Formulierungshilfe

der Bundesregierung

Zusammenstellung

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

– Drucksache 20/13184 –

mit den Beschlüssen des Ausschusses für Inneres und Heimat (4. Ausschuss)

Entwurf		Beschlüsse des 4. Ausschusses	
Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung		**Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung**	
(NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz) *) 1)		**(NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz) *))**	
Vom ...		**Vom ...**	
Der Bundestag hat das folgende Gesetz beschlossen:		Der Bundestag hat das folgende Gesetz beschlossen:	
Inhaltsübersicht		Inhaltsübersicht	
Artikel 1	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz – BSIG)	Artikel 1	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz – BSIG)
Artikel 2	Änderung des BND-Gesetzes	Artikel 2	Änderung des BND-Gesetzes
Artikel 3	Änderung der Sicherheitsüberprüfungsfeststellungsverordnung	Artikel 3	Änderung der Sicherheitsüberprüfungsfeststellungsverordnung
Artikel 4	Änderung der Besonderen Gebührenverordnung des Bundesministeriums des Innern, für Bau und Heimat für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich		
Artikel 5	Änderung des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes	Artikel 4	Änderung des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes
Artikel 6	Änderung der Gleichstellungsbeauftragtenwahlverordnung	Artikel 5	Änderung der Gleichstellungsbeauftragtenwahlverordnung

*) Notifiziert gemäß 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).

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).

Entwurf		Beschlüsse des 4. Ausschusses	
Artikel 7	Änderung des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme	Artikel 6	Änderung des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme
Artikel 8	Änderung der BSI-Zertifizierungs- und Anerkennungsverordnung	Artikel 7	Änderung der BSI-Zertifizierungs- und Anerkennungsverordnung
		Artikel 8	Änderung der BSI-Kritisverordnung
Artikel 9	Änderung der BSI-IT-Sicherheitskennzeichenverordnung	Artikel 9	Änderung der BSIIT-Sicherheitskennzeichenverordnung
Artikel 10	Änderung des De-Mail-Gesetzes	Artikel 10	Änderung des De-Mail-Gesetzes
Artikel 11	Änderung des E-Government-Gesetz	Artikel 11	Änderung des E-Government-Gesetz
Artikel 12	Änderung der Passdatenerfassungs- und Übermittlungsverordnung	Artikel 12	Änderung der Passdatenerfassungs- und Übermittlungsverordnung
Artikel 13	Änderung der Personalausweisverordnung	Artikel 13	Änderung der Personalausweisverordnung
Artikel 14	Änderung des Hinweisgeberschutzgesetzes	Artikel 14	Änderung des Hinweisgeberschutzgesetzes
Artikel 15	Änderung der Kassensicherungsverordnung	Artikel 15	Änderung der Kassensicherungsverordnung
Artikel 16	Änderung des Atomgesetzes	Artikel 16	Änderung des Atomgesetzes
Artikel 17	Änderung des Energiewirtschaftsgesetzes	Artikel 17	Änderung des Energiewirtschaftsgesetzes
Artikel 18	Änderung des Messstellenbetriebsgesetzes	Artikel 18	Änderung des Messstellenbetriebsgesetzes
Artikel 19	Änderung des Energiesicherungsgesetzes	Artikel 19	Änderung des Energiesicherungsgesetzes
Artikel 20	Änderung des Wärmeplanungsgesetzes	Artikel 20	Änderung des Wärmeplanungsgesetzes
Artikel 21	Änderung des Fünften Buches Sozialgesetzbuch	Artikel 21	Änderung des Fünften Buches Sozialgesetzbuch
Artikel 22	Änderung der Digitale Gesundheitsanwendungen-Verordnung	Artikel 22	Änderung der Digitale Gesundheitsanwendungen-Verordnung

Entwurf		Beschlüsse des 4. Ausschusses	
Artikel 23	Änderung des Sechsten Buches Sozialgesetzbuch	Artikel 23	Änderung des Sechsten Buches Sozialgesetzbuch
Artikel 24	Änderung der Verordnung zum Barrierefreiheitsstärkungsgesetz	Artikel 24	Änderung der Verordnung zum Barrierefreiheitsstärkungsgesetz
Artikel 25	Änderung des Elften Buches Sozialgesetzbuch	Artikel 25	Änderung des Elften Buches Sozialgesetzbuch
Artikel 26	Änderung des Telekommunikationsgesetzes	Artikel 26	Änderung des Telekommunikationsgesetzes
Artikel 27	Änderung der Krankenhausstrukturfonds-Verordnung	Artikel 27	Änderung der Krankenhausstrukturfonds-Verordnung
Artikel 28	Änderung der Außenwirtschaftsverordnung	Artikel 28	Änderung der Außenwirtschaftsverordnung
Artikel 29	Änderung des Vertrauensdienstegesetzes	Artikel 29	Änderung des Vertrauensdienstegesetzes
Artikel 30	Weitere Änderung des BSI-Gesetzes		
Artikel 31	Weitere Änderung des Telekommunikationsgesetzes		
Artikel 32	Weitere Änderung der Außenwirtschaftsverordnung		
Artikel 33	Inkrafttreten, Außerkrafttreten	Artikel 30	Inkrafttreten, Außerkrafttreten
Artikel 1		**Artikel 1**	
Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen		**Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen**	
(BSI-Gesetz – BSIG)		**(BSI-Gesetz – BSIG)**	
Inhaltsübersicht		Inhaltsübersicht	
Teil 1 **Allgemeine Vorschriften**		**Teil 1** **Allgemeine Vorschriften**	
§ 1	Bundesamt für Sicherheit in der Informationstechnik	§ 1	Bundesamt für Sicherheit in der Informationstechnik

Entwurf		Beschlüsse des 4. Ausschusses	
§ 2	Begriffsbestimmungen	§ 2	Begriffsbestimmungen
Teil 2 **Das Bundesamt**		**Teil 2** **Das Bundesamt**	
Kapitel 1 **Aufgaben und Befugnisse**		**Kapitel 1** **Aufgaben und Befugnisse**	
§ 3	Aufgaben des Bundesamtes	§ 3	Aufgaben des Bundesamtes
§ 4	Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes	§ 4	Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes
§ 5	Allgemeine Meldestelle für die Sicherheit in der Informationstechnik	§ 5	Allgemeine Meldestelle für die Sicherheit in der Informationstechnik
§ 6	Informationsaustausch	§ 6	Informationsaustausch
§ 7	Kontrolle der Kommunikationstechnik des Bundes, Betretensrechte	§ 7	Kontrolle der Kommunikationstechnik des Bundes, Betretensrechte
§ 8	Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes	§ 8	Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes
§ 9	Verarbeitung von Protokollierungsdaten der Kommunikationstechnik des Bundes	§ 9	Verarbeitung von Protokollierungsdaten der Kommunikationstechnik des Bundes
§ 10	Anordnungen von Maßnahmen zur Abwendung oder Behebung von Sicherheitsvorfällen	§ 10	Anordnungen von Maßnahmen zur Abwendung oder Behebung von Sicherheitsvorfällen
§ 11	Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen	§ 11	Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen
§ 12	Bestandsdatenauskunft	§ 12	Bestandsdatenauskunft
§ 13	Warnungen	§ 13	Warnungen
§ 14	Untersuchung der Sicherheit in der Informationstechnik, Auskunftsverlangen	§ 14	Untersuchung der Sicherheit in der Informationstechnik, Auskunftsverlangen
§ 15	Detektion von Angriffsmethoden und von Sicherheitsrisiken für die Netz- und IT-Sicherheit	§ 15	Detektion von Angriffsmethoden und von Sicherheitsrisiken für die Netz- und IT-Sicherheit
§ 16	Anordnungen von Maßnahmen des Bundesamtes gegenüber Anbietern von Telekommunikationsdiensten	§ 16	Anordnungen von Maßnahmen des Bundesamtes gegenüber Anbietern von Telekommunikationsdiensten
§ 17	Anordnungen von Maßnahmen des Bundesamtes gegenüber Anbietern von digitalen Diensten	§ 17	Anordnungen von Maßnahmen des Bundesamtes gegenüber Anbietern von digitalen Diensten
§ 18	Anordnungen von Maßnahmen des Bundesamtes gegenüber Herstellern von IKT-Produkten	§ 18	Anordnungen von Maßnahmen des Bundesamtes gegenüber Herstellern von IKT-Produkten
§ 19	Bereitstellung von IT-Sicherheitsprodukten	§ 19	Bereitstellung von IT-Sicherheitsprodukten
Kapitel 2 **Datenverarbeitung**		**Kapitel 2** **Datenverarbeitung**	
§ 20	Verarbeitung personenbezogener Daten	§ 20	Verarbeitung personenbezogener Daten

Entwurf		Beschlüsse des 4. Ausschusses	
§ 21	Beschränkungen der Rechte der betroffenen Person	§ 21	Beschränkungen der Rechte der betroffenen Person
§ 22	Informationspflicht bei Erhebung von personenbezogenen Daten	§ 22	Informationspflicht bei Erhebung von personenbezogenen Daten
§ 23	Auskunftsrecht der betroffenen Person	§ 23	Auskunftsrecht der betroffenen Person
§ 24	Recht auf Berichtigung	§ 24	Recht auf Berichtigung
§ 25	Recht auf Löschung	§ 25	Recht auf Löschung
§ 26	Recht auf Einschränkung der Verarbeitung	§ 26	Recht auf Einschränkung der Verarbeitung
§ 27	Widerspruchsrecht	§ 27	Widerspruchsrecht
Teil 3 Sicherheit in der Informationstechnik von Einrichtungen		**Teil 3 Sicherheit in der Informationstechnik von Einrichtungen**	
Kapitel 1 Anwendungsbereich		**Kapitel 1 Anwendungsbereich**	
§ 28	Besonders wichtige Einrichtungen und wichtige Einrichtungen	§ 28	Besonders wichtige Einrichtungen und wichtige Einrichtungen
§ 29	Einrichtungen der Bundesverwaltung	§ 29	Einrichtungen der Bundesverwaltung
Kapitel 2 Risikomanagement, Melde-, Registrierungs-, Nachweis- und Unterrichtungspflichten		**Kapitel 2 Risikomanagement, Melde-, Registrierungs-, Nachweis- und Unterrichtungspflichten**	
§ 30	Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	§ 30	Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen
§ 31	Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen	§ 31	Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen
§ 32	Meldepflichten	§ 32	Meldepflichten
§ 33	Registrierungspflicht	§ 33	Registrierungspflicht
§ 34	Besondere Registrierungspflicht für bestimmte Einrichtungsarten	§ 34	Besondere Registrierungspflicht für bestimmte Einrichtungsarten
§ 35	Unterrichtungspflichten	§ 35	Unterrichtungspflichten
§ 36	Rückmeldungen des Bundesamtes gegenüber meldenden Einrichtungen	§ 36	Rückmeldungen des Bundesamtes gegenüber meldenden Einrichtungen
§ 37	Ausnahmebescheid	§ 37	Ausnahmebescheid
§ 38	Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	§ 38	Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen
§ 39	Nachweispflichten für Betreiber kritischer Anlagen	§ 39	Nachweispflichten für Betreiber kritischer Anlagen

Entwurf		Beschlüsse des 4. Ausschusses	
§ 40	Nationale Verbindungsstelle sowie zentrale Melde- und Anlaufstelle für besonders wichtige und wichtige Einrichtungen	§ 40	Nationale Verbindungsstelle sowie zentrale Melde- und Anlaufstelle für besonders wichtige und wichtige Einrichtungen
§ 41	Untersagung des Einsatzes kritischer Komponenten	§ 41	Untersagung des Einsatzes kritischer Komponenten
§ 42	Auskunftsverlangen	§ 42	Auskunftsverlangen
Kapitel 3 Informationssicherheit der Einrichtungen der Bundesverwaltung		**Kapitel 3 Informationssicherheit der Einrichtungen der Bundesverwaltung**	
§ 43	Informationssicherheitsmanagement	§ 43	Informationssicherheitsmanagement
§ 44	Vorgaben des Bundesamtes	§ 44	Vorgaben des Bundesamtes
§ 45	Informationssicherheitsbeauftragte der Einrichtungen der Bundesverwaltung	§ 45	Informationssicherheitsbeauftragte der Einrichtungen der Bundesverwaltung
§ 46	Informationssicherheitsbeauftragte der Ressorts	§ 46	Informationssicherheitsbeauftragte der Ressorts
§ 47	Wesentliche Digitalisierungsvorhaben und Kommunikationsinfrastrukturen des Bundes	§ 47	Wesentliche Digitalisierungsvorhaben und Kommunikationsinfrastrukturen des Bundes
§ 48	Amt des Koordinators für Informationssicherheit	§ 48	Amt des Koordinators für Informationssicherheit
Teil 4 Datenbanken der Domain-Name-Registrierungsdaten		**Teil 4 Datenbanken der Domain-Name-Registrierungsdaten**	
§ 49	Pflicht zum Führen einer Datenbank	§ 49	Pflicht zum Führen einer Datenbank
§ 50	Verpflichtung zur Zugangsgewährung	§ 50	Verpflichtung zur Zugangsgewährung
§ 51	Kooperationspflicht	§ 51	Kooperationspflicht
Teil 5 Zertifizierung, Konformitätserklärung und Kennzeichen		**Teil 5 Zertifizierung, Konformitätserklärung und Kennzeichen**	
§ 52	Zertifizierung	§ 52	Zertifizierung
§ 53	Konformitätsbewertung und Konformitätserklärung	§ 53	Konformitätsbewertung und Konformitätserklärung
§ 54	Nationale Behörde für die Cybersicherheitszertifizierung	§ 54	Nationale Behörde für die Cybersicherheitszertifizierung
§ 55	Freiwilliges IT-Sicherheitskennzeichen	§ 55	Freiwilliges IT-Sicherheitskennzeichen

Entwurf		Beschlüsse des 4. Ausschusses	
Teil 6 **Verordnungsermächtigungen, Grundrechtseinschränkungen und Berichtspflichten**		**Teil 6** **Verordnungsermächtigungen, Grundrechtseinschränkungen und Berichtspflichten**	
§ 56	Ermächtigung zum Erlass von Rechtsverordnungen	§ 56	Ermächtigung zum Erlass von Rechtsverordnungen
§ 57	Einschränkung von Grundrechten	§ 57	Einschränkung von Grundrechten
§ 58	Berichtspflichten des Bundesamtes	§ 58	Berichtspflichten des Bundesamtes
Teil 7 **Aufsicht**		**Teil 7** **Aufsicht**	
§ 59	Zuständigkeit des Bundesamtes	§ 59	Zuständigkeit des Bundesamtes
§ 60	Zentrale Zuständigkeit in der Europäischen Union für bestimmte Einrichtungsarten	§ 60	Zentrale Zuständigkeit in der Europäischen Union für bestimmte Einrichtungsarten
§ 61	Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtige Einrichtungen	§ 61	Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtige Einrichtungen
§ 62	Aufsichts- und Durchsetzungsmaßnahmen für wichtige Einrichtungen	§ 62	Aufsichts- und Durchsetzungsmaßnahmen für wichtige Einrichtungen
§ 63	Verwaltungszwang	§ 63	Verwaltungszwang
§ 64	Zuwiderhandlungen durch Institutionen der sozialen Sicherung	§ 64	Zuwiderhandlungen durch Institutionen der sozialen Sicherung
Teil 8 **Bußgeldvorschriften**		**Teil 8** **Bußgeldvorschriften**	
§ 65	Bußgeldvorschriften	§ 65	Bußgeldvorschriften
Anlage 1	Sektoren besonders wichtiger und wichtiger Einrichtungen	Anlage 1	Sektoren besonders wichtiger und wichtiger Einrichtungen
Anlage 2	Sektoren wichtiger Einrichtungen	Anlage 2	Sektoren wichtiger Einrichtungen

Entwurf	Beschlüsse des 4. Ausschusses
Teil 1	Teil 1
Allgemeine Vorschriften	Allgemeine Vorschriften
§ 1	§ 1
Bundesamt für Sicherheit in der Informationstechnik	**Bundesamt für Sicherheit in der Informationstechnik**
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.	Das Bundesamt für Sicherheit in der Informationstechnik (Bundesamt) ist eine selbständige Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern und für Heimat. Es ist die zentrale Stelle für Informationssicherheit auf nationaler Ebene. Das Bundesamt führt seine Aufgaben fachlich unabhängig auf Grundlage wissenschaftlich-technischer Er-kenntnisse durch. Das Bundesamt und das Bundesministerium des Innern und für Heimat erstellen in regelmäßigen Abständen gemeinsam eine Zielvereinbarung.
§ 2	§ 2
Begriffsbestimmungen	**Begriffsbestimmungen**
Im Sinne dieses Gesetzes ist oder sind	Im Sinne dieses Gesetzes ist oder sind
1. „Beinahevorfall“ ein Ereignis, das die Verfügbarkeit, 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 worden ist oder aus anderen Gründen nicht erfolgt ist;	1. „Beinahevorfall“ ein Ereignis, das die Verfügbarkeit, 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 worden ist oder aus anderen Gründen nicht erfolgt ist;
2. „berechtigte Zugangsnachfrager“	2. „berechtigte Zugangsnachfrager“
a) das Bundesamt,	a) das Bundesamt,

Entwurf	Beschlüsse des 4. Ausschusses
b) die Landesbehörden, die die Länder als zuständige Behörden für die Aufsicht von Einrichtungen der öffentlichen Verwaltung auf regionaler Ebene nach Artikel 2 Absatz 2 Buchstabe f Nummer ii der NIS-2-Richtlinie bestimmt haben,	b) die Landesbehörden, die die Länder als zuständige Behörden für die Aufsicht von Einrichtungen der öffentlichen Verwaltung auf regionaler Ebene nach Artikel 2 Absatz 2 Buchstabe f Nummer ii der NIS-2-Richtlinie bestimmt haben,
c) Strafverfolgungsbehörden,	c) Strafverfolgungsbehörden,
d) die Polizeien des Bundes und der Länder und	d) die Polizeien des Bundes und der Länder und
e) die Verfassungsschutzbehörden des Bundes und der Länder;	e) die Verfassungsschutzbehörden des Bundes und der Länder;
3. „Bodeninfrastruktur“ den Sektor Weltraum betreffende Einrichtungen, die der Kontrolle des Startes, Fluges oder der eventuellen Landung von Weltraumgegenständen dienen;	3. „Bodeninfrastruktur“ den Sektor Weltraum betreffende Einrichtungen, die der Kontrolle des Startes, Fluges oder der eventuellen Landung von Weltraumgegenständen dienen;
4. „Cloud-Computing-Dienst“ ein digitaler Dienst, der auf Abruf die Verwaltung eines skalierbaren und elastischen Pools gemeinsam nutzbarer Rechenressourcen sowie den umfassenden Fernzugang zu diesem Pool ermöglicht, auch wenn die Rechenressourcen auf mehrere Standorte verteilt sind;	4. „Cloud-Computing-Dienst“ ein digitaler Dienst, der auf Abruf die Verwaltung eines skalierbaren und elastischen Pools gemeinsam nutzbarer Rechenressourcen sowie den umfassenden Fernzugang zu diesem Pool ermöglicht, auch wenn die Rechenressourcen auf mehrere Standorte verteilt sind;
5. „Content Delivery Network“ oder „CDN“ eine Gruppe geographisch verteilter, zusammengeschalteter Server, mitsamt der hierfür erforderlichen Infrastruktur, die mit dem Internet verbunden sind, und der Bereitstellung digitaler Inhalte und Dienste für Internetnutzer im Auftrag von Inhalte- und Diensteanbietern dienen, mit dem Ziel der Gewährleistung einer hohen Verfügbarkeit, Zugänglichkeit oder Zustellung mit möglichst niedriger Latenz;	5. „Content Delivery Network“ oder „CDN“ eine Gruppe geographisch verteilter, zusammengeschalteter Server, mitsamt der hierfür erforderlichen Infrastruktur, die mit dem Internet verbunden sind, und der Bereitstellung digitaler Inhalte und Dienste für Internetnutzer im Auftrag von Inhalte- und Diensteanbietern dienen, mit dem Ziel der Gewährleistung einer hohen Verfügbarkeit, Zugänglichkeit oder Zustellung mit möglichst niedriger Latenz;

Entwurf	Beschlüsse des 4. Ausschusses
6. „Cyberbedrohung“ eine Cyberbedrohung nach Artikel 2 Nummer 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);	6. „Cyberbedrohung“ eine Cyberbedrohung nach Artikel 2 Nummer 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);
7. „Datenverkehr“ die mittels technischer Protokolle übertragenen Daten; es können Telekommunikationsinhalte nach § 3 Absatz 1 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes und Nutzungsdaten nach § 2 Absatz 2 Nummer 3 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes enthalten sein;	7. „Datenverkehr“ die mittels technischer Protokolle übertragenen Daten; es können Telekommunikationsinhalte nach § 3 Absatz 1 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes und Nutzungsdaten nach § 2 Absatz 2 Nummer 3 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes enthalten sein;
8. „DNS-Diensteanbieter“ eine natürliche oder juristische Person, die	8. „DNS-Diensteanbieter“ eine natürliche oder juristische Person, die
a) für Internet-Endnutzer öffentlich verfügbare rekursive Dienste zur Auflösung von Domain-Namen anbietet oder	a) für Internet-Endnutzer öffentlich verfügbare rekursive Dienste zur Auflösung von Domain-Namen anbietet oder
b) autoritative Dienste zur Auflösung von Domain-Namen zur Nutzung durch Dritte, mit Ausnahme von Root-Namenservern, anbietet;	b) autoritative Dienste zur Auflösung von Domain-Namen zur Nutzung durch Dritte, mit Ausnahme von Root-Namenservern, anbietet;
9. „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;	9. „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;
10. „erhebliche Cyberbedrohung“ eine Cyberbedrohung, die das Potenzial besitzt, die informationstechnischen Systeme, Komponenten und Prozesse auf Grund der besonderen technischen Merkmale der Cyberbedrohung erheblich zu beeinträchtigen; eine Beeinträchtigung ist erheblich, wenn sie erheblichen materiellen oder immateriellen Schaden verursachen kann;	10. „erhebliche Cyberbedrohung“ eine Cyberbedrohung, die das Potenzial besitzt, die informationstechnischen Systeme, Komponenten und Prozesse auf Grund der besonderen technischen Merkmale der Cyberbedrohung erheblich zu beeinträchtigen; eine Beeinträchtigung ist erheblich, wenn sie erheblichen materiellen oder immateriellen Schaden verursachen kann;

