 GG (Recht der Wirtschaft, einschließlich gefahrenabwehrrechtlicher Annexkompetenz) in Verbindung mit Artikel 72 Absatz 2 GG.

Für Änderungen, welche die Befugnisse des Bundesamtes zum Schutz der Bundesverwaltung erweitern, hat der Bund eine Gesetzgebungskompetenz kraft Natur der Sache.

Die Zuständigkeit des Bundes für Regelungen zur bundesweiten Information einschließlich eventueller Empfehlungen und Warnungen von Verbraucherinnen und Verbrauchern auf dem Gebiet der Informationssicherheit folgt mit Blick auf die gesamtstaatliche Verantwortung der Bundesregierung ebenfalls aus der Natur der Sache (Staatsleitung), denn Fragen zur Sicherheit in der Informationstechnik haben bei stetig zunehmender Digitalisierung und Vernetzung aller Lebensbereiche regelmäßig überregionale Auswirkungen. Der Bund hat darüber hinaus die ausschließliche Gesetzgebungskompetenz nach Artikel 73 Absatz 1 Nummer 8 GG für die Rechtsverhältnisse der im Dienst des Bundes und der bundesunmittelbaren Körperschaften des öffentlichen Rechts stehenden Personen.

Die Änderungen des Telekommunikationsgesetzes (TKG) in Artikel [●] beruhen auf der Gesetzgebungskompetenz des Bundes aus Artikel 73 Absatz 1 Nummer 7 GG und auf Artikel 74 Absatz 1 Nummer 11 GG (Recht der Wirtschaft) in Verbindung mit Artikel 72 Absatz 2 GG.

Die Gesetzgebungskompetenz des Bundes für die Regelungen der Bußgeldvorschriften und Ordnungswidrigkeiten im Artikel 1 folgt aus Artikel 74 Absatz 1 Nummer 1 GG (Strafrecht).

V. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen

Der Gesetzentwurf ist mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen vereinbar. Er dient in weiten Teilen der Umsetzung der NIS-2-Richtlinie.

VI. Gesetzesfolgen

1. Rechts- und Verwaltungsvereinfachung

[●]

2. Nachhaltigkeitsaspekte

[●]

3. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

4. Erfüllungsaufwand

a. Erfüllungsaufwand für die Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

b. Erfüllungsaufwand für die Wirtschaft

[*Anm. BMI CI1 – Das Statistische Bundesamt (StBA) hatte nach inhaltlicher Finalisierung der NIS-2-Richtlinie eine Folgekostenschätzung erstellt. Diese wird nun unter Zugrundelegung des Referentenentwurfs plausibilisiert und die ausstehenden Angaben werden nachgetragen.*]

[●]

- § [●]: [●]. Hierfür entsteht der Wirtschaft ein jährlicher Erfüllungsaufwand in Höhe von circa [●] Euro.

c. Erfüllungsaufwand für die Verwaltung

[*Anm. BMI CI1 – Der EA Verwaltung im BMI inkl. Geschäftsbereich wird im Rahmen der Hausabstimmung abgefragt. Der EA Verwaltung für die übrigen Ressorts wird dann im Rahmen der Ressortabstimmung abgefragt.*]

Der Verwaltung entsteht für die Erfüllung der im Gesetz vorgesehenen zusätzlichen Aufgaben insgesamt ein Aufwand von insgesamt [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit einem jährlichen Erfüllungsaufwand in Höhe von [●] Euro. Davon entfallen [●] Euro auf jährliche Personalkosten und [●] Euro auf jährliche Sachkosten. Durch die gesetzliche Änderung entstehen einmalige Sachkosten in Höhe von [●] Euro.

Bundeskanzleramt (BKAmt)

Beim BKAmt entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

- § [●]. Hierfür benötigt das BKAmt [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●]. Euro jährlich.

Bundesministerium für Wirtschaft und Klimaschutz (BMWK)

Beim BMWK entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

- § [●]. Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●]. Euro jährlich.

Bundesministerium der Finanzen (BMF)

Beim BMF entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

- § [●]. Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●]. Euro jährlich.

Bundesministerium des Innern und für Heimat (BMI)

Beim BMI entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

- § [●]. Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●]. Euro jährlich.

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Beim BSI entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

- § [●]. Hierfür benötigt das BSI [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●]. Euro jährlich.

Bundesamt für Bevölkerungs- und Katastrophenschutz (BBK)

Beim BBK entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

- § [●]. Hierfür benötigt das BBK [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●]. Euro jährlich.

Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS)

Bei der BDBOS entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

- § [●]. Hierfür benötigt die BDBOS [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●]. Euro jährlich.

Auswärtiges Amt (AA)

Beim AA entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

- § [●]. Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●]. Euro jährlich.

Bundesministerium der Justiz (BMJ)

Beim BMJ entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

- § [●]. Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●]. Euro jährlich.

Bundesministerium für Arbeit und Soziales (BMAS)

Beim BMAS entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

- § [●]. Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●]. Euro jährlich.

Bundesministerium der Verteidigung (BMVg)

Beim BMVg entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

- § [●]. Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●]. Euro jährlich.

Bundesministerium für Ernährung und Landwirtschaft (BMEL)

Beim BMEL entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

- § [●]. Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●]. Euro jährlich.

Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ)

Beim BMFSFJ entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

- § [●]. Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●]. Euro jährlich.

Bundesministerium für Gesundheit (BMG)

Beim BMG entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

- § [●]. Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●]. Euro jährlich.

Bundesministerium für Digitales und Verkehr (BMDV)

Beim BMDV entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

- § [●]. Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●]. Euro jährlich.

Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)

Beim BMUV entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

- § [●]. Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●]. Euro jährlich.

Bundesministerium für Bildung und Forschung (BMBF)

Beim BMBF entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

- § [●]. Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●]. Euro jährlich.

Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (BMZ)

Beim BMZ entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

- § [●]. Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●]. Euro jährlich.

Bundesministerium für Wohnen, Stadtentwicklung und Bauwesen (BMWSB)

Beim BMWSB entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

- § [●]. Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●]. Euro jährlich.

Bundesbeauftragter für den Datenschutz und für die Informationsfreiheit (BfDI)

Beim BfDI entsteht ein Erfüllungsaufwand in Höhe von [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit jährlichen Personalkosten in Höhe von [●] Euro und Sacheinzelkosten in Höhe von [●] Euro.

- § [●]. Hierfür benötigt das Ministerium [●] Planstellen/Stellen ([●] hD; [●] gD; [●] mD) mit Personalkosten in Höhe von jährlich [●] Euro sowie Sacheinzelkosten in Höhe von [●]. Euro jährlich.

VII. **Weitere Kosten**

Keine.

5. **Weitere Gesetzesfolgen**

[●]

VIII. **Befristung; Evaluierung**

Eine Evaluierung oder Befristung ist nicht vorgesehen.

B. Besonderer Teil

[*Anm. BMI CI1 – Die Begründungen der einzelnen Änderungen sind der Spalte „Begründung“ in der Synopsentabelle zu entnehmen.*]

* * *