Entwurf	Beschlüsse des 4. Ausschusses
11. „erheblicher Sicherheitsvorfall“ ein Sicherheitsvorfall, der	11. „erheblicher Sicherheitsvorfall“ ein Sicherheitsvorfall, der
a) schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann oder	a) schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann oder
b) andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann,	b) andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann,
sofern durch die Rechtsverordnung nach § 56 Absatz 5 keine konkretisierende Begriffsbestimmung erfolgt;	sofern durch die Rechtsverordnung nach § 56 Absatz 5 keine konkretisierende Begriffsbestimmung erfolgt;
12. „Forschungseinrichtung“ eine Einrichtung, deren primäres Ziel es ist, angewandte Forschung oder experimentelle Entwicklung im Hinblick auf die Nutzung der Ergebnisse dieser Forschung für kommerzielle Zwecke durchzuführen; Bildungseinrichtungen gelten nicht als Forschungseinrichtungen;	12. „Forschungseinrichtung“ eine Einrichtung, deren primäres Ziel es ist, angewandte Forschung oder experimentelle Entwicklung im Hinblick auf die Nutzung der Ergebnisse dieser Forschung für kommerzielle Zwecke durchzuführen; Bildungseinrichtungen gelten nicht als Forschungseinrichtungen;
13. „Geschäftsleitung“ eine natürliche Person, die nach Gesetz, Satzung oder Gesellschaftsvertrag zur Führung der Geschäfte und zur Vertretung einer besonders wichtigen Einrichtung oder wichtigen Einrichtung berufen ist; Leiterinnen und Leiter von Einrichtungen der Bundesverwaltung nach § 29 gelten nicht als Geschäftsleitung;	13. „Geschäftsleitung“ eine natürliche Person, die nach Gesetz, Satzung oder Gesellschaftsvertrag zur Führung der Geschäfte und zur Vertretung einer besonders wichtigen Einrichtung oder wichtigen Einrichtung berufen ist; Leiterinnen und Leiter von Einrichtungen der Bundesverwaltung nach § 29 gelten nicht als Geschäftsleitung;
14. „IKT-Dienst“ ein IKT-Dienst nach Artikel 2 Nummer 13 der Verordnung (EU) 2019/881;	14. „IKT-Dienst“ ein IKT-Dienst nach Artikel 2 Nummer 13 der Verordnung (EU) 2019/881;
15. „IKT-Produkt“ ein IKT-Produkt nach Artikel 2 Nummer 12 der Verordnung (EU) 2019/881;	15. „IKT-Produkt“ ein IKT-Produkt nach Artikel 2 Nummer 12 der Verordnung (EU) 2019/881;
16. „IKT-Prozess“ ein IKT-Prozess nach Artikel 2 Nummer 14 der Verordnung (EU) 2019/881;	16. „IKT-Prozess“ ein IKT-Prozess nach Artikel 2 Nummer 14 der Verordnung (EU) 2019/881;
17. „Informationssicherheit“ der angemessene Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen;	17. „Informationssicherheit“ der angemessene Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen;

Entwurf	Beschlüsse des 4. Ausschusses
18. „Informationstechnik“ ein technisches Mittel zur Verarbeitung von Informationen;	18. „Informationstechnik“ ein technisches Mittel zur Verarbeitung von Informationen;
19. „Institutionen der Sozialen Sicherung“ Körperschaften gemäß § 29 des Vierten Buches Sozialgesetzbuch, Arbeitsgemeinschaften gemäß § 94 des Zehnten Buches Sozialgesetzbuch, die Deutsche Gesetzliche Unfallversicherung e. V. sowie die Deutsche Post AG, soweit sie mit der Berechnung oder Auszahlung von Sozialleistungen betraut ist;	19. „Institutionen der Sozialen Sicherung“ Körperschaften gemäß § 29 des Vierten Buches Sozialgesetzbuch, Arbeitsgemeinschaften gemäß § 94 des Zehnten Buches Sozialgesetzbuch, die Deutsche Gesetzliche Unfallversicherung e. V. sowie die Deutsche Post AG, soweit sie mit der Berechnung oder Auszahlung von Sozialleistungen betraut ist;
20. „Internet Exchange Point“ oder „IXP“ eine Infrastruktur, die	20. „Internet Exchange Point“ oder „IXP“ eine Infrastruktur, die
a) die Zusammenschaltung von mehr als zwei unabhängigen autonomen Systemen ermöglicht, die in erster Linie zum Austausch von Internet-Datenverkehr genutzt wird,	a) die Zusammenschaltung von mehr als zwei unabhängigen autonomen Systemen ermöglicht, die in erster Linie zum Austausch von Internet-Datenverkehr genutzt wird,
b) nur der Zusammenschaltung autonomer Systeme dient und	b) nur der Zusammenschaltung autonomer Systeme dient und
c) nicht voraussetzt, dass	c) nicht voraussetzt, dass
aa) der Internet-Datenverkehr zwischen zwei beliebigen teilnehmenden autonomen Systemen über ein drittes autonomes System läuft oder	aa) der Internet-Datenverkehr zwischen zwei beliebigen teilnehmenden autonomen Systemen über ein drittes autonomes System läuft oder
bb) den betreffenden Datenverkehr verändert oder diesen anderweitig beeinträchtigt;	bb) den betreffenden Datenverkehr verändert oder diesen anderweitig beeinträchtigt;

Entwurf	Beschlüsse des 4. Ausschusses
21. „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; nicht als „Kommunikationstechnik des Bundes“ gelten die Kommunikationstechnik des Bundesverfassungsgerichts, der Bundesgerichte, soweit sie nicht öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen, des Bundestages, des Bundesrates, des Bundespräsidenten und des Bundesrechnungshofes, soweit sie ausschließlich in deren eigener Zuständigkeit betrieben wird;	21. „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; nicht als „Kommunikationstechnik des Bundes“ gelten die Kommunikationstechnik des Bundesverfassungsgerichts, der Bundesgerichte, soweit sie nicht öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen, des Bundestages, des Bundesrates, des Bundespräsidenten und des Bundesrechnungshofes, soweit sie ausschließlich in deren eigener Zuständigkeit betrieben wird;
22. „kritische Anlage“ eine Anlage, die für die Erbringung einer kritischen Dienstleistung erheblich ist; die kritischen Anlagen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 56 Absatz 4 näher bestimmt;	22. „kritische Anlage“ eine Anlage, die für die Erbringung einer kritischen Dienstleistung erheblich ist; die kritischen Anlagen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 56 Absatz 4 näher bestimmt;
23. „kritische Komponenten“ IKT-Produkte,	23. „kritische Komponenten“ IKT-Produkte, die in einer Rechtsverordnung aufgrund von § 56 Absatz 7 als kritische Komponenten bestimmt werden;
a) die in kritischen Anlagen eingesetzt werden,	
b) bei denen Störungen der Verfügbarkeit, Integrität und Vertraulichkeit zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit kritischer Anlagen oder zu Gefährdungen für die öffentliche Sicherheit führen können und	
c) die auf Grund eines Gesetzes unter Verweis auf diese Vorschrift	
aa) als kritische Komponenten bestimmt werden oder	

Entwurf	Beschlüsse des 4. Ausschusses
bb) eine auf Grund eines Gesetzes als kritisch bestimmte Funktion realisieren;	
werden für einen der in Nummer 24 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, so gibt es in diesem Sektor keine kritischen Komponenten im Sinne dieser Nummer;	
24. „kritische Dienstleistung“ eine Dienstleistung zur Versorgung der Allgemeinheit in den Sektoren Energie, Transport und Verkehr, Finanzwesen, Sozialversicherungsträger sowie Grundsicherung für Arbeitssuchende, Gesundheitswesen, Wasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum oder Siedlungsabfallentsorgung, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde;	24. „kritische Dienstleistung“ eine Dienstleistung zur Versorgung der Allgemeinheit in den Sektoren Energie, Transport und Verkehr, Finanzwesen, Sozialversicherungsträger sowie Grundsicherung für Arbeitssuchende, Gesundheitswesen, Wasser, Ernährung, Informationstechnik und Telekommunikation, Weltraum oder Siedlungsabfallentsorgung, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde;
25. „Managed Security Service Provider“ oder „MSSP“ ein MSP, der Unterstützung für Tätigkeiten im Zusammenhang mit dem Risikomanagement im Bereich der Cybersicherheit durchführt oder erbringt;	25. „Managed Security Service Provider“ oder „MSSP“ ein MSP, der Unterstützung für Tätigkeiten im Zusammenhang mit dem Risikomanagement im Bereich der Cybersicherheit durchführt oder erbringt;
26. „Managed Service Provider“ oder „MSP“ ein Anbieter von Diensten 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;	26. „Managed Service Provider“ oder „MSP“ ein Anbieter von Diensten 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;

Entwurf	Beschlüsse des 4. Ausschusses
27. „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;	27. „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;
28. „Online-Marktplatz“ ein Dienst nach § 312l Absatz 3 des Bürgerlichen Gesetzbuchs;	28. „Online-Marktplatz“ ein Dienst nach § 312l Absatz 3 des Bürgerlichen Gesetzbuchs;
29. „Online-Suchmaschine“ ein digitaler Dienst nach Artikel 2 Nummer 5 der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten (ABl. L 186 vom 11.7.2019, S. 57);	29. „Online-Suchmaschine“ ein digitaler Dienst nach Artikel 2 Nummer 5 der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates vom 20. Juni 2019 zur Förderung von Fairness und Transparenz für gewerbliche Nutzer von Online-Vermittlungsdiensten (ABl. L 186 vom 11.7.2019, S. 57);
30. „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;	30. „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;
31. „Protokolldaten“ Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die	31. „Protokolldaten“ Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die
a) zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind und	a) zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind und
b) unabhängig vom Inhalt des Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden;	b) unabhängig vom Inhalt des Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden;

Entwurf	Beschlüsse des 4. Ausschusses
Protokolldaten können Verkehrsdaten nach § 3 Nummer 70 des Telekommunikationsgesetzes und Nutzungsdaten nach § 2 Absatz 2 Nummer 3 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes enthalten;	Protokolldaten können Verkehrsdaten nach § 3 Nummer 70 des Telekommunikationsgesetzes und Nutzungsdaten nach § 2 Absatz 2 Nummer 3 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes enthalten;
32. „Protokollierungsdaten“ Aufzeichnungen über technische Ereignisse oder Zustände innerhalb informationstechnischer Systeme;	32. „Protokollierungsdaten“ Aufzeichnungen über technische Ereignisse oder Zustände innerhalb informationstechnischer Systeme;
33. „qualifizierter Vertrauensdienst“ ein qualifizierter Vertrauensdienst nach Artikel 3 Nummer 17 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73);	33. „qualifizierter Vertrauensdienst“ ein qualifizierter Vertrauensdienst nach Artikel 3 Nummer 17 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73);
34. „qualifizierter Vertrauensdiensteanbieter“ ein qualifizierter Vertrauensdiensteanbieter nach Artikel 3 Nummer 20 der Verordnung (EU) Nr. 910/2014;	34. „qualifizierter Vertrauensdiensteanbieter“ ein qualifizierter Vertrauensdiensteanbieter nach Artikel 3 Nummer 20 der Verordnung (EU) Nr. 910/2014;
35. „Rechenzentrumsdienst“ ein Dienst, der Strukturen umfasst, die dem vorrangigen Zweck der zentralen Unterbringung, der Zusammenschaltung und dem Betrieb von IT- oder Netzwerkausrüstungen dienen, und die Datenverarbeitungsdienste erbringen, mitsamt allen benötigten Anlagen und Infrastrukturen, insbesondere für die Stromverteilung und die Umgebungskontrolle;	35. „Rechenzentrumsdienst“ ein Dienst, der Strukturen umfasst, die dem vorrangigen Zweck der zentralen Unterbringung, der Zusammenschaltung und dem Betrieb von IT- oder Netzwerkausrüstungen dienen, und die Datenverarbeitungsdienste erbringen, mitsamt allen benötigten Anlagen und Infrastrukturen, insbesondere für die Stromverteilung und die Umgebungskontrolle;
36. „Schadprogramme“ Programme und sonstige informationstechnische Routinen und Verfahren, die dazu dienen, unbefugt Daten zu nutzen oder zu löschen oder unbefugt auf sonstige informationstechnische Abläufe einzuwirken;	36. „Schadprogramme“ Programme und sonstige informationstechnische Routinen und Verfahren, die dazu dienen, unbefugt Daten zu nutzen oder zu löschen oder unbefugt auf sonstige informationstechnische Abläufe einzuwirken;

Entwurf	Beschlüsse des 4. Ausschusses
37. „Schnittstellen der Kommunikationstechnik des Bundes“ sicherheitsrelevante Netzwerkübergänge innerhalb der Kommunikationstechnik des Bundes sowie zwischen dieser und der Informationstechnik der einzelnen Einrichtungen der Bundesverwaltung, der Informationstechnik von Gruppen von Einrichtungen der Bundesverwaltung oder der Informationstechnik Dritter; nicht als Schnittstellen der Kommunikationstechnik des Bundes gelten die Komponenten an den Netzwerkübergängen, die in eigener Zuständigkeit der in Nummer 21 genannten Gerichte und Verfassungsorgane betrieben werden;	37. „Schnittstellen der Kommunikationstechnik des Bundes“ sicherheitsrelevante Netzwerkübergänge innerhalb der Kommunikationstechnik des Bundes sowie zwischen dieser und der Informationstechnik der einzelnen Einrichtungen der Bundesverwaltung, der Informationstechnik von Gruppen von Einrichtungen der Bundesverwaltung oder der Informationstechnik Dritter; nicht als Schnittstellen der Kommunikationstechnik des Bundes gelten die Komponenten an den Netzwerkübergängen, die in eigener Zuständigkeit der in Nummer 21 genannten Gerichte und Verfassungsorgane betrieben werden;
38. „Schwachstelle“ eine Eigenschaft von IKT-Produkten oder IKT-Diensten, die von Dritten ausgenutzt werden kann, um sich gegen den Willen des Berechtigten Zugang zu den IKT-Produkten oder IKT-Diensten zu verschaffen oder die Funktion der IKT-Produkte oder IKT-Dienste zu beeinflussen;	38. „Schwachstelle“ eine Eigenschaft von IKT-Produkten oder IKT-Diensten, die von Dritten ausgenutzt werden kann, um sich gegen den Willen des Berechtigten Zugang zu den IKT-Produkten oder IKT-Diensten zu verschaffen oder die Funktion der IKT-Produkte oder IKT-Dienste zu beeinflussen;
39. „Sicherheit in der Informationstechnik“ die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen	39. „Sicherheit in der Informationstechnik“ die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen
a) in informationstechnischen Systemen, Komponenten oder Prozessen oder	a) in informationstechnischen Systemen, Komponenten oder Prozessen oder
b) bei der Anwendung informationstechnischer Systeme, Komponenten oder Prozesse;	b) bei der Anwendung informationstechnischer Systeme, Komponenten oder Prozesse;
40. „Sicherheitsvorfall“ ein Ereignis, das die Verfügbarkeit, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über informationstechnische Systeme, Komponenten und Prozesse angeboten werden oder zugänglich sind, beeinträchtigt;	40. „Sicherheitsvorfall“ ein Ereignis, das die Verfügbarkeit, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über informationstechnische Systeme, Komponenten und Prozesse angeboten werden oder zugänglich sind, beeinträchtigt;

Entwurf	Beschlüsse des 4. Ausschusses
41. „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;	41. „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;
42. „Top Level Domain Name Registry“ eine natürliche oder juristische Person, die 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, unabhängig davon, ob der Betrieb durch die natürliche oder juristische Person selbst erfolgt oder ausgelagert wird; keine Top Level Domain Name Registry sind Register, die TLD-Namen nur für eigene Zwecke verwenden;	42. „Top Level Domain Name Registry“ eine natürliche oder juristische Person, die 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, unabhängig davon, ob der Betrieb durch die natürliche oder juristische Person selbst erfolgt oder ausgelagert wird; keine Top Level Domain Name Registry sind Register, die TLD-Namen nur für eigene Zwecke verwenden;
43. „Vertrauensdienst“ ein Vertrauensdienst nach Artikel 3 Nummer 16 der Verordnung (EU) Nr. 910/2014;	43. „Vertrauensdienst“ ein Vertrauensdienst nach Artikel 3 Nummer 16 der Verordnung (EU) Nr. 910/2014;
44. „Vertrauensdiensteanbieter“ ein Vertrauensdiensteanbieter nach Artikel 3 Nummer 19 der Verordnung (EU) Nr. 910/2014;	44. „Vertrauensdiensteanbieter“ ein Vertrauensdiensteanbieter nach Artikel 3 Nummer 19 der Verordnung (EU) Nr. 910/2014;
45. „weltraumgestützte Dienste“ Dienste, die den Sektor Weltraum betreffen, die auf Daten und Informationen beruhen, die entweder von Weltraumgegenständen erzeugt oder über diese weitergegeben werden und deren Störung zu breiteren Kaskadeneffekten, die weitreichende und lang anhaltende negative Auswirkungen auf die Erbringung von Diensten im gesamten Binnenmarkt haben können, führen kann;	45. „weltraumgestützte Dienste“ Dienste, die den Sektor Weltraum betreffen, die auf Daten und Informationen beruhen, die entweder von Weltraumgegenständen erzeugt oder über diese weitergegeben werden und deren Störung zu breiteren Kaskadeneffekten, die weitreichende und lang anhaltende negative Auswirkungen auf die Erbringung von Diensten im gesamten Binnenmarkt haben können, führen kann;

Entwurf	Beschlüsse des 4. Ausschusses
46. „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.	46. „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.
Teil 2	Teil 2
Das Bundesamt	Das Bundesamt
Kapitel 1	Kapitel 1
Aufgaben und Befugnisse	Aufgaben und Befugnisse
§ 3	§ 3
Aufgaben des Bundesamtes	**Aufgaben des Bundesamtes**
(1) Das Bundesamt fördert die Sicherheit in der Informationstechnik. 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:
1. Gefahren für die Sicherheit in der Informationstechnik des Bundes abwehren;	1. Gefahren für die Sicherheit in der Informationstechnik des Bundes abwehren;
2. Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen sammeln und auswerten und die gewonnenen Erkenntnisse anderen Stellen zur Verfügung stellen, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist, und Dritten zur Verfügung stellen, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist;	2. Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen sammeln und auswerten und die gewonnenen Erkenntnisse anderen Stellen zur Verfügung stellen, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist, und Dritten zur Verfügung stellen, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist;
3. Aufgaben in der Kooperationsgruppe und im CSIRTs-Netzwerk nach Artikel 14 und 15 der NIS-2-Richtlinie wahrnehmen;	3. Aufgaben in der Kooperationsgruppe und im CSIRTs-Netzwerk nach Artikel 14 und 15 der NIS-2-Richtlinie wahrnehmen;

Entwurf	Beschlüsse des 4. Ausschusses
4. Sicherheitsrisiken bei der Anwendung der Informationstechnik sowie Entwicklung von Sicherheitsvorkehrungen untersuchen, insbesondere 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;	4. Sicherheitsrisiken bei der Anwendung der Informationstechnik sowie Entwicklung von Sicherheitsvorkehrungen untersuchen, insbesondere 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;
5. Kriterien, Verfahren und Werkzeuge 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 entwickeln;	5. Kriterien, Verfahren und Werkzeuge 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 entwickeln;
6. Peer Reviews nach Artikel 19 der NIS-2-Richtlinie durchführen;	6. Peer Reviews nach Artikel 19 der NIS-2-Richtlinie durchführen;
7. Sicherheitsanforderungen für die Kommunikationsinfrastruktur der ressortübergreifenden Kommunikationsnetze sowie weiterer staatlicher Kommunikationsinfrastrukturen des Bundes im Benehmen mit den jeweiligen Betreibern festlegen sowie Einhaltung dieser Sicherheitsanforderungen überprüfen;	7. Sicherheitsanforderungen für die Kommunikationsinfrastruktur der ressortübergreifenden Kommunikationsnetze sowie weiterer staatlicher Kommunikationsinfrastrukturen des Bundes im Benehmen mit den jeweiligen Betreibern festlegen sowie Einhaltung dieser Sicherheitsanforderungen überprüfen;
8. Sicherheit von informationstechnischen Systemen oder Komponenten prüfen und bewerten sowie Sicherheitszertifikate erteilen;	8. Sicherheit von informationstechnischen Systemen oder Komponenten prüfen und bewerten sowie Sicherheitszertifikate erteilen;
9. Aufgaben und Befugnisse nach Artikel 58 Absatz 7 und 8 der Verordnung (EU) 2019/881 als nationale Behörde für die Cybersicherheitszertifizierung wahrnehmen;	9. Aufgaben und Befugnisse nach Artikel 58 Absatz 7 und 8 der Verordnung (EU) 2019/881 als nationale Behörde für die Cybersicherheitszertifizierung wahrnehmen;
10. Konformität im Bereich der IT-Sicherheit von informationstechnischen Systemen und Komponenten mit technischen Richtlinien des Bundesamtes prüfen und bestätigen;	10. Konformität im Bereich der IT-Sicherheit von informationstechnischen Systemen und Komponenten mit technischen Richtlinien des Bundesamtes prüfen und bestätigen;

Entwurf	Beschlüsse des 4. Ausschusses
11. informationstechnische Systeme 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, prüfen, bewerten und zulassen;	11. informationstechnische Systeme 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, prüfen, bewerten und zulassen;
12. Schlüsseldaten und Betrieb von Krypto- und Sicherheitsmanagementsystemen für informationssichernde Systeme des Bundes herstellen, die im Bereich des staatlichen Geheimschutzes oder auf Anforderung der betroffenen Behörde auch in anderen Bereichen eingesetzt werden;	12. Schlüsseldaten und Betrieb von Krypto- und Sicherheitsmanagementsystemen für informationssichernde Systeme des Bundes herstellen, die im Bereich des staatlichen Geheimschutzes oder auf Anforderung der betroffenen Behörde auch in anderen Bereichen eingesetzt werden;
13. bei organisatorischen und technischen Sicherheitsmaßnahmen unterstützen und beraten sowie technische Prüfungen zum Schutz amtlich geheim gehaltener Informationen nach § 4 des Sicherheitsüberprüfungsgesetzes gegen die Kenntnisnahme durch Unbefugte durchführen;	13. bei organisatorischen und technischen Sicherheitsmaßnahmen unterstützen und beraten sowie technische Prüfungen zum Schutz amtlich geheim gehaltener Informationen nach § 4 des Sicherheitsüberprüfungsgesetzes gegen die Kenntnisnahme durch Unbefugte durchführen;
14. sicherheitstechnische Anforderungen an die einzusetzende Informationstechnik des Bundes und an die Eignung von Auftragnehmern im Bereich von Informationstechnik des Bundes mit besonderem Schutzbedarf entwickeln;	14. sicherheitstechnische Anforderungen an die einzusetzende Informationstechnik des Bundes und an die Eignung von Auftragnehmern im Bereich von Informationstechnik des Bundes mit besonderem Schutzbedarf entwickeln;
15. IT-Sicherheitsprodukte und IT-Sicherheitsdienstleistungen für Einrichtungen der Bundesverwaltung bereitstellen;	15. IT-Sicherheitsprodukte und IT-Sicherheitsdienstleistungen für Einrichtungen der Bundesverwaltung bereitstellen;

Entwurf	Beschlüsse des 4. Ausschusses
16. die für die Sicherheit in der Informationstechnik zuständigen Stellen des Bundes, insbesondere soweit sie Beratungs- oder Kontrollaufgaben wahrnehmen, unterstützen; dies gilt vorrangig für die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, deren oder dessen Unterstützung im Rahmen der Unabhängigkeit erfolgt, die ihr oder ihm bei der Erfüllung ihrer oder seiner Aufgaben nach 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) und dem Bundesdatenschutzgesetz zusteht;	16. die für die Sicherheit in der Informationstechnik zuständigen Stellen des Bundes, insbesondere soweit sie Beratungs- oder Kontrollaufgaben wahrnehmen, unterstützen; dies gilt vorrangig für die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, deren oder dessen Unterstützung im Rahmen der Unabhängigkeit erfolgt, die ihr oder ihm bei der Erfüllung ihrer oder seiner Aufgaben nach 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) und dem Bundesdatenschutzgesetz zusteht;
17. Einrichtungen der Bundesverwaltung in Fragen der Informationssicherheit, einschließlich der Behandlung von Sicherheitsvorfällen, beraten und unterstützen sowie konkrete, praxisnahe Hilfsmittel zur Umsetzung von Informationssicherheitsvorgaben, insbesondere zur Umsetzung der Vorgaben nach § 30 und § 44, bereitstellen;	17. Einrichtungen der Bundesverwaltung in Fragen der Informationssicherheit, einschließlich der Behandlung von Sicherheitsvorfällen, beraten und unterstützen sowie konkrete, praxisnahe Hilfsmittel zur Umsetzung von Informationssicherheitsvorgaben, insbesondere zur Umsetzung der Vorgaben nach § 30 und § 44, bereitstellen;
18. Unterstützung	18. Unterstützung
a) der Polizeien und Strafverfolgungsbehörden des Bundes bei der Wahrnehmung ihrer gesetzlichen Aufgaben,	a) der Polizeien und Strafverfolgungsbehörden des Bundes bei der Wahrnehmung ihrer gesetzlichen Aufgaben,

Entwurf	Beschlüsse des 4. Ausschusses
b) des Bundesamtes für Verfassungsschutz und des Militärischen Abschirmdienstes bei der Auswertung und Bewertung von Informationen, die bei der Beobachtung von Bestrebungen anfallen, die gegen die freiheitliche demokratische Grundordnung, den Bestand des Staates oder die Sicherheit des Bundes oder eines Landes gerichtet sind, oder die bei der Beobachtung sicherheitsgefährdender oder geheimdienstlicher Tätigkeiten im Rahmen der gesetzlichen Befugnisse nach dem Bundesverfassungsschutzgesetz beziehungsweise dem MAD-Gesetz anfallen,	b) des Bundesamtes für Verfassungsschutz und des Militärischen Abschirmdienstes bei der Auswertung und Bewertung von Informationen, die bei der Beobachtung von Bestrebungen anfallen, die gegen die freiheitliche demokratische Grundordnung, den Bestand des Staates oder die Sicherheit des Bundes oder eines Landes gerichtet sind, oder die bei der Beobachtung sicherheitsgefährdender oder geheimdienstlicher Tätigkeiten im Rahmen der gesetzlichen Befugnisse nach dem Bundesverfassungsschutzgesetz beziehungsweise dem MAD-Gesetz anfallen,
c) des Bundesnachrichtendienstes bei der Wahrnehmung seiner gesetzlichen Aufgaben;	c) des Bundesnachrichtendienstes bei der Wahrnehmung seiner gesetzlichen Aufgaben;
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;
19. die zuständigen Stellen der Länder in Fragen der Abwehr von Gefahren für die Sicherheit in der Informationstechnik auf deren Ersuchen unterstützen;	19. die zuständigen Stellen der Länder in Fragen der Abwehr von Gefahren für die Sicherheit in der Informationstechnik auf deren Ersuchen unterstützen;
20. Einrichtungen der Bundesverwaltung sowie Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik, insbesondere unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen, beraten, informieren und warnen;	20. Einrichtungen der Bundesverwaltung sowie Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik, insbesondere unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen, beraten, informieren und warnen;

Entwurf	Beschlüsse des 4. Ausschusses
21. Verbraucherschutz und Verbraucherinformation im Bereich der Sicherheit in der Informationstechnik, insbesondere Beratung und Warnung von Verbrauchern in Fragen der Sicherheit in der Informationstechnik unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen;	21. Verbraucherschutz und Verbraucherinformation im Bereich der Sicherheit in der Informationstechnik, insbesondere Beratung und Warnung von Verbrauchern in Fragen der Sicherheit in der Informationstechnik unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen;
22. geeignete Kommunikationsstrukturen zur Krisenfrüherkennung, Krisenreaktion und Krisenbewältigung aufbauen sowie Zusammenarbeit zum Schutz der Sicherheit in der Informationstechnik kritischer Anlagen im Verbund mit der Privatwirtschaft koordinieren;	22. geeignete Kommunikationsstrukturen zur Krisenfrüherkennung, Krisenreaktion und Krisenbewältigung aufbauen sowie Zusammenarbeit zum Schutz der Sicherheit in der Informationstechnik kritischer Anlagen im Verbund mit der Privatwirtschaft koordinieren;
23. 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;	23. 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;
24. Aufgaben nach § 40 als zentrale Stelle für die Sicherheit in der Informationstechnik besonders wichtiger Einrichtungen und wichtiger Einrichtungen einschließlich des Ersuchens und Erbringens von Amtshilfe nach Artikel 37 der NIS-2-Richtinie;	24. Aufgaben nach § 40 als zentrale Stelle für die Sicherheit in der Informationstechnik besonders wichtiger Einrichtungen und wichtiger Einrichtungen einschließlich des Ersuchens und Erbringens von Amtshilfe nach Artikel 37 der NIS-2-Richtinie;
25. bei der Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen nach § 11 unterstützen;	25. bei der Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen nach § 11 unterstützen;
26. Empfehlungen für Identifizierungs- und Authentisierungsverfahren und Bewertung dieser Verfahren im Hinblick auf die Informationssicherheit erarbeiten;	26. Empfehlungen für Identifizierungs- und Authentisierungsverfahren und Bewertung dieser Verfahren im Hinblick auf die Informationssicherheit erarbeiten;
27. einen Stand der Technik von sicherheitstechnischen Anforderungen an IT-Produkte, unter Berücksichtigung bestehender Normen und Standards sowie unter Einbeziehung der betroffenen Wirtschaftsverbände, beschreiben und veröffentlichen;	27. einen Stand der Technik von sicherheitstechnischen Anforderungen an IT-Produkte, unter Berücksichtigung bestehender Normen und Standards sowie unter Einbeziehung der betroffenen Wirtschaftsverbände, beschreiben und veröffentlichen;

Entwurf	Beschlüsse des 4. Ausschusses
28. mit nationalen Computer-Notfallteams von Drittländern oder gleichwertigen Stellen von Drittländern kooperieren sowie diese Teams oder Stellen unterstützen; Einsätze des Bundesamtes in Drittländern dürfen nicht gegen den Willen des Staates erfolgen, auf dessen Hoheitsgebiet die Maßnahme stattfinden soll; die Entscheidung über einen Einsatz des Bundesamtes in Drittländern trifft das Bundesministerium des Innern und für Heimat im Einvernehmen mit dem Auswärtigen Amt;	28. mit nationalen Computer-Notfallteams von Drittländern oder gleichwertigen Stellen von Drittländern kooperieren sowie diese Teams oder Stellen unterstützen; Einsätze des Bundesamtes in Drittländern dürfen nicht gegen den Willen des Staates erfolgen, auf dessen Hoheitsgebiet die Maßnahme stattfinden soll; die Entscheidung über einen Einsatz des Bundesamtes in Drittländern trifft das Bundesministerium des Innern und für Heimat im Einvernehmen mit dem Auswärtigen Amt;
29. mit der Bundesanstalt für Finanzdienstleistungsaufsicht kooperieren und Informationen austauschen, soweit dies für ihre Aufgabenerfüllung erforderlich ist, insbesondere in Bezug auf die ergriffenen Maßnahmen gemäß der Verordnung (EU) 2022/2554; die Bundesanstalt für Finanzdienstleistungsaufsicht übermittelt an das Bundesamt die für dessen Aufgabenerfüllung erforderlichen Informationen.	29. mit der Bundesanstalt für Finanzdienstleistungsaufsicht kooperieren und Informationen austauschen, soweit dies für ihre Aufgabenerfüllung erforderlich ist, insbesondere in Bezug auf die ergriffenen Maßnahmen gemäß der Verordnung (EU) 2022/2554; die Bundesanstalt für Finanzdienstleistungsaufsicht übermittelt an das Bundesamt die für dessen Aufgabenerfüllung erforderlichen Informationen.
(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.
(3) Das Bundesamt kann besonders wichtige Einrichtungen auf deren Ersuchen bei der Sicherung ihrer Informationstechnik beraten und unterstützen oder auf qualifizierte Sicherheitsdienstleister verweisen.	(3) Das Bundesamt kann besonders wichtige Einrichtungen auf deren Ersuchen bei der Sicherung ihrer Informationstechnik beraten und unterstützen oder auf qualifizierte Sicherheitsdienstleister verweisen.
§ 4	§ 4
Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes	**Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes**
(1) Das Bundesamt ist die zentrale Meldestelle für die Zusammenarbeit der Einrichtungen der Bundesverwaltung in Angelegenheiten der Sicherheit in der Informationstechnik.	(1) Das Bundesamt ist die zentrale Meldestelle für die Zusammenarbeit der Einrichtungen der Bundesverwaltung in Angelegenheiten der Sicherheit in der Informationstechnik.
(2) Das Bundesamt hat zur Wahrnehmung dieser Aufgabe	(2) Das Bundesamt hat zur Wahrnehmung dieser Aufgabe

Entwurf	Beschlüsse des 4. Ausschusses
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,	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,
2. die Einrichtungen der Bundesverwaltung 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,
3. den Einrichtungen der Bundesverwaltung Empfehlungen zum Umgang mit den Gefahren bereitzustellen.	3. den Einrichtungen der Bundesverwaltung Empfehlungen zum Umgang mit den Gefahren bereitzustellen.
(3) 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 Verfassungsorgans oder der gesetzlich geregelten Unabhängigkeit einzelner Stellen stünde.	(3) 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 Verfassungsorgans oder der gesetzlich geregelten Unabhängigkeit einzelner Stellen stünde.
§ 5	§ 5
Allgemeine Meldestelle für die Sicherheit in der Informationstechnik	**Allgemeine Meldestelle für die Sicherheit in der Informationstechnik**
(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 nach Artikel 12 Absatz 1 der NIS-2-Richtlinie.	(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 nach Artikel 12 Absatz 1 der NIS-2-Richtlinie.

Entwurf	Beschlüsse des 4. Ausschusses
(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. Erfolgt die Meldung nicht anonym, kann der Meldende zum Zeitpunkt der Meldung oder später verlangen, dass seine personenbezogenen Daten nur anonymisiert weitergegeben werden dürfen. Dies gilt nicht in den Fällen des § 8 Absatz 6 und 7 Satz 1. Eine Übermittlung der personenbezogenen Daten in den Fällen von § 8 Absatz 6 und 7 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, in der 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.	(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. Erfolgt die Meldung nicht anonym, kann der Meldende zum Zeitpunkt der Meldung oder später verlangen, dass seine personenbezogenen Daten nur anonymisiert weitergegeben werden dürfen. Dies gilt nicht in den Fällen des § 8 Absatz 6 und 7 Satz 1. Eine Übermittlung der personenbezogenen Daten in den Fällen von § 8 Absatz 6 und 7 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, in der 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.
(3) Das Bundesamt soll die gemäß Absatz 2 gemeldeten Informationen nutzen, um	(3) Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 1 gibt das Bundesamt die Informationen zu den nach Absatz 2 gemeldeten Schwachstellen unverzüglich an den verantwortlichen Hersteller oder Produktverantwortlichen zum Zwecke der Schließung der Schwachstelle weiter, sofern diese nicht bereits öffentlich bekannt sind. Das Bundesamt soll die gemäß Absatz 2 gemeldeten Informationen nutzen, um
1. Dritte über bekannt gewordene Schwachstellen, Schadprogramme oder erfolgte oder versuchte Angriffe auf die Sicherheit in der Informationstechnik zu informieren, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist,	1. Dritte, insbesondere Verbraucher, über bekannt gewordene Schwachstellen, Schadprogramme oder erfolgte oder versuchte Angriffe auf die Sicherheit in der Informationstechnik zu informieren, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist,

Entwurf	Beschlüsse des 4. Ausschusses
2. die Öffentlichkeit oder betroffene Kreise gemäß § 13 zu warnen und zu informieren,	2. die Öffentlichkeit oder betroffene Kreise gemäß § 13 zu warnen und zu informieren,
3. Einrichtungen der Bundesverwaltung 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,
4. besonders wichtige Einrichtungen und wichtige Einrichtungen gemäß § 40 Absatz 3 Nummer 4 Buchstabe a über die sie betreffenden Informationen zu unterrichten,	4. besonders wichtige Einrichtungen und wichtige Einrichtungen gemäß § 40 Absatz 3 Nummer 4 Buchstabe a über die sie betreffenden Informationen zu unterrichten,
5. seine Aufgaben als zuständige Behörde, CSIRT und zentrale Anlaufstelle im Sinne der NIS-2-Richtlinie wahrzunehmen.	5. seine Aufgaben als zuständige Behörde, CSIRT und zentrale Anlaufstelle im Sinne der NIS-2-Richtlinie wahrzunehmen,
	6. Informationen zu Schwachstellen an die Agentur der Europäischen Union für Cybersicherheit zur Veröffentlichung in der europäischen Schwachstellendatenbank nach Artikel 12 Absatz 2 der NIS-2-Richtlinie zu übermitteln,
	7. seine Aufgabe nach § 3 Absatz 1 Nr. 21 wahrzunehmen und die Verbraucher auf verständliche Weise über öffentlich bekannte Schwachstellen und Sicherheitsrisiken aufzuklären.
(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
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
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.
(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.

Entwurf	Beschlüsse des 4. Ausschusses
	(6) Das BSI veröffentlicht … [Einsetzen: spätestens ein Jahr nach Inkrafttreten des Gesetzes] eine Verfahrensbeschreibung zur Durchführung der Absätze 1 bis 3.
§ 6	§ 6
Informationsaustausch	**Informationsaustausch**
(1) Das Bundesamt betreibt eine Online-Plattform zum Informationsaustausch mit wichtigen Einrichtungen, besonders wichtigen Einrichtungen und Einrichtungen der Bundesverwaltung. Es kann die beteiligten Hersteller, Lieferanten oder Dienstleister zum Austausch über Cyberbedrohungen, Schwachstellen, Beinahevorfälle und IT-Sicherheitsmaßnahmen sowie zur Aufdeckung und Abwehr von Cyberangriffen hinzuziehen. Das Bundesamt kann weiteren Stellen die Teilnahme ermöglichen.	(1) Das Bundesamt betreibt eine Online-Plattform zum Informationsaustausch mit wichtigen Einrichtungen, besonders wichtigen Einrichtungen und Einrichtungen der Bundesverwaltung. Es kann die beteiligten Hersteller, Lieferanten oder Dienstleister zum Austausch über Cyberbedrohungen, Schwachstellen, Beinahevorfälle und IT-Sicherheitsmaßnahmen sowie zur Aufdeckung und Abwehr von Cyberangriffen hinzuziehen. Das Bundesamt kann weiteren Stellen sowie Verbrauchern die Teilnahme ermöglichen.
(2) Das Bundesamt gibt Teilnahmebedingungen für den Informationsaustausch und die Plattformnutzung zwischen den Teilnehmenden vor.	(2) Das Bundesamt gibt Teilnahmebedingungen für den Informationsaustausch und die Plattformnutzung zwischen den Teilnehmenden vor.
§ 7	§ 7
Kontrolle der Kommunikationstechnik des Bundes, Betretensrechte	**Kontrolle der Kommunikationstechnik des Bundes, Betretensrechte**
(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	(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
1. die Bereitstellung der zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1 und 20 erforderlichen Informationen, insbesondere zu technischen Details, zu Strategien, Planungen und Regelungen mit Bezug zur Kommunikationstechnik des Bundes einschließlich Aufbau- und Ablauforganisation verlangen sowie	1. die Bereitstellung der zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1 und 20 erforderlichen Informationen, insbesondere zu technischen Details, zu Strategien, Planungen und Regelungen mit Bezug zur Kommunikationstechnik des Bundes einschließlich Aufbau- und Ablauforganisation verlangen sowie

Entwurf	Beschlüsse des 4. Ausschusses
2. 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.	2. 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, sowie
	3. Penetrationstests durchführen.
(2) Dem Bundesamt ist in den Zeiten, zu denen die Räume normalerweise für die jeweilige geschäftliche oder betriebliche Nutzung zur Verfügung stehen, Zugang zu den Grundstücken und Betriebsräumen, einschließlich Datenverarbeitungsanlagen und -geräten, die für die Kommunikationstechnik des Bundes verwendet werden, 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, Zugang zu den Grundstücken und Betriebsräumen, einschließlich Datenverarbeitungsanlagen und -geräten, die für die Kommunikationstechnik des Bundes verwendet werden, zu gewähren, soweit dies zur Erfüllung der Zwecke nach Absatz 1 erforderlich ist.
(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 einsehen 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 einsehen sowie Unterlagen und Datenträger des Betreibers einsehen und unentgeltlich Kopien, auch in elektronischer Form, anfertigen.
(4) Das Bundesamt informiert über das Ergebnis seiner Kontrolle nach den Absätzen 1 bis 3	(4) Das Bundesamt informiert über das Ergebnis seiner Kontrolle nach den Absätzen 1 bis 3
1. den jeweiligen überprüften Betreiber,	1. den jeweiligen überprüften Betreiber,
2. die oder den Informationssicherheitsbeauftragten des Ressorts und	2. die oder den Informationssicherheitsbeauftragten des Ressorts und
3. die zuständige Rechts- und Fachaufsicht.	3. die zuständige Rechts- und Fachaufsicht.

Entwurf	Beschlüsse des 4. Ausschusses
(5) Das Bundesamt führt vor der Finalisierung des Prüfberichts eine Sachverhaltsklärung mit der geprüften Einrichtung durch. Mit der Mitteilung soll das Bundesamt Vorschläge zur Verbesserung der Informationssicherheit, insbesondere zur Beseitigung der festgestellten Mängel, verbinden. Für die Mitteilung an Stellen außerhalb des Betreibers gilt § 4 Absatz 3 entsprechend. Das Bundesamt kann im Benehmen mit dem oder der Informationssicherheitsbeauftragten des jeweils zuständigen Ressorts Einrichtungen der Bundesverwaltung anweisen, die Vorschläge zur Verbesserung innerhalb einer angemessenen Frist umzusetzen.	(5) Das Bundesamt führt vor der Finalisierung des Prüfberichts eine Sachverhaltsklärung mit der geprüften Einrichtung durch. Mit der Mitteilung soll das Bundesamt Vorschläge zur Verbesserung der Informationssicherheit, insbesondere zur Beseitigung der festgestellten Mängel, verbinden. Für die Mitteilung an Stellen außerhalb des Betreibers gilt § 4 Absatz 3 entsprechend. Das Bundesamt kann im Benehmen mit dem oder der Informationssicherheitsbeauftragten des jeweils zuständigen Ressorts die Umsetzung der Vorschläge zur Verbesserung innerhalb einer angemessenen Frist durch die Einrichtungen der Bundesverwaltung anordnen.
(6) Ausgenommen von den Befugnissen nach den Absätzen 1 bis 3 sind Kontrollen der Auslandsinformations- und -kommunikationstechnik nach § 9 Absatz 2 des Gesetzes über den Auswärtigen Dienst, soweit sie 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.	(6) Ausgenommen von den Befugnissen nach den Absätzen 1 bis 3 sind Kontrollen der Auslandsinformations- und -kommunikationstechnik nach § 9 Absatz 2 des Gesetzes über den Auswärtigen Dienst, soweit sie 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.
(7) 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.	(7) 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.

Entwurf	Beschlüsse des 4. Ausschusses
(8) Stellt das Bundesamt im Rahmen seiner Kontrollen fest, dass ein Verstoß gegen die Verpflichtungen dieses Gesetzes eine offensichtliche Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Nummer 12 der Verordnung (EU) 2016/679 zur Folge hat, die gemäß Artikel 33 dieser Verordnung zu melden ist, so unterrichtet es unverzüglich die zuständigen Aufsichtsbehörden.	(8) Stellt das Bundesamt im Rahmen seiner Kontrollen fest, dass ein Verstoß gegen die Verpflichtungen dieses Gesetzes eine Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Nummer 12 der Verordnung (EU) 2016/679 zur Folge haben kann, die gemäß Artikel 33 dieser Verordnung zu melden ist, so unterrichtet es unverzüglich die zuständigen Aufsichtsbehörden.
(9) Das Bundesamt unterrichtet den Haushaltsausschuss des Deutschen Bundestages kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres über die Anwendung dieser Vorschrift.	
§ 8	§ 8
Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes	**Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes**
(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
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,
2. die an den Schnittstellen der Kommunikationstechnik des Bundes anfallenden Daten automatisiert auswerten, soweit dies für die Erkennung und Abwehr von Schadprogrammen und sonstigen erheblichen Gefahren für die Kommunikationstechnik des Bundes erforderlich ist.	2. die an den Schnittstellen der Kommunikationstechnik des Bundes anfallenden Daten automatisiert auswerten, soweit dies für die Erkennung und Abwehr von Schadprogrammen und sonstigen erheblichen Gefahren für die Kommunikationstechnik des Bundes erforderlich ist.

Entwurf	Beschlüsse des 4. Ausschusses
Sofern nicht die nachfolgenden Absätze eine weitere Verwendung gestatten, müssen die automatisierte Auswertung dieser Daten und deren anschließende vollständige und nicht wiederherstellbare Löschung unverzüglich erfolgen. 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 zu 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, müssen die automatisierte Auswertung dieser Daten und deren anschließende vollständige und nicht wiederherstellbare Löschung unverzüglich erfolgen. 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 zu Schnittstellendaten nach Satz 1 Nummer 2 sicherzustellen. Protokolldaten der Bundesgerichte dürfen nur in deren Einvernehmen erhoben werden.

Entwurf	Beschlüsse des 4. Ausschusses
(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 4 Satz 2 zur Abwehr von Gefahren, die von dem gefundenen Schadprogramm ausgehen, oder zur Erkennung und Abwehr anderer Schadprogramme oder sonstiger erheblicher Gefahren für die Kommunikationstechnik des Bundes 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 oder einer sonstigen erheblichen Gefahr für die Kommunikationstechnik des Bundes erfolgt. Die Daten 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.	(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 4 Satz 2 zur Abwehr von Gefahren, die von dem gefundenen Schadprogramm ausgehen, oder zur Erkennung und Abwehr anderer Schadprogramme oder sonstiger erheblicher Gefahren für die Kommunikationstechnik des Bundes 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 oder einer sonstigen erheblichen Gefahr für die Kommunikationstechnik des Bundes erfolgt. Die Daten 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.
(3) 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.	(3) 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.

Entwurf	Beschlüsse des 4. Ausschusses
(4) Eine über die Absätze 1 und 2 hinausgehende Verwendung personenbezogener Daten ist nur zulässig, wenn bestimmte Tatsachen den Verdacht begründen, dass	(4) Eine über die Absätze 1 und 2 hinausgehende Verwendung personenbezogener Daten ist nur zulässig, wenn bestimmte Tatsachen den Verdacht begründen, dass
1. diese Daten ein Schadprogramm enthalten,	1. diese Daten ein Schadprogramm enthalten,
2. diese Daten durch ein Schadprogramm übermittelt wurden,	2. diese Daten durch ein Schadprogramm übermittelt wurden,
3. diese Daten im Zusammenhang mit einer sonstigen erheblichen Gefahr für die Kommunikationstechnik des Bundes stehen oder	3. diese Daten im Zusammenhang mit einer sonstigen erheblichen Gefahr für die Kommunikationstechnik des Bundes stehen oder
4. sich aus diesen Daten Hinweise auf ein Schadprogramm oder eine sonstige erhebliche Gefahr für die Kommunikationstechnik des Bundes ergeben können,	4. sich aus diesen Daten Hinweise auf ein Schadprogramm oder eine sonstige erhebliche Gefahr für die Kommunikationstechnik des Bundes ergeben können,
und soweit die Datenverarbeitung erforderlich ist, um den Verdacht zu bestätigen oder zu widerlegen. Im Falle der Bestätigung des Verdachts ist die weitere Verarbeitung personenbezogener Daten zulässig, soweit dies erforderlich ist	und soweit die Datenverarbeitung erforderlich ist, um den Verdacht zu bestätigen oder zu widerlegen. Im Falle der Bestätigung des Verdachts ist die weitere Verarbeitung personenbezogener Daten zulässig, soweit dies erforderlich ist
1. zur Abwehr des Schadprogramms der sonstigen erheblichen Gefahren für die Kommunikationstechnik des Bundes,	1. zur Abwehr des Schadprogramms oder sonstigen erheblichen Gefahren für die Kommunikationstechnik des Bundes,
2. zur Abwehr von Gefahren, die von dem aufgefundenen Schadprogramm ausgehen, oder	2. zur Abwehr von Gefahren, die von dem aufgefundenen Schadprogramm ausgehen, oder
3. zur Erkennung und Abwehr anderer Schadprogramme oder Gefahren für die Kommunikationstechnik des Bundes.	3. zur Erkennung und Abwehr anderer Schadprogramme oder Gefahren für die Kommunikationstechnik des Bundes.

Entwurf	Beschlüsse des 4. Ausschusses
Ein Schadprogramm kann beseitigt oder in seiner Funktionsweise gehindert werden. Es dürfen die erforderlichen technischen Maßnahmen getroffen werden, um eine sonstige erhebliche Gefahr für die Kommunikationstechnik des Bundes zu beseitigen. Das Bundesamt kann die Daten an die betroffene Einrichtung der Bundesverwaltung übermitteln, soweit dies für eine Verwendung nach den Sätzen 1 bis 4 erforderlich ist. 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. Die Anordnung nach Satz 4 muss die daraus erwachsenden Übermittlungsbefugnisse nach Absatz 6 berücksichtigen.	Ein Schadprogramm kann beseitigt oder in seiner Funktionsweise gehindert werden. Es dürfen die erforderlichen technischen Maßnahmen getroffen werden, um eine sonstige erhebliche Gefahr für die Kommunikationstechnik des Bundes zu beseitigen. Das Bundesamt kann die Daten an die betroffene Einrichtung der Bundesverwaltung übermitteln, soweit dies für eine Verwendung nach den Sätzen 1 bis 4 erforderlich ist. 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. Die Anordnung nach Satz 4 muss die daraus erwachsenden Übermittlungsbefugnisse nach Absatz 6 berücksichtigen.

Entwurf	Beschlüsse des 4. Ausschusses
(5) Die Beteiligten des Kommunikationsvorgangs sind spätestens nach dem Erkennen und der Abwehr eines Schadprogramms oder seiner Wirkungen oder von sonstigen erheblichen Gefahren für die Kommunikationstechnik des Bundes, 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 wenn 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 6 und 7 erfolgt die Benachrichtigung durch die dort genannten Behörden in entsprechender Anwendung der für diese Behörden geltenden Vorschriften. Enthalten diese Vorschriften keine Bestimmungen zu Benachrichtigungspflichten, sind die Vorschriften der Strafprozessordnung entsprechend anzuwenden.	(5) Die Beteiligten des Kommunikationsvorgangs sind spätestens nach dem Erkennen und der Abwehr eines Schadprogramms oder seiner Wirkungen oder von sonstigen erheblichen Gefahren für die Kommunikationstechnik des Bundes, 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 wenn 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 6 und 7 erfolgt die Benachrichtigung durch die dort genannten Behörden in entsprechender Anwendung der für diese Behörden geltenden Vorschriften. Enthalten diese Vorschriften keine Bestimmungen zu Benachrichtigungspflichten, sind die Vorschriften der Strafprozessordnung entsprechend anzuwenden.
(6) Das Bundesamt kann die nach Absatz 4 verwendeten personenbezogenen Daten an die Strafverfolgungsbehörden zur Verfolgung einer mittels eines Schadprogramms oder im Rahmen einer sonstigen erheblichen Gefahr für die Kommunikationstechnik des Bundes begangenen Straftat nach den §§ 202a, 202b, 303a oder 303b des Strafgesetzbuches übermitteln. Es kann diese Daten ferner übermitteln	(6) Das Bundesamt kann die nach Absatz 4 verwendeten personenbezogenen Daten an die Strafverfolgungsbehörden zur Verfolgung einer mittels eines Schadprogramms oder im Rahmen einer sonstigen erheblichen Gefahr für die Kommunikationstechnik des Bundes begangenen Straftat nach den §§ 202a, 202b, 303a oder 303b des Strafgesetzbuches übermitteln. Es kann diese Daten ferner übermitteln
1. an die Polizeien des Bundes und der Länder zur Abwehr einer Gefahr für die öffentliche Sicherheit, die unmittelbar von einem Schadprogramm ausgeht,	1. an die Polizeien des Bundes und der Länder zur Abwehr einer Gefahr für die öffentliche Sicherheit, die unmittelbar von einem Schadprogramm ausgeht,

Entwurf	Beschlüsse des 4. Ausschusses
2. an das Bundesamt für Verfassungsschutz zur Unterrichtung über Tatsachen, die sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht erkennen lassen, sowie an den Militärischen Abschirmdienst, wenn sich diese Tätigkeiten gegen Personen, Dienststellen oder Einrichtungen im Geschäftsbereich des Bundesministeriums der Verteidigung richten,	2. an das Bundesamt für Verfassungsschutz zur Unterrichtung über Tatsachen, die sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht erkennen lassen, sowie an den Militärischen Abschirmdienst, wenn sich diese Tätigkeiten gegen Personen, Dienststellen oder Einrichtungen im Geschäftsbereich des Bundesministeriums der Verteidigung richten,
3. an den Bundesnachrichtendienst zur Unterrichtung über Tatsachen, die einen internationalen kriminellen, terroristischen oder staatlichen Angriff mittels Schadprogrammen oder vergleichbarer schädlich wirkender informationstechnischer Mittel auf die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Systemen in Fällen von erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland erkennen lassen.	3. an den Bundesnachrichtendienst zur Unterrichtung über Tatsachen, die einen internationalen kriminellen, terroristischen oder staatlichen Angriff mittels Schadprogrammen oder vergleichbarer schädlich wirkender informationstechnischer Mittel auf die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Systemen in Fällen von erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland erkennen lassen.
(7) Für sonstige Zwecke kann das Bundesamt die Daten nach Absatz 4 Satz 1 übermitteln	(7) Für sonstige Zwecke kann das Bundesamt die Daten nach Absatz 4 Satz 1 übermitteln
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,
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,
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 oder § 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 oder § 1 Absatz 1 des MAD-Gesetzes genannten Schutzgüter gerichtet sind,

Entwurf	Beschlüsse des 4. Ausschusses
4. an den Bundesnachrichtendienst, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand 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,	4. an den Bundesnachrichtendienst, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand 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,
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 4 erfolgt nach Anordnung des Bundesministeriums des Innern und für 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 4 erfolgt nach Anordnung des Bundesministeriums des Innern und für Heimat; die §§ 9 bis 16 des Artikel 10-Gesetzes gelten entsprechend.

Entwurf	Beschlüsse des 4. Ausschusses
(8) 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 4 Erkenntnisse aus dem Kernbereich privater Lebensgestaltung oder Daten nach Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 erlangt, dürfen diese Erkenntnisse und Daten nicht verwendet werden. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung sind unverzüglich zu löschen. Dies gilt auch in Zweifelsfällen. Die Tatsache der Erlangung und Löschung dieser Erkenntnisse 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 Kalenderjahres, das dem Jahr folgt, in dem die der Dokumentation erstellt worden ist. Werden im Rahmen der Absätze 5 oder 6 Inhalte oder Umstände der Kommunikation von in § 53 Absatz 1 Satz 1 der Strafprozessordnung genannten Personen übermittelt, auf die sich das Zeugnisverweigerungsrecht dieser 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.	(8) 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 4 Erkenntnisse aus dem Kernbereich privater Lebensgestaltung oder Daten nach Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 erlangt, dürfen diese Erkenntnisse und Daten nicht verwendet werden. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung sind unverzüglich zu löschen. Dies gilt auch in Zweifelsfällen. Die Tatsache der Erlangung und Löschung dieser Erkenntnisse 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 Kalenderjahres, das dem Jahr folgt, in dem die der Dokumentation erstellt worden ist. Werden im Rahmen der Absätze 5 oder 6 Inhalte oder Umstände der Kommunikation von in § 53 Absatz 1 Satz 1 der Strafprozessordnung genannten Personen übermittelt, auf die sich das Zeugnisverweigerungsrecht dieser 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.
(9) Vor Aufnahme der Datenerhebung und -verwendung hat das Bundesamt ein Datenerhebungs- und -verwendungskonzept zu erstellen und für Kontrollen durch die Bundesbeauftragte oder 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. Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit teilt das Ergebnis seiner Kontrollen nach § 16 des Bundesdatenschutzgesetzes auch den Ressorts mit.	(9) Vor Aufnahme der Datenerhebung und -verwendung hat das Bundesamt ein Datenerhebungs- und -verwendungskonzept zu erstellen und für Kontrollen durch die Bundesbeauftragte oder 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. Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit teilt das Ergebnis seiner Kontrollen nach § 16 des Bundesdatenschutzgesetzes auch den Ressorts mit.

Entwurf	Beschlüsse des 4. Ausschusses
(10) Das Bundesamt unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres über	(10) Das Bundesamt unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres über
1. die Anzahl der Vorgänge, in denen Daten nach Absatz 6 Satz 1, Absatz 6 Satz 2 Nummer 1 oder Absatz 7 Nummer 1 übermittelt wurden, aufgegliedert nach den einzelnen Übermittlungsbefugnissen,	1. die Anzahl der Vorgänge, in denen Daten nach Absatz 6 Satz 1, Absatz 6 Satz 2 Nummer 1 oder Absatz 7 Nummer 1 übermittelt wurden, aufgegliedert nach den einzelnen Übermittlungsbefugnissen,
2. die Anzahl der personenbezogenen Auswertungen nach Absatz 4 Satz 1, in denen der Verdacht widerlegt wurde,	2. die Anzahl der personenbezogenen Auswertungen nach Absatz 4 Satz 1, in denen der Verdacht widerlegt wurde,
3. die Anzahl der Fälle, in denen das Bundesamt nach Absatz 5 Satz 2 oder 3 von einer Benachrichtigung der Betroffenen abgesehen hat.	3. die Anzahl der Fälle, in denen das Bundesamt nach Absatz 5 Satz 2 oder 3 von einer Benachrichtigung der Betroffenen abgesehen hat.
(11) Das Bundesamt unterrichtet kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres den Ausschuss für Inneres und Heimat des Deutschen Bundestages über die Anwendung dieser Vorschrift.	(11) Das Bundesamt unterrichtet kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres den Ausschuss für Inneres und Heimat des Deutschen Bundestages über die Anwendung dieser Vorschrift.

Entwurf	Beschlüsse des 4. Ausschusses
§ 9	§ 9
Verarbeitung von Protokollierungsdaten der Kommunikationstechnik des Bundes	**Verarbeitung von Protokollierungsdaten der Kommunikationstechnik des Bundes**
(1) 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.	(1) 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.
(2) Die Einrichtungen der Bundesverwaltung sind verpflichtet, das Bundesamt bei Maßnahmen nach Absatz 1 zu unterstützen und hierbei den Zugang des Bundesamtes zu einrichtungsinternen Protokollierungsdaten nach Absatz 1 sicherzustellen. Hierzu dürfen sie dem Bundesamt die entsprechenden Protokollierungsdaten übermitteln. § 8 Absatz 1 Satz 5, Absatz 2 bis 5, 9 und 10 gilt entsprechend. § 7 Absatz 7 gilt für die Verpflichtung nach Satz 1 entsprechend.	(2) Die Einrichtungen der Bundesverwaltung sind verpflichtet, das Bundesamt bei Maßnahmen nach Absatz 1 zu unterstützen und hierbei den Zugang des Bundesamtes zu einrichtungsinternen Protokollierungsdaten nach Absatz 1 sicherzustellen. Hierzu dürfen sie dem Bundesamt die entsprechenden Protokollierungsdaten übermitteln. § 8 Absatz 1 Satz 5, Absatz 2 bis 5, 9 und 10 gilt entsprechend. § 7 Absatz 7 gilt für die Verpflichtung nach Satz 1 entsprechend.

Entwurf	Beschlüsse des 4. Ausschusses
§ 10	§ 10
Anordnungen von Maßnahmen zur Abwendung oder Behebung von Sicherheitsvorfällen	**Anordnungen von Maßnahmen zur Abwendung oder Behebung von Sicherheitsvorfällen**
Das Bundesamt kann im Einzelfall gegenüber Einrichtungen der Bundesverwaltung Maßnahmen anordnen, die zur Abwendung oder Behebung eines gegenwärtigen Sicherheitsvorfalls erforderlich sind. Ferner kann das Bundesamt die Einrichtungen der Bundesverwaltung zur Berichterstattung innerhalb einer angemessenen Frist zu den nach Satz 1 angeordneten Maßnahmen auffordern. Der oder die jeweils zuständige Informationssicherheitsbeauftragte des Ressorts wird über Anweisungen und Aufforderungen nach den Sätzen 1 und 2 durch das Bundesamt informiert. Der Bericht ist dem Bundesamt und zugleich dem oder der Informationssicherheitsbeauftragten des jeweils zuständigen Ressorts zu übermitteln. Für die Berichterstattung gilt § 4 Absatz 3 entsprechend.	Das Bundesamt kann im Einzelfall gegenüber Einrichtungen der Bundesverwaltung Maßnahmen anordnen, die zur Abwendung oder Behebung eines Sicherheitsvorfalls erforderlich sind. Ferner kann das Bundesamt die Einrichtungen der Bundesverwaltung zur Berichterstattung innerhalb einer angemessenen Frist zu den nach Satz 1 angeordneten Maßnahmen auffordern. Der oder die jeweils zuständige Informationssicherheitsbeauftragte des Ressorts wird über Anweisungen und Aufforderungen nach den Sätzen 1 und 2 durch das Bundesamt informiert. Der Bericht ist dem Bundesamt und zugleich dem oder der Informationssicherheitsbeauftragten des jeweils zuständigen Ressorts zu übermitteln. Für die Berichterstattung gilt § 4 Absatz 3 entsprechend.

Entwurf	Beschlüsse des 4. Ausschusses
§ 11	§ 11
Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen	**Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen**
(1) Handelt es sich bei einer Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines informationstechnischen Systems einer Einrichtung der Bundesverwaltung oder einer besonders wichtigen Einrichtung oder einer wichtigen Einrichtung um einen herausgehobenen Fall, so kann das Bundesamt auf Ersuchen der betroffenen Einrichtung oder des betroffenen Betreibers oder einer anderen für die Einrichtung oder den Betreiber zuständigen Behörde 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 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.	(1) Handelt es sich bei einer Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines informationstechnischen Systems einer Einrichtung der Bundesverwaltung oder einer besonders wichtigen Einrichtung oder einer wichtigen Einrichtung um einen herausgehobenen Fall, so kann das Bundesamt auf Ersuchen der betroffenen Einrichtung oder des betroffenen Betreibers oder einer anderen für die Einrichtung oder den Betreiber zuständigen Behörde 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 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.
(2) Ein herausgehobener Fall nach Absatz 1 liegt insbesondere dann vor, wenn es sich um einen Angriff von besonderer technischer Qualität handelt oder wenn 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 wenn die zügige Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems von besonderem öffentlichem Interesse ist.

Entwurf	Beschlüsse des 4. Ausschusses
(3) Das Bundesamt darf bei Maßnahmen nach Absatz 1 personenbezogene oder dem Fernmeldegeheimnis unterliegende Daten 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 8 ist entsprechend anzuwenden.	(3) Das Bundesamt darf bei Maßnahmen nach Absatz 1 personenbezogene oder dem Fernmeldegeheimnis unterliegende Daten 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 8 ist entsprechend anzuwenden.
(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 Informationen können entsprechend § 8 Absatz 6 und 7 übermittelt werden. Hiervon sind erforderliche Informationsaustausche zwischen dem Bundesamt und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe nach § 3 Absatz 7 des Dachgesetzes zur Stärkung der physischen Resilienz kritischer Anlagen (KRITIS-Dachgesetz) ausgenommen. Zugang zu den in Verfahren nach Absatz 1 geführten Akten wird Dritten nicht gewährt.	(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 Informationen können entsprechend § 8 Absatz 6 und 7 übermittelt werden. Hiervon sind erforderliche Informationsaustausche zwischen dem Bundesamt und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe nach § 3 Absatz 7 des Dachgesetzes zur Stärkung der physischen Resilienz kritischer Anlagen (KRITIS-Dachgesetz) ausgenommen. Zugang zu den in Verfahren nach Absatz 1 geführten Akten wird Dritten nicht gewährt.

Entwurf	Beschlüsse des 4. Ausschusses
(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.
(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.
(7) In begründeten Einzelfällen kann das Bundesamt auch bei anderen als den in Absatz 1 genannten Einrichtungen tätig werden, wenn das Bundesamt darum ersucht wurde und wenn es sich um einen herausgehobenen Fall nach Absatz 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 das Bundesamt darum ersucht wurde und wenn es sich um einen herausgehobenen Fall nach Absatzes 2 handelt. Ein begründeter Einzelfall liegt in der Regel vor, wenn eine Stelle eines Landes betroffen ist.
(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 Tätigkeiten, die einer Genehmigung nach dem Atomgesetz bedürfen, haben bei Maßnahmen des Bundesamtes nach diesem § 11 die Vorgaben aufgrund des Atomgesetzes Vorrang.	(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 Tätigkeiten, die einer Genehmigung nach dem Atomgesetz bedürfen, haben bei Maßnahmen des Bundesamtes nach diesem § 11 die Vorgaben aufgrund des Atomgesetzes Vorrang.

Entwurf	Beschlüsse des 4. Ausschusses
§ 12	§ 12
Bestandsdatenauskunft	**Bestandsdatenauskunft**
(1) Das Bundesamt darf zur Erfüllung seiner gesetzlichen Aufgabe nach § 3 Absatz 1 Satz 1 Nummer 1, 2, 20, 24 o der 25 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 Sektoren des § 2 Nummer 24 oder der öffentlichen Sicherheit, um damit eine Beeinträchtigung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme einer besonders wichtigen Einrichtung oder wichtigen Einrichtung 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 wenn die in die Auskunft aufzunehmenden Daten im Einzelfall erforderlich sind, um die Betroffenen nach Absatz 4 vor dieser Beeinträchtigung zu warnen, über diese Beeinträchtigung zu informieren oder bei der Beseitigung zu beraten oder zu unterstützen.	(1) Das Bundesamt darf zur Erfüllung seiner gesetzlichen Aufgabe nach § 3 Absatz 1 Satz 1 Nummer 1, 2, 20, 24 o der 25 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 Sektoren des § 2 Nummer 24 oder der öffentlichen Sicherheit, um damit eine Beeinträchtigung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme einer besonders wichtigen Einrichtung oder wichtigen Einrichtung 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 wenn die in die Auskunft aufzunehmenden Daten im Einzelfall erforderlich sind, um die Betroffenen nach Absatz 4 vor dieser Beeinträchtigung zu warnen, über diese Beeinträchtigung zu informieren oder bei der Beseitigung zu beraten oder zu unterstützen.
(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.
(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.

Entwurf	Beschlüsse des 4. Ausschusses
(4) Nach erfolgter Auskunft weist das Bundesamt die besonders wichtige Einrichtung oder die wichtige Einrichtung auf die bei ihr drohenden Beeinträchtigungen hin. Nach Möglichkeit weist das Bundesamt die besonders wichtige Einrichtung oder die wichtige Einrichtung auf technische Mittel hin, mittels derer die festgestellten Beeinträchtigungen durch die besonders wichtige Einrichtung oder die wichtige Einrichtung selbst beseitigt werden können.	(4) Nach erfolgter Auskunft weist das Bundesamt die besonders wichtige Einrichtung oder die wichtige Einrichtung auf die bei ihr drohenden Beeinträchtigungen hin. Nach Möglichkeit weist das Bundesamt die besonders wichtige Einrichtung oder die wichtige Einrichtung auf technische Mittel hin, mittels derer die festgestellten Beeinträchtigungen durch die besonders wichtige Einrichtung oder die wichtige Einrichtung selbst beseitigt werden können.
(5) Das Bundesamt kann personenbezogene Daten, die es im Rahmen dieser Vorschrift verarbeitet, entsprechend § 8 Absatz 6 und 7 übermitteln.	(5) Das Bundesamt kann personenbezogene Daten, die es im Rahmen dieser Vorschrift verarbeitet, entsprechend § 8 Absatz 6 und 7 übermitteln.
(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 6 oder wenn Tatsachen die Annahme rechtfertigen, dass die Voraussetzungen einer Weitergabe nach § 8 Absatz 6 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.	(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 6 oder wenn Tatsachen die Annahme rechtfertigen, dass die Voraussetzungen einer Weitergabe nach § 8 Absatz 6 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.
(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
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
2. die Übermittlungen nach Absatz 5.	2. die Übermittlungen nach Absatz 5.
(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.

Entwurf	Beschlüsse des 4. Ausschusses
§ 13	§ 13
Warnungen	**Warnungen**
(1) Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 20 und 21 kann das Bundesamt	(1) Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 20 und 21 kann das Bundesamt
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:
a) Warnungen vor Schwachstellen und anderen Sicherheitsrisiken in informationstechnischen Produkten und Diensten,	a) Warnungen vor Schwachstellen und anderen Sicherheitsrisiken in informationstechnischen Produkten und Diensten,
b) Warnungen vor Schadprogrammen,	b) Warnungen vor Schadprogrammen,
c) Warnungen bei einem Verlust oder einem unerlaubten Zugriff auf Daten,	c) Warnungen bei einem Verlust oder einem unerlaubten Zugriff auf Daten,
d) Informationen über sicherheitsrelevante IT-Eigenschaften von Produkten und	d) Informationen über sicherheitsrelevante IT-Eigenschaften von Produkten und
e) Informationen über Verstöße besonders wichtiger Einrichtungen oder wichtiger Einrichtungen gegen die Pflichten aus diesem Gesetz sowie	e) Informationen über Verstöße besonders wichtiger Einrichtungen oder wichtiger Einrichtungen gegen die Pflichten aus diesem Gesetz sowie
2. Sicherheitsmaßnahmen und Einsatz bestimmter Sicherheitsprodukte empfehlen.	2. Sicherheitsmaßnahmen und Einsatz bestimmter Sicherheitsprodukte empfehlen.
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.
(2) Die Hersteller betroffener Produkte sind rechtzeitig vor Veröffentlichung der Warnungen zu informieren. Diese Informationspflicht besteht nicht,	(2) Die Hersteller betroffener Produkte sind rechtzeitig vor Veröffentlichung der Warnungen zu informieren. Diese Informationspflicht besteht nicht,
1. wenn hierdurch die Erreichung des mit der Maßnahme verfolgten Zwecks gefährdet würde oder	1. wenn hierdurch die Erreichung des mit der Maßnahme verfolgten Zwecks gefährdet würde oder

Entwurf	Beschlüsse des 4. Ausschusses
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.
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.	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.
(3) Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 20 und 21 kann das Bundesamt die Öffentlichkeit unter Nennung der Bezeichnung und des Herstellers des betroffenen Produkts und Dienstes	(3) Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 20 und 21 kann das Bundesamt die Öffentlichkeit unter Nennung der Bezeichnung und des Herstellers des betroffenen Produkts und Dienstes
1. 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	1. 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
2. Sicherheitsmaßnahmen sowie den Einsatz bestimmter informationstechnischer Produkte und Dienste empfehlen.	2. Sicherheitsmaßnahmen sowie den Einsatz bestimmter informationstechnischer Produkte und Dienste empfehlen.
Stellen sich die an die Öffentlichkeit gegebenen Informationen im Nachhinein als falsch heraus oder stellen sich 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.	Stellen sich die an die Öffentlichkeit gegebenen Informationen im Nachhinein als falsch heraus oder stellen sich 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.

Entwurf	Beschlüsse des 4. Ausschusses
§ 14	§ 14
Untersuchung der Sicherheit in der Informationstechnik, Auskunftsverlangen	**Untersuchung der Sicherheit in der Informationstechnik, Auskunftsverlangen**
(1) Das Bundesamt kann zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 20, 21, 24 oder 25 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, 20, 21, 24 oder 25 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.
(2) Soweit erforderlich, kann das Bundesamt für Untersuchungen nach Absatz 1 Satz 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 § 65 vorgesehenen Sanktionen.	(2) Soweit erforderlich, kann das Bundesamt für Untersuchungen nach Absatz 1 Satz 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 § 65 vorgesehenen Sanktionen.
(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.

Entwurf	Beschlüsse des 4. Ausschusses
(4) Die Auskünfte und die aus den Untersuchungen gewonnenen Erkenntnisse dürfen nur zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 20, 21, 24 und 25 genutzt werden. Das Bundesamt darf seine Erkenntnisse weitergeben und veröffentlichen, soweit dies zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 20, 21, 24 und 25 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 zu den untersuchten informationstechnischen Produkten und Systemen weitergegeben oder veröffentlicht werden.	(4) Die Auskünfte und die aus den Untersuchungen gewonnenen Erkenntnisse dürfen nur zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 20, 21, 24 und 25 genutzt werden. Das Bundesamt darf seine Erkenntnisse weitergeben und veröffentlichen, soweit dies zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 20, 21, 24 und 25 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 zu den untersuchten informationstechnischen Produkten und Systemen weitergegeben oder veröffentlicht werden.
(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. § 13 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. § 13 Absatz 2 Satz 2 gilt entsprechend.
§ 15	§ 15
Detektion von Angriffsmethoden und von Sicherheitsrisiken für die Netz- und IT-Sicherheit	**Detektion von Angriffsmethoden und von Sicherheitsrisiken für die Netz- und IT-Sicherheit**
(1) Das Bundesamt kann im Rahmen seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 2, 20 oder 24 zur Detektion von bekannten Schwachstellen und anderen Sicherheitsrisiken bei Einrichtungen der Bundesverwaltung, bei besonders wichtigen Einrichtungen oder bei wichtigen Einrichtungen Abfragen an den Schnittstellen öffentlich erreichbarer informationstechnischer Systeme zu öffentlichen Telekommunikationsnetzen durchführen,	(1) Das Bundesamt kann im Rahmen seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 2, 20 oder 24 zur Detektion von bekannten Schwachstellen und anderen Sicherheitsrisiken Abfragen an den Schnittstellen öffentlich erreichbarer informationstechnischer Systeme zu öffentlichen Telekommunikationsnetzen durchführen,

Entwurf	Beschlüsse des 4. Ausschusses
1. um festzustellen, ob diese Schnittstellen unzureichend geschützt und dadurch in ihrer Sicherheit oder Funktionsfähigkeit gefährdet sein können, oder	1. um festzustellen, ob diese Schnittstellen unzureichend geschützt und dadurch in ihrer Sicherheit oder Funktionsfähigkeit gefährdet sein können, oder
2. wenn die entsprechenden Einrichtungen darum ersuchen.	2. wenn die entsprechenden Einrichtungen der Bundesverwaltung, besonders wichtige oder wichtige Einrichtungen darum ersuchen.
Die dadurch gewonnenen Erkenntnisse dürfen nur zum Zweck der Information nach Absatz 2 verwendet werden. Erlangt das Bundesamt dabei Informationen, die durch Artikel 10 des Grundgesetzes geschützt sind, sind diese unverzüglich zu löschen.	Erlangt das Bundesamt dabei Informationen, die durch Artikel 10 des Grundgesetzes geschützt sind, sind diese unverzüglich zu löschen.
(2) Wird durch Abfragen gemäß Absatz 1 eine bekannte Schwachstelle oder ein anderes Sicherheitsrisiko eines informationstechnischen Systems erkannt, informiert das Bundesamt darüber unverzüglich die für das informationstechnische System Verantwortlichen. Gehört das informationstechnische System zu einer Einrichtung der Bundesverwaltung, sind zugleich die Informationssicherheitsbeauftragten der betroffenen Einrichtung der Bundesverwaltung nach § 45 und des übergeordneten Ressorts nach § 46 zu informieren. Das Bundesamt soll dabei auf bestehende Möglichkeiten zur Abhilfe des Sicherheitsrisikos hinweisen. Sind dem Bundesamt die Verantwortlichen nicht bekannt oder ist ihre Identifikation nur mit unverhältnismäßigem Aufwand oder über eine Bestandsdatenabfrage nach § 12 möglich, so ist hilfsweise der betreibende Dienstleister des jeweiligen Netzes oder Systems unverzüglich zu benachrichtigen, wenn überwiegende Sicherheitsinteressen nicht entgegenstehen.	(2) Wird durch Abfragen gemäß Absatz 1 eine bekannte Schwachstelle oder ein anderes Sicherheitsrisiko eines informationstechnischen Systems erkannt, informiert das Bundesamt darüber unverzüglich die für das informationstechnische System Verantwortlichen der Einrichtung der Bundesverwaltung, der besonders wichtigen oder der wichtigen Einrichtung. Gehört das informationstechnische System zu einer Einrichtung der Bundesverwaltung, sind zugleich die Informationssicherheitsbeauftragten der betroffenen Einrichtung der Bundesverwaltung nach § 45 und des übergeordneten Ressorts nach § 46 zu informieren. Das Bundesamt soll dabei auf bestehende Möglichkeiten zur Abhilfe des Sicherheitsrisikos hinweisen. Sind dem Bundesamt die Verantwortlichen nicht bekannt oder ist ihre Identifikation nur mit unverhältnismäßigem Aufwand oder über eine Bestandsdatenabfrage nach § 12 möglich, so ist hilfsweise der betreibende Dienstleister des jeweiligen Netzes oder Systems unverzüglich zu benachrichtigen, wenn überwiegende Sicherheitsinteressen nicht entgegenstehen.
(3) 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 gemäß Absatz 1 durchgeführten Abfragen.	(3) 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 gemäß Absatz 1 durchgeführten Abfragen.

Entwurf	Beschlüsse des 4. Ausschusses
(4) Das Bundesamt legt der Bundesbeauftragten oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu den Abfragen nach Absatz 1 auf Anforderung eine Liste der geprüften Systeme der Einrichtungen der Bundesverwaltung, der besonders wichtigen Einrichtungen und der wichtigen Einrichtungen zur Kontrolle vor.	(4) Das Bundesamt legt der Bundesbeauftragten oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu den Abfragen nach Absatz 1 auf Anforderung eine Liste der geprüften Systeme der Einrichtungen der Bundesverwaltung, der besonders wichtigen Einrichtungen und der wichtigen Einrichtungen zur Kontrolle vor.
(5) Das Bundesamt darf zur Erfüllung seiner Aufgaben Systeme und Verfahren einsetzen, die 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.	(5) Das Bundesamt darf zur Erfüllung seiner Aufgaben Systeme und Verfahren einsetzen, die 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.
§ 16	§ 16
Anordnungen von Maßnahmen des Bundesamtes gegenüber Anbietern von Telekommunikationsdiensten	**Anordnungen von Maßnahmen des Bundesamtes gegenüber Anbietern von Telekommunikationsdiensten**
(1) Zur Abwehr erheblicher Gefahren für die in Absatz 2 genannten Schutzgüter kann das Bundesamt anordnen, dass ein Anbieter von öffentlich zugänglichen Telekommunikationsdiensten im Sinne des Telekommunikationsgesetzes (Anbieter von öffentlich zugänglichen Telekommunikationsdiensten) mit mehr als 100 000 Kunden	(1) Zur Abwehr erheblicher Gefahren für die in Absatz 2 genannten Schutzgüter kann das Bundesamt anordnen, dass ein Anbieter von öffentlich zugänglichen Telekommunikationsdiensten im Sinne des Telekommunikationsgesetzes (Anbieter von öffentlich zugänglichen Telekommunikationsdiensten) mit mehr als 100 000 Kunden
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
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,

Entwurf	Beschlüsse des 4. Ausschusses
sofern und soweit der Anbieter von öffentlich zugänglichen Telekommunikationsdiensten dazu technisch in der Lage 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 8 Satz 2 bis 8 gilt entsprechend. Widerspruch und Anfechtungsklage gegen die Anordnungen nach Satz 1 haben keine aufschiebende Wirkung.	sofern und soweit der Anbieter von öffentlich zugänglichen Telekommunikationsdiensten dazu technisch in der Lage 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 8 Satz 2 bis 8 gilt entsprechend. Widerspruch und Anfechtungsklage gegen die Anordnungen nach Satz 1 haben keine aufschiebende Wirkung.
(2) Schutzgüter gemäß Absatz 1 Satz 1 sind die Verfügbarkeit, Integrität oder Vertraulichkeit	(2) Schutzgüter gemäß Absatz 1 Satz 1 sind die Verfügbarkeit, Integrität oder Vertraulichkeit
1. der Kommunikationstechnik des Bundes, einer besonders wichtigen Einrichtung oder einer wichtigen Einrichtung,	1. der Kommunikationstechnik des Bundes, einer besonders wichtigen Einrichtung oder einer wichtigen Einrichtung,
2. von Informations- oder Kommunikationsdiensten oder	2. von Informations- oder Kommunikationsdiensten oder
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.
(3) Ordnet das Bundesamt eine Maßnahme nach Absatz 1 Satz 1 Nummer 1 an, so kann es gegenüber dem Anbieter von öffentlich zugänglichen Telekommunikationsdiensten auch anordnen, den Datenverkehr an eine vom Bundesamt benannte Anschlusskennung umzuleiten.	(3) Ordnet das Bundesamt eine Maßnahme nach Absatz 1 Satz 1 Nummer 1 an, so kann es gegenüber dem Anbieter von öffentlich zugänglichen Telekommunikationsdiensten auch anordnen, den Datenverkehr an eine vom Bundesamt benannte Anschlusskennung umzuleiten.

Entwurf	Beschlüsse des 4. Ausschusses
(4) Das Bundesamt darf Daten, die von einem Anbieter von öffentlich zugänglichen Telekommunikationsdiensten 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 8 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 Anbieter von öffentlich zugänglichen Telekommunikationsdiensten 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 8 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.
§ 17	§ 17
Anordnungen von Maßnahmen des Bundesamtes gegenüber Anbietern von digitalen Diensten	**Anordnungen von Maßnahmen des Bundesamtes gegenüber Anbietern von digitalen Diensten**
Das Bundesamt kann in Einzelfällen zur Abwehr erheblicher Gefahren für informationstechnische Systeme einer Vielzahl von Nutzern, die von digitalen Diensten von Anbietern von digitalen Diensten nach § 2 Absatz 2 Nummer 1 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes ausgehen, die durch ungenügende technische und organisatorische Vorkehrungen nach § 19 Absatz 4 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes unzureichend gesichert sind und dadurch keinen hinreichenden Schutz bieten vor	Das Bundesamt kann in Einzelfällen zur Abwehr erheblicher Gefahren für informationstechnische Systeme einer Vielzahl von Nutzern, die von digitalen Diensten von Anbietern von digitalen Diensten nach § 2 Absatz 2 Nummer 1 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes ausgehen, die durch ungenügende technische und organisatorische Vorkehrungen nach § 19 Absatz 4 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes unzureichend gesichert sind und dadurch keinen hinreichenden Schutz bieten vor
1. unerlaubten Zugriffen auf die für diese digitalen Dienste genutzten technischen Einrichtungen oder	1. unerlaubten Zugriffen auf die für diese digitalen Dienste genutzten technischen Einrichtungen oder
2. Störungen, auch soweit sie durch äußere Angriffe bedingt sind,	2. Störungen, auch soweit sie durch äußere Angriffe bedingt sind,

Entwurf	Beschlüsse des 4. Ausschusses
gegenüber dem jeweiligen Anbieter von digitalen Diensten nach § 2 Absatz 2 Nummer 1 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes anordnen, dass dieser die jeweils zur Herstellung des ordnungsgemäßen Zustands seiner digitalen Dienste erforderlichen technischen und organisatorischen Maßnahmen ergreift, um den ordnungsgemäßen Zustand seiner digitalen Dienste herzustellen. Die Zuständigkeit der Aufsichtsbehörden der Länder bleibt im Übrigen unberührt.	gegenüber dem jeweiligen Anbieter von digitalen Diensten nach § 2 Absatz 2 Nummer 1 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes anordnen, dass dieser die jeweils zur Herstellung des ordnungsgemäßen Zustands seiner digitalen Dienste erforderlichen technischen und organisatorischen Maßnahmen ergreift, um den ordnungsgemäßen Zustand seiner digitalen Dienste herzustellen. Die Zuständigkeit der Aufsichtsbehörden der Länder bleibt im Übrigen unberührt.
§ 18	§ 18
Anordnungen von Maßnahmen des Bundesamtes gegenüber Herstellern von IKT-Produkten	**Anordnungen von Maßnahmen des Bundesamtes gegenüber Herstellern von IKT-Produkten**
Soweit erforderlich, kann das Bundesamt von einem Hersteller, deren IKT-Produkte von erheblichen Sicherheitsvorfällen betroffen sind, die Mitwirkung an der Beseitigung oder Vermeidung erheblicher Sicherheitsvorfälle bei besonders wichtigen Einrichtungen und wichtigen Einrichtungen verlangen.	Soweit erforderlich, kann das Bundesamt von einem Hersteller, deren IKT-Produkte von erheblichen Sicherheitsvorfällen betroffen sind, die Mitwirkung an der Beseitigung oder Vermeidung erheblicher Sicherheitsvorfälle bei besonders wichtigen Einrichtungen und wichtigen Einrichtungen verlangen.
§ 19	§ 19
Bereitstellung von IT-Sicherheitsprodukten	**Bereitstellung von IT-Sicherheitsprodukten**
Die Bereitstellung von IT-Sicherheitsprodukten durch das Bundesamt nach § 3 Absatz 1 Satz 2 Nummer 15 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 und der Bundeshaushaltsordnung bleiben unberührt. Wenn das Bundesamt IT-Sicherheitsprodukte bereitstellt, können die Einrichtungen der Bundesverwaltung oder von ihnen beauftragte Dritte diese Produkte beim Bundesamt abrufen.	Die Bereitstellung von IT-Sicherheitsprodukten durch das Bundesamt nach § 3 Absatz 1 Satz 2 Nummer 15 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 und der Bundeshaushaltsordnung bleiben unberührt. Wenn das Bundesamt IT-Sicherheitsprodukte bereitstellt, können die Einrichtungen der Bundesverwaltung oder von ihnen beauftragte Dritte diese Produkte beim Bundesamt abrufen.

Entwurf	Beschlüsse des 4. Ausschusses
Kapitel 2	Kapitel 2
Datenverarbeitung	Datenverarbeitung
§ 20	§ 20
Verarbeitung personenbezogener Daten	**Verarbeitung personenbezogener Daten**
(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.
(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 in der jeweils geltenden Fassung und von § 23 des Bundesdatenschutzgesetzes zulässig, wenn	(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 in der jeweils geltenden Fassung und von § 23 des Bundesdatenschutzgesetzes zulässig, wenn
1. die Verarbeitung erforderlich ist	1. die Verarbeitung erforderlich ist
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
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
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.
(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

Entwurf	Beschlüsse des 4. Ausschusses
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,
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
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.
(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.
§ 21	§ 21
Beschränkungen der Rechte der betroffenen Person	**Beschränkungen der Rechte der betroffenen Person**
Für die Rechte der betroffenen Person gegenüber dem 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 gegenüber dem 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.
§ 22	§ 22
Informationspflicht bei Erhebung von personenbezogenen Daten	**Informationspflicht bei Erhebung von personenbezogenen Daten**
(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

Entwurf	Beschlüsse des 4. Ausschusses
1. die Informationserteilung die ordnungsgemäße Erfüllung der in der Zuständigkeit des Bundesamtes liegenden Aufgaben gefährden würde oder	1. die Informationserteilung die ordnungsgemäße Erfüllung der in der Zuständigkeit des Bundesamtes liegenden Aufgaben gefährden würde oder
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
und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss.	und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss.
(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.
§ 23	§ 23
Auskunftsrecht der betroffenen Person	**Auskunftsrecht der betroffenen Person**
(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
1. die Auskunftserteilung die ordnungsgemäße Erfüllung der Aufgaben gefährden würde, die in der Zuständigkeit des Bundesamtes liegen,	1. die Auskunftserteilung die ordnungsgemäße Erfüllung der Aufgaben gefährden würde, die in der Zuständigkeit des Bundesamtes liegen,
2. die Auskunftserteilung	2. die Auskunftserteilung
a) die öffentliche Sicherheit oder die Gewährleistung der Netz- und Informationssicherheit gefährden würde oder	a) die öffentliche Sicherheit oder die Gewährleistung der Netz- und Informationssicherheit gefährden würde oder

Entwurf	Beschlüsse des 4. Ausschusses
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
3. die Auskunftserteilung strafrechtliche Ermittlungen oder die Verfolgung von Straftaten gefährden würde	3. die Auskunftserteilung strafrechtliche Ermittlungen oder die Verfolgung von Straftaten gefährden würde
und deswegen das Interesse der betroffenen Person an der Auskunftserteilung zurücktreten muss.	und deswegen das Interesse der betroffenen Person an der Auskunftserteilung zurücktreten muss.
(2) § 34 Absatz 2 bis 4 des Bundesdatenschutzgesetzes gilt entsprechend.	(2) § 34 Absatz 2 bis 4 des Bundesdatenschutzgesetzes gilt entsprechend.
§ 24	§ 24
Recht auf Berichtigung	**Recht auf Berichtigung**
(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.
(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.
§ 25	§ 25
Recht auf Löschung	**Recht auf Löschung**
(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

Entwurf	Beschlüsse des 4. Ausschusses
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
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.
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.
(2) Ist die Löschung lediglich für eine etwaige gerichtliche Überprüfung von Maßnahmen nach § 8 Absatz 4 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 8 bleibt unberührt.	(2) Ist die Löschung lediglich für eine etwaige gerichtliche Überprüfung von Maßnahmen nach § 8 Absatz 4 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 8 bleibt unberührt.
§ 26	§ 26
Recht auf Einschränkung der Verarbeitung	**Recht auf Einschränkung der Verarbeitung**
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
1. die Verarbeitung oder Weiterverarbeitung durch dieses Gesetz ausdrücklich geregelt ist oder	1. die Verarbeitung oder Weiterverarbeitung durch dieses Gesetz ausdrücklich geregelt ist oder
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.

Entwurf	Beschlüsse des 4. Ausschusses
§ 27	§ 27
Widerspruchsrecht	**Widerspruchsrecht**
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
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
2. eine Rechtsvorschrift das Bundesamt zur Verarbeitung verpflichtet.	2. eine Rechtsvorschrift das Bundesamt zur Verarbeitung verpflichtet.
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.	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.
Teil 3	Teil 3
Sicherheit in der Informationstechnik von Einrichtungen	Sicherheit in der Informationstechnik von Einrichtungen
Kapitel 1	Kapitel 1
Anwendungsbereich	Anwendungsbereich
§ 28	§ 28
Besonders wichtige Einrichtungen und wichtige Einrichtungen	**Besonders wichtige Einrichtungen und wichtige Einrichtungen**
(1) Als besonders wichtige Einrichtung gelten	(1) Als besonders wichtige Einrichtung gelten
1. Betreiber kritischer Anlagen,	1. Betreiber kritischer Anlagen,

Entwurf	Beschlüsse des 4. Ausschusses
2. qualifizierte Vertrauensdiensteanbieter, Top Level Domain Name Registries oder DNS-Diensteanbieter,	2. qualifizierte Vertrauensdiensteanbieter, Top Level Domain Name Registries oder DNS-Diensteanbieter,
3. Anbieter öffentlich zugänglicher Telekommunikationsdienste oder Betreiber öffentlicher Telekommunikationsnetze, die	3. Anbieter öffentlich zugänglicher Telekommunikationsdienste oder Betreiber öffentlicher Telekommunikationsnetze, die
a) mindestens 50 Mitarbeiter beschäftigen oder	a) mindestens 50 Mitarbeiter beschäftigen oder
b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen,	b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen,
4. sonstige natürliche oder juristische Personen oder rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbieten, die einer der in Anlage 1 bestimmten Einrichtungsarten zuzuordnen sind und die	4. sonstige natürliche oder juristische Personen oder rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbieten, die einer der in Anlage 1 bestimmten Einrichtungsarten zuzuordnen sind und die
a) mindestens 250 Mitarbeiter beschäftigen oder	a) mindestens 250 Mitarbeiter beschäftigen oder
b) einen Jahresumsatz von über 50 Millionen Euro und zudem eine Jahresbilanzsumme von über 43 Millionen Euro aufweisen.	b) einen Jahresumsatz von über 50 Millionen Euro und zudem eine Jahresbilanzsumme von über 43 Millionen Euro aufweisen.
Davon ausgenommen sind Einrichtungen der Bundesverwaltung, sofern sie nicht gleichzeitig Betreiber kritischer Anlagen sind.	Davon ausgenommen sind Einrichtungen der Bundesverwaltung, sofern sie nicht gleichzeitig Betreiber kritischer Anlagen sind.
(2) Als wichtige Einrichtungen gelten	(2) Als wichtige Einrichtungen gelten
1. Vertrauensdiensteanbieter,	1. Vertrauensdiensteanbieter,
2. Anbieter öffentlich zugänglicher Telekommunikationsdienste oder Betreiber öffentlicher Telekommunikationsnetze, die	2. Anbieter öffentlich zugänglicher Telekommunikationsdienste oder Betreiber öffentlicher Telekommunikationsnetze, die
a) weniger als 50 Mitarbeiter beschäftigen und	a) weniger als 50 Mitarbeiter beschäftigen und

Entwurf	Beschlüsse des 4. Ausschusses
b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils 10 Millionen Euro oder weniger aufweisen,	b) einen Jahresumsatz oder eine Jahresbilanzsumme von jeweils 10 Millionen Euro oder weniger aufweisen,
3. natürliche oder juristische Personen oder rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbietet, die einer der in den Anlagen 1 und 2 bestimmten Einrichtungsarten zuzuordnen sind und die	3. natürliche oder juristische Personen oder rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbietet, die einer der in den Anlagen 1 und 2 bestimmten Einrichtungsarten zuzuordnen sind und die
a) mindestens 50 Mitarbeiter beschäftigen oder	a) mindestens 50 Mitarbeiter beschäftigen oder
b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen.	b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen.
Davon ausgenommen sind besonders wichtige Einrichtungen und Einrichtungen der Bundesverwaltung.	Davon ausgenommen sind besonders wichtige Einrichtungen und Einrichtungen der Bundesverwaltung.
(3) Bei der Bestimmung von Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme nach den Absätzen 1 und 2 ist auf	(3) Bei der Bestimmung von Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme nach den Absätzen 1 und 2 ist auf
1. die der Einrichtungsart zuzuordnende Geschäftstätigkeit abzustellen und	1. die der Einrichtungsart zuzuordnende Geschäftstätigkeit abzustellen und
2. außer für rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft die Empfehlung der Kommission 2003/361/EG vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20. Mai 2003, S. 36) mit Ausnahme von Artikel 3 Absatz 4 des Anhangs anzuwenden.	2. außer für rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft die Empfehlung der Kommission 2003/361/EG vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20. Mai 2003, S. 36) mit Ausnahme von Artikel 3 Absatz 4 des Anhangs anzuwenden.

Entwurf	Beschlüsse des 4. Ausschusses
Die Daten von Partner- oder verbundenen Unternehmen im Sinne der Empfehlung der Kommission 2003/361/EG sind nicht hinzuzurechnen, wenn das Unternehmen unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände mit Blick auf die Beschaffenheit und den Betrieb der informationstechnischen Systeme, Komponenten und Prozesse unabhängig von seinen Partner- oder verbundenen Unternehmen ist.	Die Daten von Partner- oder verbundenen Unternehmen im Sinne der Empfehlung der Kommission 2003/361/EG sind nicht hinzuzurechnen, wenn das Unternehmen unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände mit Blick auf die Beschaffenheit und den Betrieb der informationstechnischen Systeme, Komponenten und Prozesse unabhängig von seinen Partner- oder verbundenen Unternehmen ist.
(4) Die §§ 30, 31, 32, 35, 36, 38, 39, 61 und 62 sind nicht anzuwenden auf besonders wichtige Einrichtungen und wichtige Einrichtungen, die	(4) Die §§ 30, 31, 32, 35, 36, 38, 39, 61 und 62 sind nicht anzuwenden auf besonders wichtige Einrichtungen und wichtige Einrichtungen, die
1. ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen,	1. ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen,
2. Energieversorgungsnetze oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 1 des Gesetzes vom 14. Mai 2024 (BGBl. 2024 I Nr. 161) geändert worden ist, betreiben und den Regelungen des § 5c des Energiewirtschaftsgesetzes unterliegen.	2. Energieversorgungsnetze, Energieanlagen oder digitale Energiedienste im Sinne des Energiewirtschaftsgesetz vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 26 des Gesetzes vom 15. Juli 2024 (BGBl. 2024 I Nr. 236) geändert worden ist, betreiben und den Regelungen des § 5c des Energiewirtschaftsgesetzes unterliegen.
Satz 1 gilt nicht für die dort aufgeführten besonders wichtigen und wichtigen Einrichtungen, soweit sie über die in Satz 1 Nummer 1 und 2 genannten Anlagen hinaus weitere kritische Anlagen nach § 2 Nummer 22 betreiben oder aufgrund weiterer Tätigkeiten einer der in Anlage 1 oder 2 bestimmten Einrichtungsarten zuzuordnen sind. Satz 2 gilt für alle informationstechnischen Systeme, die für den Betrieb der weiteren kritischen Anlagen erforderlich sind.	Satz 1 gilt nicht für die dort aufgeführten besonders wichtigen und wichtigen Einrichtungen, soweit sie über die in Satz 1 Nummer 1 und 2 genannten Anlagen hinaus weitere kritische Anlagen nach § 2 Nummer 22 betreiben oder aufgrund weiterer Tätigkeiten einer der in Anlage 1 oder 2 bestimmten Einrichtungsarten zuzuordnen sind. Satz 2 gilt für alle informationstechnischen Systeme, die für den Betrieb der weiteren kritischen Anlagen erforderlich sind.
(5) Die §§ 30, 31, 32, 35, 36, 38 und 39 gelten nicht für	(5) Die §§ 30, 31, 32, 35, 36, 38 und 39 gelten nicht für

Entwurf	Beschlüsse des 4. Ausschusses
1. Finanzunternehmen nach Artikel 2 Absatz 2 der Verordnung (EU) 2022/2554 und Unternehmen, für die die Anforderungen der Verordnung (EU) 2022/2554 auf Grund von § 1a Absatz 2 des Kreditwesengesetzes oder § 293 Absatz 5 des Versicherungsaufsichtsgesetzes gelten,	1. Finanzunternehmen nach Artikel 2 Absatz 2 der Verordnung (EU) 2022/2554 und Unternehmen, für die die Anforderungen der Verordnung (EU) 2022/2554 auf Grund von § 1a Absatz 2 des Kreditwesengesetzes oder § 293 Absatz 5 des Versicherungsaufsichtsgesetzes gelten,
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.	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.
(6) § 32 gilt nicht für Betreiber kritischer Anlagen, soweit sie eine Anlage für Unternehmen nach Absatz 5 Nummer 1 betreiben.	(6) § 32 gilt nicht für Betreiber kritischer Anlagen, soweit sie eine Anlage für Unternehmen nach Absatz 5 Nummer 1 betreiben.
(7) Ein Betreiber kritischer Anlagen ist eine natürliche oder juristische Person oder eine rechtlich unselbstständige Organisationseinheit einer Gebietskörperschaft, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf eine oder mehrere kritische Anlagen ausübt. Abweichend von Satz 1 hat im Sektor Finanzwesen bestimmenden Einfluss auf eine Anlage, wer die tatsächliche Sachherrschaft ausübt. Die rechtlichen und wirtschaftlichen Umstände bleiben insoweit unberücksichtigt.	(7) Ein Betreiber kritischer Anlagen ist eine natürliche oder juristische Person oder eine rechtlich unselbstständige Organisationseinheit einer Gebietskörperschaft, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf eine oder mehrere kritische Anlagen ausübt. Abweichend von Satz 1 hat im Sektor Finanzwesen bestimmenden Einfluss auf eine Anlage, wer die tatsächliche Sachherrschaft ausübt. Die rechtlichen und wirtschaftlichen Umstände bleiben insoweit unberücksichtigt.
(8) Dieses Gesetz findet keine Anwendung auf rechtlich unselbstständige Organisationseinheiten von Gebietskörperschaften und auf juristische Personen, an denen ausschließlich Gebietskörperschaften, ausgenommen der Bund, beteiligt sind, wenn sie	(8) Dieses Gesetz findet keine Anwendung auf rechtlich unselbstständige Organisationseinheiten von Gebietskörperschaften und auf juristische Personen, an denen ausschließlich Gebietskörperschaften, ausgenommen der Bund, beteiligt sind, wenn sie
1. zu dem Zweck errichtet wurden, im öffentlichen Auftrag Leistungen für Verwaltungen zu erbringen, und	1. zu dem Zweck errichtet wurden, im öffentlichen Auftrag Leistungen für Verwaltungen zu erbringen, und

Entwurf	Beschlüsse des 4. Ausschusses
2. durch vergleichbare landesrechtliche Vorschriften unter Bezugnahme auf diesen Absatz reguliert werden.	2. durch vergleichbare landesrechtliche Vorschriften unter Bezugnahme auf diesen Absatz reguliert werden.
§ 29	§ 29
Einrichtungen der Bundesverwaltung	**Einrichtungen der Bundesverwaltung**
(1) Einrichtungen der Bundesverwaltung im Sinne dieses Gesetzes sind, mit Ausnahme der Institutionen der Sozialen Sicherung und der Bundesbank,	(1) Einrichtungen der Bundesverwaltung im Sinne dieses Gesetzes sind, mit Ausnahme der Institutionen der Sozialen Sicherung und der Deutschen Bundesbank,
1. Bundesbehörden,	1. Bundesbehörden,
2. öffentlich-rechtlich organisierte IT-Dienstleister der Bundesverwaltung sowie	2. öffentlich-rechtlich organisierte IT-Dienstleister der Bundesverwaltung sowie
3. weitere Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie ihre Vereinigungen, ungeachtet ihrer Rechtsform, auf Bundesebene, soweit durch das Bundesamt im Einvernehmen mit dem jeweils zuständigen Ressort angeordnet.	3. weitere Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie ihre Vereinigungen, ungeachtet ihrer Rechtsform, auf Bundesebene, soweit durch das Bundesamt im Einvernehmen mit dem jeweils zuständigen Ressort angeordnet.
(2) Für Einrichtungen der Bundesverwaltung sind die Regelungen für besonders wichtige Einrichtungen anzuwenden, nicht jedoch die Regelungen der §§ 38, 40 Absatz 3 und der §§ 61 und 65. Für Einrichtungen der Bundesverwaltung, ausgenommen das Bundeskanzleramt und die Bundesministerien, sind zusätzlich die Regelungen des § 30 nicht anzuwenden.	(2) Für Einrichtungen der Bundesverwaltung sind die Regelungen für besonders wichtige Einrichtungen anzuwenden, nicht jedoch die Regelungen der §§ 38, 40 Absatz 3 und der §§ 61 und 65. Für Einrichtungen der Bundesverwaltung, ausgenommen das Bundeskanzleramt und die Bundesministerien, sind zusätzlich die Regelungen des § 30 nicht anzuwenden.

Entwurf	Beschlüsse des 4. Ausschusses
(3) Die Geschäftsbereiche des Auswärtigen Amts und des Bundesministeriums der Verteidigung sowie des Bundesnachrichtendienstes und des Bundesamtes für Verfassungsschutz sind zusätzlich zu den Regelungen gemäß Absatz 2 Satz 2 von den Regelungen der § 7 Absatz 5 Satz 4, § 10, 13 Absatz 1 Nummer 1 Buchstabe e sowie der §§ 30, 33 und 35 ausgenommen. Das Auswärtige Amt erlässt im Einvernehmen mit dem Bundesministerium des Innern und für Heimat eine allgemeine Verwaltungsvorschrift, um die Ziele der NIS-2-Richtlinie im Geschäftsbereich des Auswärtigen Amts durch ergebnisäquivalente Maßnahmen umzusetzen.	(3) Die Geschäftsbereiche des Auswärtigen Amts und des Bundesministeriums der Verteidigung sowie des Bundesnachrichtendienstes und des Bundesamtes für Verfassungsschutz sind zusätzlich zu den Regelungen gemäß Absatz 2 Satz 2 von den Regelungen der § 7 Absatz 5 Satz 4, § 10, 13 Absatz 1 Nummer 1 Buchstabe e sowie der §§ 30, 33 und 35 ausgenommen. Das Auswärtige Amt erlässt im Einvernehmen mit dem Bundesministerium des Innern und für Heimat eine allgemeine Verwaltungsvorschrift, um die Ziele der NIS-2-Richtlinie im Geschäftsbereich des Auswärtigen Amts durch ergebnisäquivalente Maßnahmen umzusetzen.

Entwurf	Beschlüsse des 4. Ausschusses
Kapitel 2	Kapitel 2
Risikomanagement, Melde-, Registrierungs-, Nachweis- und Unterrichtungspflichten	Risikomanagement, Melde-, Registrierungs-, Nachweis- und Unterrichtungspflichten
§ 30	§ 30
Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	**Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen**
(1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen, die nach Absatz 2 konkretisiert werden, zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. Bei der Bewertung der Verhältnismäßigkeit der Maßnahmen nach Satz 1 sind das Ausmaß der Risikoexposition, die Größe der Einrichtung, die Umsetzungskosten und die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen. Die Einhaltung der Verpflichtung nach Satz 1 ist durch die Einrichtungen zu dokumentieren.	(1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen, die nach Absatz 2 konkretisiert werden, zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. Bei der Bewertung der Verhältnismäßigkeit der Maßnahmen nach Satz 1 sind das Ausmaß der Risikoexposition, die Größe der Einrichtung, die Umsetzungskosten und die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen. Die Einhaltung der Verpflichtung nach Satz 1 ist durch die Einrichtungen zu dokumentieren.
(2) Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen. Die Maßnahmen müssen zumindest Folgendes umfassen:	(2) Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen. Die Maßnahmen müssen zumindest Folgendes umfassen:
1. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik,	1. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik,
2. Bewältigung von Sicherheitsvorfällen,	2. Bewältigung von Sicherheitsvorfällen,

Entwurf	Beschlüsse des 4. Ausschusses
3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,	3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern,	4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern,
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,	5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik,	6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik,
7. grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Sicherheit in der Informationstechnik,	7. grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Sicherheit in der Informationstechnik,
8. Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,	8. Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,
9. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und für das Management von Anlagen,	9. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und für das Management von Anlagen,
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.	10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Entwurf	Beschlüsse des 4. Ausschusses
(3) Der von der Europäischen Kommission gemäß Artikel 21 Absatz 5 Unterabsatz 1 der NIS-2-Richtlinie erlassene Durchführungsrechtsakt zur Festlegung der technischen und methodischen Anforderungen an die in Absatz 1 genannten Maßnahmen in Bezug auf DNS-Diensteanbieter, Top Level Domain Name Registries, Cloud-Computing-Dienstleister, Anbieter von Rechenzentrumsdiensten, Betreiber von Content Delivery Networks, Managed Service Provider, Managed Security Service Provider, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter hat für die vorgenannten Einrichtungsarten Vorrang.	(3) Der von der Europäischen Kommission gemäß Artikel 21 Absatz 5 Unterabsatz 1 der NIS-2-Richtlinie erlassene Durchführungsrechtsakt zur Festlegung der technischen und methodischen Anforderungen an die in Absatz 1 genannten Maßnahmen in Bezug auf DNS-Diensteanbieter, Top Level Domain Name Registries, Cloud-Computing-Dienstleister, Anbieter von Rechenzentrumsdiensten, Betreiber von Content Delivery Networks, Managed Service Provider, Managed Security Service Provider, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter hat für die vorgenannten Einrichtungsarten Vorrang.
(4) Sofern die Europäische 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 2 genannten Maßnahmen festgelegt werden, so gehen diese Anforderungen den in Absatz 2 genannten Maßnahmen vor, soweit sie diesen entgegenstehen.	(4) Sofern die Europäische 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 2 genannten Maßnahmen festgelegt werden, so gehen diese Anforderungen den in Absatz 2 genannten Maßnahmen vor, soweit sie diesen entgegenstehen.
(5) Sofern die Durchführungsrechtsakte der Europäischen Kommission nach Artikel 21 Absatz 5 der NIS-2-Richtlinie keine abschließenden Bestimmungen über die technischen und methodischen Anforderungen sowie erforderlichenfalls über die sektoralen Anforderungen an die in Absatz 2 genannten Maßnahmen in Bezug auf besonders wichtige Einrichtungen und wichtige Einrichtungen enthalten, können diese Bestimmungen vom Bundesministerium des Innern und für Heimat im Benehmen mit den jeweils betroffenen Ressorts durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, unter Berücksichtigung der möglichen Folgen unzureichender Maßnahmen sowie der Bedeutung bestimmter Einrichtungen präzisiert und erweitert werden.	(5) Sofern die Durchführungsrechtsakte der Europäischen Kommission nach Artikel 21 Absatz 5 der NIS-2-Richtlinie keine abschließenden Bestimmungen über die technischen und methodischen Anforderungen sowie erforderlichenfalls über die sektoralen Anforderungen an die in Absatz 2 genannten Maßnahmen in Bezug auf besonders wichtige Einrichtungen und wichtige Einrichtungen enthalten, können diese Bestimmungen vom Bundesministerium des Innern und für Heimat im Benehmen mit den jeweils betroffenen Ressorts durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, unter Berücksichtigung der möglichen Folgen unzureichender Maßnahmen sowie der Bedeutung bestimmter Einrichtungen präzisiert und erweitert werden.

Entwurf	Beschlüsse des 4. Ausschusses
(6) Besonders wichtige Einrichtungen und wichtige Einrichtung dürfen durch Rechtsverordnung nach § 56 Absatz 3 bestimmte IKT-Produkte, IKT-Dienste und IKT-Prozesse nur verwenden, wenn diese über eine Cybersicherheitszertifizierung gemäß europäischer Schemata nach Artikel 49 der Verordnung (EU) 2019/881 verfügen.	(6) Besonders wichtige Einrichtungen und wichtige Einrichtung dürfen durch Rechtsverordnung nach § 56 Absatz 3 bestimmte IKT-Produkte, IKT-Dienste und IKT-Prozesse nur verwenden, wenn diese über eine Cybersicherheitszertifizierung gemäß europäischer Schemata nach Artikel 49 der Verordnung (EU) 2019/881 verfügen.
(7) 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.	(7) 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.
(8) Besonders wichtige Einrichtungen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach Absatz 1 vorschlagen. Diese vorgeschlagenen Sicherheitsstandards müssen Durchführungsrechtsakte der Europäischen Kommission so berücksichtigen, dass sie nicht im Widerspruch zu den dort genannten Anforderungen stehen sowie darin enthaltende Vorgaben nicht unterschritten werden. Das Bundesamt stellt auf Antrag fest, ob die vorgeschlagenen Sicherheitsstandards branchenspezifisch und geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten. Die Feststellung erfolgt	(8) Besonders wichtige Einrichtungen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach Absatz 1 vorschlagen. Diese vorgeschlagenen Sicherheitsstandards müssen Durchführungsrechtsakte der Europäischen Kommission so berücksichtigen, dass sie nicht im Widerspruch zu den dort genannten Anforderungen stehen sowie darin enthaltende Vorgaben nicht unterschritten werden. Das Bundesamt stellt auf Antrag fest, ob die vorgeschlagenen Sicherheitsstandards branchenspezifisch und geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten. Die Feststellung erfolgt
1. im Einvernehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe;	1. im Einvernehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe;
2. im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes.	2. im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes.
Im Sektor Gesundheitswesen ist, soweit keine zuständige Aufsichtsbehörde des Bundes besteht, abweichend von Satz 4 Nummer 2 das Benehmen mit dem Bundesministerium für Gesundheit herzustellen.	Im Sektor Gesundheitswesen ist, soweit keine zuständige Aufsichtsbehörde des Bundes besteht, abweichend von Satz 4 Nummer 2 das Benehmen mit dem Bundesministerium für Gesundheit herzustellen. Für die Feststellung werden keine Gebühren oder Auslagen für die Tätigkeit des Bundesamtes erhoben.

Entwurf	Beschlüsse des 4. Ausschusses
(9) Betreiber kritischer Anlagen können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach § 39 Absatz 1 vorschlagen. Absatz 8 Satz 2 bis 5 gelten entsprechend.	(9) Betreiber kritischer Anlagen können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen in Bezug auf kritische Anlagen nach § 30 Absatz 1 Satz 1 in Verbindung mit § 31 Absatz 1 und 2 Satz 1 vorschlagen. Absatz 8 Satz 2 bis 6 gelten entsprechend.
§ 31	§ 31
Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen	**Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen**
(1) Für Betreiber kritischer Anlagen gelten für die informationstechnischen Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Anlagen maßgeblich sind, im Vergleich zu anderen informationstechnischen Systemen, Komponenten und Prozessen besonders wichtiger Einrichtungen auch über das Schutzniveau dieser Einrichtungen hinausgehende Maßnahmen nach § 30 Absatz 1 Satz 1 als verhältnismäßig, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage steht.	(1) Für Betreiber kritischer Anlagen gelten für die informationstechnischen Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Anlagen maßgeblich sind, im Vergleich zu anderen informationstechnischen Systemen, Komponenten und Prozessen besonders wichtiger Einrichtungen auch über das Schutzniveau dieser Einrichtungen hinausgehende Maßnahmen nach § 30 Absatz 1 Satz 1 als verhältnismäßig, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage steht.
(2) 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.	(2) Betreiber kritischer Anlagen sind verpflichtet, für die informationstechnischen Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Anlagen maßgeblich sind, 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.

Entwurf	Beschlüsse des 4. Ausschusses
§ 32	§ 32
Meldepflichten	**Meldepflichten**
(1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, folgende Informationen an eine vom Bundesamt und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete gemeinsame Meldestelle zu melden:	(1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, folgende Informationen an eine vom Bundesamt und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete gemeinsame Meldestelle zu melden:
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 Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte;	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 Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte;
2. unverzüglich, spätestens jedoch innerhalb von 72 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, eine Meldung über diesen 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;	2. unverzüglich, spätestens jedoch innerhalb von 72 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall, eine Meldung über diesen 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;
3. auf Ersuchen des Bundesamtes eine Zwischenmeldung über relevante Statusaktualisierungen;	3. auf Ersuchen des Bundesamtes eine Zwischenmeldung über relevante Statusaktualisierungen;
4. spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls gemäß Nummer 2, vorbehaltlich Absatz 2, eine Abschlussmeldung, die Folgendes enthält:	4. spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls gemäß Nummer 2, vorbehaltlich Absatz 2, eine Abschlussmeldung, die Folgendes enthält:
a) eine ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen;	a) eine ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen;

Entwurf	Beschlüsse des 4. Ausschusses
b) Angaben zur Art der Bedrohung beziehungsweise ihrer zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat;	b) Angaben zur Art der Bedrohung beziehungsweise ihrer zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat;
c) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen;	c) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen;
d) gegebenenfalls die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls.	d) gegebenenfalls die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls.
Die Verpflichtung nach Satz 1 gilt frühestens ab Einrichtung des Meldewegs.	Die Verpflichtung nach Satz 1 gilt frühestens ab Einrichtung des Meldewegs.
(2) Dauert der Sicherheitsvorfall zum im Absatz 1 Nummer 4 genannten Zeitpunkt noch an, legt die betreffende Einrichtung statt einer Abschlussmeldung zu diesem Zeitpunkt eine Fortschrittsmeldung vor. Die Abschlussmeldung ist dem Bundesamt nach abschließender Bearbeitung des Sicherheitsvorfalls durch die betreffende Einrichtung vorzulegen.	(2) Dauert der Sicherheitsvorfall zum im Absatz 1 Nummer 4 genannten Zeitpunkt noch an, legt die betreffende Einrichtung statt einer Abschlussmeldung zu diesem Zeitpunkt eine Fortschrittsmeldung vor. Die Abschlussmeldung ist dem Bundesamt nach abschließender Bearbeitung des Sicherheitsvorfalls durch die betreffende Einrichtung vorzulegen.
(3) Betreiber kritischer Anlagen sind zusätzlich verpflichtet, Angaben zur Art der betroffenen Anlage und der kritischen Dienstleistung sowie zu 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.	(3) Betreiber kritischer Anlagen sind zusätzlich verpflichtet, Angaben zur Art der betroffenen Anlage und der kritischen Dienstleistung sowie zu 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.
(4) Das Bundesamt legt die Einzelheiten zur Ausgestaltung des Meldeverfahrens und zur Konkretisierung der Meldungsinhalte nach Anhörung der betroffenen Betreiber und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe fest, soweit sie möglichen Durchführungsrechtsakten der Europäischen Kommission nicht widersprechen. Die Informationen nach Satz 1 werden durch das Bundesamt auf dessen Internetseite veröffentlicht.	(4) Das Bundesamt legt die Einzelheiten zur Ausgestaltung des Meldeverfahrens und zur Konkretisierung der Meldungsinhalte nach Anhörung der betroffenen Betreiber und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe fest, soweit sie möglichen Durchführungsrechtsakten der Europäischen Kommission nicht widersprechen. Die Informationen nach Satz 1 werden durch das Bundesamt auf dessen Internetseite veröffentlicht.
(5) Das Bundesamt stellt den zuständigen Aufsichtsbehörden des Bundes unverzüglich die bei ihm eingegangenen Meldungen zur Verfügung.	(5) Das Bundesamt stellt den zuständigen Aufsichtsbehörden des Bundes unverzüglich die bei ihm eingegangenen Meldungen zur Verfügung.

Entwurf	Beschlüsse des 4. Ausschusses
(6) Das Bundesamt kann meldenden Einrichtungen nach Maßgabe des § 36 Absatz 1 Angebote zu deren Unterstützung bei der Behebung des Sicherheitsvorfalls machen.	(6) Das Bundesamt kann meldenden Einrichtungen nach Maßgabe des § 36 Absatz 1 Angebote zu deren Unterstützung bei der Behebung des Sicherheitsvorfalls machen.
§ 33	§ 33
Registrierungspflicht	**Registrierungspflicht**
(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 oder Domain-Name-Registry-Dienste anbieten, dem Bundesamt über eine gemeinsam vom Bundesamt und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete Registrierungsmöglichkeit folgenden Angaben zu übermitteln:	(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 oder Domain-Name-Registry-Dienste anbieten, dem Bundesamt über eine gemeinsam vom Bundesamt und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete Registrierungsmöglichkeit folgenden Angaben zu übermitteln:
1. Name der Einrichtung, einschließlich der Rechtsform und falls einschlägig der Handelsregisternummer,	1. Name der Einrichtung, einschließlich der Rechtsform und falls einschlägig der Handelsregisternummer,
2. Anschrift und aktuelle Kontaktdaten, einschließlich E-Mail-Adresse, öffentliche IP-Adressbereiche und Telefonnummern,	2. Anschrift und aktuelle Kontaktdaten, einschließlich E-Mail-Adresse, öffentliche IP-Adressbereiche und Telefonnummern,
3. relevanter in Anlage 1 oder 2 genannter Sektor oder, falls einschlägig, Branche,	3. relevanter in Anlage 1 oder 2 genannter Sektor oder, falls einschlägig, Branche,
4. Auflistung derjenigen Mitgliedstaaten der Europäischen Union, in denen die Einrichtung Dienste der in Anlage 1 oder 2 genannten Einrichtungsarten erbringt, und	4. Auflistung derjenigen Mitgliedstaaten der Europäischen Union, in denen die Einrichtung Dienste der in Anlage 1 oder 2 genannten Einrichtungsarten erbringt, und
5. die für die Tätigkeiten, aufgrund derer die Registrierung erfolgt, zuständigen Aufsichtsbehörden des Bundes und der Länder.	5. die für die Tätigkeiten, aufgrund derer die Registrierung erfolgt, zuständigen Aufsichtsbehörden des Bundes und der Länder.

Entwurf	Beschlüsse des 4. Ausschusses
(2) Betreiber kritischer Anlagen übermitteln mit den Angaben nach Absatz 1 die kritische Dienstleistung, die öffentlichen IP-Adressbereiche der von ihnen betriebenen Anlagen sowie die für die von ihnen betriebenen kritischen Anlagen ermittelte Anlagenkategorie und ermittelte Versorgungskennzahlen gemäß der Rechtsverordnung nach § 56 Absatz 4 sowie den Standort der Anlagen und eine Kontaktstelle. Die Betreiber stellen sicher, dass sie über ihre in Satz 1 genannte Kontaktstelle jederzeit erreichbar sind.	(2) Betreiber kritischer Anlagen übermitteln mit den Angaben nach Absatz 1 die kritische Dienstleistung, die bei ihnen zum Einsatz kommenden Typen von kritischen Komponenten, die öffentlichen IP-Adressbereiche der von ihnen betriebenen Anlagen sowie die für die von ihnen betriebenen kritischen Anlagen ermittelte Anlagenkategorie und ermittelte Versorgungskennzahlen gemäß der Rechtsverordnung nach § 56 Absatz 4 sowie den Standort der Anlagen und eine Kontaktstelle. Die Betreiber stellen sicher, dass sie über ihre in Satz 1 genannte Kontaktstelle jederzeit erreichbar sind.
(3) Die Registrierung von besonders wichtigen Einrichtungen und wichtigen Einrichtungen und Domain-Name-Registry-Diensteanbietern kann das Bundesamt im Einvernehmen mit den jeweils zuständigen Aufsichtsbehörden auch selbst vornehmen, wenn ihre Pflicht zur Registrierung nicht erfüllt wird.	(3) Die Registrierung von besonders wichtigen Einrichtungen und wichtigen Einrichtungen und Domain-Name-Registry-Diensteanbietern kann das Bundesamt im Einvernehmen mit den jeweils zuständigen Aufsichtsbehörden auch selbst vornehmen, wenn ihre Pflicht zur Registrierung nicht erfüllt wird.
(4) Rechtfertigen Tatsachen die Annahme, dass eine Einrichtung ihre Pflicht zur Registrierung nach Absatz 1 oder 2 nicht erfüllt, so hat diese Einrichtung dem Bundesamt auf Verlangen die aus Sicht des Bundesamtes für die Bewertung erforderlichen Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorzulegen und Auskunft zu erteilen, soweit nicht Geheimschutzinteressen oder überwiegende Sicherheitsinteressen entgegenstehen.	(4) Rechtfertigen Tatsachen die Annahme, dass eine Einrichtung ihre Pflicht zur Registrierung nach Absatz 1 oder 2 nicht erfüllt, so hat diese Einrichtung dem Bundesamt auf Verlangen die aus Sicht des Bundesamtes für die Bewertung erforderlichen Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorzulegen und Auskunft zu erteilen, soweit nicht Geheimschutzinteressen oder überwiegende Sicherheitsinteressen entgegenstehen.
(5) Bei Änderungen der nach Absatz 1 oder 2 zu übermittelnden Angaben sind dem Bundesamt geänderte Versorgungskennzahlen einmal jährlich zu übermitteln und alle anderen Angaben unverzüglich, spätestens jedoch zwei Wochen ab dem Zeitpunkt, zu dem die Einrichtung Kenntnis von der Änderung erhalten hat, zu übermitteln.	(5) Bei Änderungen der nach Absatz 1 oder 2 zu übermittelnden Angaben sind dem Bundesamt geänderte Versorgungskennzahlen sowie Änderungen der bei Betreibern kritischer Anlagen zum Einsatz kommenden Typen von kritischen Komponenten einmal jährlich zu übermitteln und alle anderen Angaben unverzüglich, spätestens jedoch zwei Wochen ab dem Zeitpunkt, zu dem die Einrichtung Kenntnis von der Änderung erhalten hat, zu übermitteln.

Entwurf	Beschlüsse des 4. Ausschusses
(6) Das Bundesamt legt die Einzelheiten zur Ausgestaltung des Registrierungsverfahrens im Einvernehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe fest. Die Festlegung nach Satz 1 erfolgt durch eine öffentliche Mitteilung auf der Internetseite des Bundesamtes.	(6) Das Bundesamt legt die Einzelheiten zur Ausgestaltung des Registrierungsverfahrens im Einvernehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe fest. Die Festlegung nach Satz 1 erfolgt durch eine öffentliche Mitteilung auf der Internetseite des Bundesamtes.
§ 34	§ 34
Besondere Registrierungspflicht für bestimmte Einrichtungsarten	**Besondere Registrierungspflicht für bestimmte Einrichtungsarten**
(1) Eine Einrichtung der in § 60 Absatz 1 Satz 1 genannten Einrichtungsart ist verpflichtet, spätestens drei Monate, nachdem sie als eine der vorgenannten Einrichtungen gelten, dem Bundesamt die folgenden Angaben zu übermitteln:	(1) Eine Einrichtung der in § 60 Absatz 1 Satz 1 genannten Einrichtungsart ist verpflichtet, spätestens drei Monate, nachdem sie als eine der vorgenannten Einrichtungen gelten, dem Bundesamt die folgenden Angaben zu übermitteln:
1. Name der Einrichtung;	1. Name der Einrichtung;
2. einschlägiger Sektor, Branche und Einrichtungsart wie in Anlage 1 bestimmt;	2. einschlägiger Sektor, Branche und Einrichtungsart wie in Anlage 1 bestimmt;
3. Anschrift der Hauptniederlassung in der Europäischen Union nach § 60 Absatz 2 und ihrer sonstigen Niederlassungen in der Europäischen Union oder, falls er nicht in der Europäischen Union niedergelassen ist, Anschrift seines nach § 60 Absatz 3 benannten Vertreters;	3. Anschrift der Hauptniederlassung in der Europäischen Union nach § 60 Absatz 2 und ihrer sonstigen Niederlassungen in der Europäischen Union oder, falls er nicht in der Europäischen Union niedergelassen ist, Anschrift seines nach § 60 Absatz 3 benannten Vertreters;
4. aktuelle Kontaktdaten, einschließlich E-Mail-Adressen und Telefonnummern der Einrichtung und soweit erforderlich, ihres nach § 60 Absatz 3 benannten Vertreters;	4. aktuelle Kontaktdaten, einschließlich E-Mail-Adressen und Telefonnummern der Einrichtung und soweit erforderlich, ihres nach § 60 Absatz 3 benannten Vertreters;
5. die Mitgliedstaaten der Europäischen Union, in denen die Einrichtung Dienste erbringt, und	5. die Mitgliedstaaten der Europäischen Union, in denen die Einrichtung Dienste erbringt, und
6. die öffentlichen IP-Adressbereiche der Einrichtung.	6. die öffentlichen IP-Adressbereiche der Einrichtung.

Entwurf	Beschlüsse des 4. Ausschusses
(2) Im Fall einer Änderung der gemäß Absatz 1 übermittelten Angaben unterrichten die Einrichtungen der in § 60 Absatz 1 Satz 1 genannten Einrichtungsart das Bundesamt unverzüglich über diese Änderung, jedoch spätestens innerhalb von drei Monaten ab dem Tag, an dem die Änderung eingetreten ist.	(2) Im Fall einer Änderung der gemäß Absatz 1 übermittelten Angaben unterrichten die Einrichtungen der in § 60 Absatz 1 Satz 1 genannten Einrichtungsart das Bundesamt unverzüglich über diese Änderung, jedoch spätestens innerhalb von drei Monaten ab dem Tag, an dem die Änderung eingetreten ist.
(3) Mit Ausnahme der in Absatz 1 Nummer 6 genannten Angaben leitet das Bundesamt die nach diesem § 34 übermittelten Angaben an die Agentur der Europäischen Union für Cybersicherheit weiter.	(3) Mit Ausnahme der in Absatz 1 Nummer 6 genannten Angaben leitet das Bundesamt die nach diesem § 34 übermittelten Angaben an die Agentur der Europäischen Union für Cybersicherheit weiter.
(4) Das Bundesamt kann für die Übermittlung der Angaben nach den Absätzen 1 und 2 einen geeigneten Meldeweg vorsehen.	(4) Das Bundesamt kann für die Übermittlung der Angaben nach den Absätzen 1 und 2 einen geeigneten Meldeweg vorsehen.
§ 35	§ 35
Unterrichtungspflichten	**Unterrichtungspflichten**
(1) Im Fall eines erheblichen Sicherheitsvorfalls kann das Bundesamt besonders wichtigen Einrichtungen und wichtigen Einrichtungen anordnen, die Empfänger ihrer Dienste unverzüglich über diesen erheblichen Sicherheitsvorfall zu unterrichten, der die Erbringung des jeweiligen Dienstes beeinträchtigen könnte. Das Bundesamt setzt die für die Einrichtung zuständige Aufsichtsbehörde des Bundes über Anweisungen nach Satz 1 in Kenntnis. Die Unterrichtung nach Satz 1 kann auch durch eine Veröffentlichung auf der Internetseite der Einrichtung erfolgen.	(1) Im Fall eines erheblichen Sicherheitsvorfalls kann das Bundesamt besonders wichtigen Einrichtungen und wichtigen Einrichtungen anordnen, die Empfänger ihrer Dienste unverzüglich über diesen erheblichen Sicherheitsvorfall zu unterrichten, der die Erbringung des jeweiligen Dienstes beeinträchtigen könnte. Das Bundesamt setzt die für die Einrichtung zuständige Aufsichtsbehörde des Bundes über Anweisungen nach Satz 1 in Kenntnis. Die Unterrichtung nach Satz 1 kann auch durch eine Veröffentlichung auf der Internetseite der Einrichtung erfolgen.

Entwurf	Beschlüsse des 4. Ausschusses
(2) Einrichtungen nach Absatz 1 Satz 1 aus den Sektoren Finanzwesen, Sozialversicherungsträger sowie Grundsicherung für Arbeitssuchende, digitale Infrastruktur, Verwaltung von IKT-Diensten und Digitale Dienste teilen den potenziell von einer erheblichen Cyberbedrohung betroffenen Empfängern ihrer Dienste und dem Bundesamt unverzüglich alle Maßnahmen oder Abhilfemaßnahmen mit, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können. Die Einrichtungen informieren zugleich diese Empfänger auch über die erhebliche Cyberbedrohung selbst. Die Pflichten nach Satz 1 oder 2 gelten nur dann, wenn in Abwägung der Interessen der Einrichtung und des Empfängers die Interessen des Empfängers überwiegen.	(2) Einrichtungen nach Absatz 1 Satz 1 aus den Sektoren Finanzwesen, Sozialversicherungsträger sowie Grundsicherung für Arbeitssuchende, digitale Infrastruktur, Verwaltung von IKT-Diensten und Digitale Dienste teilen den potenziell von einer erheblichen Cyberbedrohung betroffenen Empfängern ihrer Dienste und dem Bundesamt unverzüglich alle Maßnahmen oder Abhilfemaßnahmen mit, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können. Die Einrichtungen informieren zugleich diese Empfänger auch über die erhebliche Cyberbedrohung selbst. Die Pflichten nach Satz 1 oder 2 gelten nur dann, wenn in Abwägung der Interessen der Einrichtung und des Empfängers die Interessen des Empfängers überwiegen.
§ 36	§ 36
Rückmeldungen des Bundesamtes gegenüber meldenden Einrichtungen	**Rückmeldungen des Bundesamtes gegenüber meldenden Einrichtungen**
(1) Im Fall einer Meldung einer Einrichtung gemäß § 32 übermittelt das Bundesamt dieser unverzüglich und nach Möglichkeit innerhalb von 24 Stunden eine Bestätigung über den Eingang der Meldung und, auf Ersuchen der Einrichtung, Orientierungshilfen oder operative Beratung zu Abhilfemaßnahmen. Das Bundesamt kann auf Ersuchen der betreffenden Einrichtung zusätzliche technische Unterstützung leisten.	(1) Im Fall einer Meldung einer Einrichtung gemäß § 32 übermittelt das Bundesamt dieser unverzüglich und nach Möglichkeit innerhalb von 24 Stunden eine Bestätigung über den Eingang der Meldung und, auf Ersuchen der Einrichtung, Orientierungshilfen oder operative Beratung zu Abhilfemaßnahmen. Das Bundesamt kann auf Ersuchen der betreffenden Einrichtung zusätzliche technische Unterstützung leisten.
(2) Ist eine Sensibilisierung der Öffentlichkeit erforderlich, um einen erheblichen Sicherheitsvorfall zu verhindern oder zu bewältigen, oder liegt die Offenlegung des erheblichen Sicherheitsvorfalls anderweitig im öffentlichen Interesse, so kann das Bundesamt nach Anhörung der betreffenden Einrichtung diese dazu verpflichten, die Öffentlichkeit über den erheblichen Sicherheitsvorfall zu informieren. Das Bundesamt kann entsprechend der Voraussetzungen nach Satz 1 die Öffentlichkeit auch selbst informieren. Handelt es sich bei der betreffenden Einrichtung um eine Einrichtung der Bundesverwaltung, gilt für die Information der Öffentlichkeit § 4 Absatz 3 entsprechend.	(2) Ist eine Sensibilisierung der Öffentlichkeit erforderlich, um einen erheblichen Sicherheitsvorfall zu verhindern oder zu bewältigen, oder liegt die Offenlegung des erheblichen Sicherheitsvorfalls anderweitig im öffentlichen Interesse, so kann das Bundesamt nach Anhörung der betreffenden Einrichtung diese dazu verpflichten, die Öffentlichkeit über den erheblichen Sicherheitsvorfall zu informieren. Das Bundesamt kann entsprechend der Voraussetzungen nach Satz 1 die Öffentlichkeit auch selbst informieren. Handelt es sich bei der betreffenden Einrichtung um eine Einrichtung der Bundesverwaltung, gilt für die Information der Öffentlichkeit § 4 Absatz 3 entsprechend.

Entwurf	Beschlüsse des 4. Ausschusses
§ 37	§ 37
Ausnahmebescheid	**Ausnahmebescheid**
(1) Das Bundesministerium des Innern und für Heimat kann auf Vorschlag des Bundeskanzleramts, des Bundesministeriums der Justiz, des Bundesministeriums der Verteidigung, des Bundesministeriums der Finanzen, der Ministerien für Inneres und Justiz der Länder oder auf eigenes Betreiben eine besonders wichtige Einrichtung oder eine wichtige Einrichtung von Verpflichtungen nach diesem Gesetz nach Maßgabe des Absatzes 2 teilweise befreien (einfacher Ausnahmebescheid) oder nach Maßgabe des Absatzes 3 insgesamt befreien (erweiterter Ausnahmebescheid), sofern die Einrichtung Vorgaben einhält, die den Verpflichtungen nach diesem Gesetz gleichwertig sind. Die Entscheidung nach Satz 1 erfolgt mit dem jeweils zuständigen Ministerium im Einvernehmen, im Fall der Ministerien für Inneres und Justiz der Länder im Benehmen.	(1) Das Bundesministerium des Innern und für Heimat kann auf Vorschlag des Bundeskanzleramts, des Bundesministeriums der Justiz, des Bundesministeriums der Verteidigung, des Bundesministeriums der Finanzen, der Ministerien für Inneres und Justiz der Länder oder auf eigenes Betreiben eine besonders wichtige Einrichtung oder eine wichtige Einrichtung von Verpflichtungen nach diesem Gesetz nach Maßgabe des Absatzes 2 teilweise befreien (einfacher Ausnahmebescheid) oder nach Maßgabe des Absatzes 3 insgesamt befreien (erweiterter Ausnahmebescheid), sofern die Einrichtung Vorgaben einhält, die den Verpflichtungen nach diesem Gesetz gleichwertig sind. Die Entscheidung nach Satz 1 erfolgt mit dem jeweils zuständigen Ministerium im Einvernehmen, im Fall der Ministerien für Inneres und Justiz der Länder im Benehmen.
(2) Einrichtungen, die	(2) Einrichtungen, die
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	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
2. ausschließlich für Behörden, die Aufgaben in relevanten Bereichen erfüllen, tätig sind oder Dienste erbringen,	2. ausschließlich für Behörden, die Aufgaben in relevanten Bereichen erfüllen, tätig sind oder Dienste erbringen,
können für diese Tätigkeiten oder Dienste von den Risikomanagementmaßnahmen nach § 30 und den Meldepflichten nach § 32 befreit werden. Die Sicherheit in der Informationstechnik dieser Einrichtungen muss in diesen Fällen anderweitig gewährleistet sein und beaufsichtigt werden.	können für diese Tätigkeiten oder Dienste von den Risikomanagementmaßnahmen nach § 30 und den Meldepflichten nach § 32 befreit werden. Die Sicherheit in der Informationstechnik dieser Einrichtungen muss in diesen Fällen anderweitig gewährleistet sein und beaufsichtigt werden.

Entwurf	Beschlüsse des 4. Ausschusses
(3) Einrichtungen, die ausschließlich in relevanten Bereichen tätig sind oder Dienste erbringen, können insgesamt von den in Absatz 2 genannten Pflichten und von den Registrierungspflichten nach § 33 und § 34 befreit werden. Absatz 2 Satz 2 gilt entsprechend.	(3) Einrichtungen, die ausschließlich in relevanten Bereichen tätig sind oder Dienste erbringen, können insgesamt von den in Absatz 2 genannten Pflichten und von den Registrierungspflichten nach § 33 und § 34 befreit werden. Absatz 2 Satz 2 gilt entsprechend.
(4) Die Absätze 1 bis 3 gelten nicht, wenn die betreffende Einrichtung ein Vertrauensdiensteanbieter ist.	(4) Die Absätze 1 bis 3 gelten nicht, wenn die betreffende Einrichtung ein Vertrauensdiensteanbieter ist.
(5) Ein Ausnahmebescheid nach diesem Gesetz ist zu widerrufen, wenn nachträglich Tatsachen eintreten, die zur Ablehnung einer Erteilung einer Ausnahme hätten führen müssen. Abweichend von Satz 1 kann im Falle eines vorübergehenden Wegfalls der Voraussetzungen des Absatzes 2 Nummer 1 oder 2 von einem Widerruf abgesehen werden.	(5) Ein Ausnahmebescheid nach diesem Gesetz ist zu widerrufen, wenn nachträglich Tatsachen eintreten, die zur Ablehnung einer Erteilung einer Ausnahme hätten führen müssen. Abweichend von Satz 1 kann im Falle eines vorübergehenden Wegfalls der Voraussetzungen des Absatzes 2 Nummer 1 oder 2 von einem Widerruf abgesehen werden.
§ 38	§ 38
Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	**Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen**
(1) Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen.	(1) Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen.
(2) Geschäftsleitungen, die ihre Pflichten nach Absatz 1 verletzen, haften ihrer Einrichtung für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Einrichtung anwendbaren Regeln des Gesellschaftsrechts. Nach diesem Gesetz haften sie nur, wenn die für die Einrichtung maßgeblichen gesellschaftsrechtlichen Bestimmungen keine Haftungsregelung nach Satz 1 enthalten.	(2) Geschäftsleitungen, die ihre Pflichten nach Absatz 1 verletzen, haften ihrer Einrichtung für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Einrichtung anwendbaren Regeln des Gesellschaftsrechts. Nach diesem Gesetz haften sie nur, wenn die für die Einrichtung maßgeblichen gesellschaftsrechtlichen Bestimmungen keine Haftungsregelung nach Satz 1 enthalten.

Entwurf	Beschlüsse des 4. Ausschusses
(3) Die Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.	(3) Die Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.
§ 39	§ 39
Nachweispflichten für Betreiber kritischer Anlagen	**Nachweispflichten für Betreiber kritischer Anlagen**
(1) Betreiber kritischer Anlagen haben die Umsetzung der Maßnahmen nach § 30 Absatz 1 Satz 1 in Verbindung mit § 31 Absatz 1 und 2 Satz 1 zu einem vom Bundesamt im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe festgelegten Zeitpunkt, frühestens drei Jahre nachdem sie erstmals oder spätestens drei Jahre nachdem sie erneut als ein Betreiber einer kritischen Anlage gelten, und anschließend alle drei Jahre dem Bundesamt durch Sicherheitsaudits, Prüfungen oder Zertifizierungen nachzuweisen. Die Betreiber übermitteln dem Bundesamt die Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich Angaben über die 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 Sicherheitsmängel verlangen. Das Bundesamt kann die Vorlage eines geeigneten Nachweises über die erfolgte Mängelbeseitigung verlangen.	(1) Betreiber kritischer Anlagen haben die Umsetzung der Maßnahmen in Bezug auf kritische Anlagen nach § 30 Absatz 1 Satz 1 in Verbindung mit § 31 Absatz 1 und 2 Satz 1 zu einem vom Bundesamt im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe festgelegten Zeitpunkt, frühestens drei Jahre nachdem sie erstmals oder spätestens drei Jahre nachdem sie erneut als ein Betreiber einer kritischen Anlage gelten, und anschließend alle drei Jahre dem Bundesamt durch Sicherheitsaudits, Prüfungen oder Zertifizierungen nachzuweisen. Die Betreiber übermitteln dem Bundesamt die Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich Angaben über die 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 Sicherheitsmängel verlangen. Das Bundesamt kann die Vorlage eines geeigneten Nachweises über die erfolgte Mängelbeseitigung verlangen.

Entwurf	Beschlüsse des 4. Ausschusses
(2) Das Bundesamt kann zur Ausgestaltung des Verfahrens der Prüfungen und Erbringung der Nachweise nach Absatz 1 folgende Anforderungen festlegen:	(2) Das Bundesamt kann zur Ausgestaltung des Verfahrens der Prüfungen und Erbringung der Nachweise nach Absatz 1 folgende Anforderungen festlegen:
1. Anforderungen an die Art und Weise der Durchführung,	1. Anforderungen an die Art und Weise der Durchführung,
2. Anforderungen an die Geeignetheit der zu erbringenden Nachweise sowie	2. Anforderungen an die Geeignetheit der zu erbringenden Nachweise sowie
3. nach Anhörung der betroffenen Betreiber und Einrichtungen und der betroffenen Wirtschaftsverbände fachliche und organisatorische Anforderungen an die prüfenden Stellen im Einvernehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.	3. nach Anhörung der betroffenen Betreiber und Einrichtungen und der betroffenen Wirtschaftsverbände fachliche und organisatorische Anforderungen an die prüfenden Stellen im Einvernehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe.
Die Festlegung nach Satz 1 erfolgt durch eine öffentliche Mitteilung auf der Internetseite des Bundesamtes.	Die Festlegung nach Satz 1 erfolgt durch eine öffentliche Mitteilung auf der Internetseite des Bundesamtes.
(3) Abweichend von Absatz 1 Satz 1 legt das Bundesamt für Betreiber kritischer Anlagen, die bis zum Inkrafttreten dieses Gesetzes Betreiber Kritischer Infrastrukturen waren nach § 2 Absatz 10 des BSI-Gesetzes 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, den Zeitpunkt der Nachweiserbringung auf frühestens drei Jahre nach Erbringung des letzten Nachweises nach § 8a Absatz 3 des BSI-Gesetzes 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, fest.	(3) Abweichend von Absatz 1 Satz 1 legt das Bundesamt für Betreiber kritischer Anlagen, die bis zum Inkrafttreten dieses Gesetzes Betreiber Kritischer Infrastrukturen waren nach § 2 Absatz 10 des BSI-Gesetzes 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, den Zeitpunkt der Nachweiserbringung auf frühestens drei Jahre nach Erbringung des letzten Nachweises nach § 8a Absatz 3 des BSI-Gesetzes 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, fest.

Entwurf	Beschlüsse des 4. Ausschusses
§ 40	§ 40
Nationale Verbindungsstelle sowie zentrale Melde- und Anlaufstelle für besonders wichtige und wichtige Einrichtungen	**Nationale Verbindungsstelle sowie zentrale Melde- und Anlaufstelle für besonders wichtige und wichtige Einrichtungen**
(1) Das Bundesamt ist die nationale Verbindungsstelle sowie die zentrale Melde- und Anlaufstelle für die Aufsicht für besonders wichtige Einrichtungen und wichtige Einrichtungen in der Sicherheit in der Informationstechnik.	(1) Das Bundesamt ist die nationale Verbindungsstelle sowie die zentrale Melde- und Anlaufstelle für die Aufsicht für besonders wichtige Einrichtungen und wichtige Einrichtungen in der Sicherheit in der Informationstechnik.
(2) Zur Wahrnehmung seiner Aufgabe als nationale Verbindungsstelle koordiniert das Bundesamt	(2) Zur Wahrnehmung seiner Aufgabe als nationale Verbindungsstelle koordiniert das Bundesamt
1. die grenzüberschreitende Zusammenarbeit der Länderbehörden, die die Länder als zuständige Behörden für die Aufsicht von Einrichtungen der öffentlichen Verwaltung auf regionaler Ebene nach Artikel 2 Absatz 2 Buchstabe f Nummer ii der NIS-2-Richtlinie bestimmt haben, sowie der Bundesnetzagentur und der 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 Agentur der Europäischen Union für Cybersicherheit sowie	1. die grenzüberschreitende Zusammenarbeit der Länderbehörden, die die Länder als zuständige Behörden für die Aufsicht von Einrichtungen der öffentlichen Verwaltung auf regionaler Ebene nach Artikel 2 Absatz 2 Buchstabe f Nummer ii der NIS-2-Richtlinie bestimmt haben, sowie der Bundesnetzagentur und der 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 Agentur der Europäischen Union für Cybersicherheit sowie
2. die sektorübergreifende Zusammenarbeit der in Nummer 1 genannten Länderbehörden, des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe, der Bundesnetzagentur und der Bundesanstalt für Finanzdienstleistungsaufsicht.	2. die sektorübergreifende Zusammenarbeit der in Nummer 1 genannten Länderbehörden, des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe, der Bundesnetzagentur und der Bundesanstalt für Finanzdienstleistungsaufsicht.
(3) Zur Wahrnehmung seiner Aufgabe als zentrale Meldestelle hat das Bundesamt	(3) Zur Wahrnehmung seiner Aufgabe als zentrale Meldestelle hat das Bundesamt
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 und zu Angriffen,	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 und zu Angriffen,

Entwurf	Beschlüsse des 4. Ausschusses
2. die Relevanz dieser Informationen nach Nummer 1 für die Verfügbarkeit kritischer Dienstleistungen in Zusammenarbeit mit den zuständigen Aufsichtsbehörden und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe zu analysieren,	2. die Relevanz dieser Informationen nach Nummer 1 für die Verfügbarkeit kritischer Dienstleistungen in Zusammenarbeit mit den zuständigen Aufsichtsbehörden und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe zu analysieren,
3. das Lagebild bezüglich der Sicherheit in der Informationstechnik von kritischen Anlagen, besonders wichtigen Einrichtungen und wichtigen Einrichtungen kontinuierlich zu aktualisieren und	3. das Lagebild bezüglich der Sicherheit in der Informationstechnik von kritischen Anlagen, besonders wichtigen Einrichtungen und wichtigen Einrichtungen kontinuierlich zu aktualisieren und
4. unverzüglich	4. unverzüglich
a) die Betreiber kritischer Anlagen über sie betreffende Informationen nach den Nummern 1 bis 3 nach § 33 Absatz 1 Nummer 2 zu unterrichten und	a) die Betreiber kritischer Anlagen über sie betreffende Informationen nach den Nummern 1 bis 3 nach § 33 Absatz 1 Nummer 2 zu unterrichten und
b) die zuständigen Behörden eines anderen Mitgliedstaats der Europäischen Union über nach Absatz 5 oder nach vergleichbaren Regelungen gemeldete erhebliche Störungen, die Auswirkungen in diesem Mitgliedstaat haben, unter Berücksichtigung der Interessen nationaler Sicherheit und Verteidigung zu unterrichten und	b) die zuständigen Behörden eines anderen Mitgliedstaats der Europäischen Union über nach Absatz 5 oder nach vergleichbaren Regelungen gemeldete erhebliche Störungen, die Auswirkungen in diesem Mitgliedstaat haben, unter Berücksichtigung der Interessen nationaler Sicherheit und Verteidigung zu unterrichten und
c) das Auswärtige Amt über nach § 32 Absatz 1 gemeldete erhebliche Sicherheitsvorfälle mit internationalem Bezug, zu unterrichten und	c) das Auswärtige Amt über nach § 32 Absatz 1 gemeldete erhebliche Sicherheitsvorfälle mit internationalem Bezug, zu unterrichten und
d) im Rahmen vorab zwischen dem Bundesamt und den Empfängern abgestimmter Prozesse zur Weitergabe und Wahrung der notwendigen Vertraulichkeit die zu diesem Zweck dem Bundesamt von den Ländern als zentrale Kontaktstellen benannten Behörden oder die zuständigen Behörden des Bundes über die zur Erfüllung ihrer Aufgaben erforderlichen Informationen zu unterrichten.	d) im Rahmen vorab zwischen dem Bundesamt und den Empfängern abgestimmter Prozesse zur Weitergabe und Wahrung der notwendigen Vertraulichkeit die zu diesem Zweck dem Bundesamt von den Ländern als zentrale Kontaktstellen benannten Behörden oder die zuständigen Behörden des Bundes über die zur Erfüllung ihrer Aufgaben erforderlichen Informationen zu unterrichten.
(4) Zur Wahrnehmung seiner Aufgabe als zentrale Anlaufstelle hat das Bundesamt	(4) Zur Wahrnehmung seiner Aufgabe als zentrale Anlaufstelle hat das Bundesamt

Entwurf	Beschlüsse des 4. Ausschusses
1. Anfragen der in Absatz 2 genannten Stellen anzunehmen und an die zuständigen in Absatz 2 genannten Stellen weiterzuleiten,	1. Anfragen der in Absatz 2 genannten Stellen anzunehmen und an die zuständigen in Absatz 2 genannten Stellen weiterzuleiten,
2. Antworten auf die in Absatz 2 Nummer 2 genannten Anfragen zu erstellen und dabei die in Absatz 1 genannten Stellen zu beteiligen oder Antworten der in Absatz 2 genannten Stellen an die in Absatz 2 genannten Stellen weiterzuleiten, nach § 32 eingegangene Meldungen an zentrale Anlaufstellen der anderen betroffenen Mitgliedstaaten der Europäischen Union weiterzuleiten,	2. Antworten auf die in Absatz 2 Nummer 2 genannten Anfragen zu erstellen und dabei die in Absatz 1 genannten Stellen zu beteiligen oder Antworten der in Absatz 2 genannten Stellen an die in Absatz 2 genannten Stellen weiterzuleiten, nach § 32 eingegangene Meldungen an zentrale Anlaufstellen der anderen betroffenen Mitgliedstaaten der Europäischen Union weiterzuleiten,
3. wenn ein erheblicher Sicherheitsvorfall zwei oder mehr Mitgliedstaaten der Europäischen Union betrifft, die anderen betroffenen Mitgliedstaaten und die Agentur der Europäischen Union für Cybersicherheit über den erheblichen Sicherheitsvorfall zu unterrichten, wobei die Art der gemäß § 32 Absatz 2 erhaltenen Informationen mitzuteilen und das wirtschaftliche Interesse der Einrichtung sowie die Vertraulichkeit der bereitgestellten Informationen zu wahren ist.	3. wenn ein erheblicher Sicherheitsvorfall zwei oder mehr Mitgliedstaaten der Europäischen Union betrifft, die anderen betroffenen Mitgliedstaaten und die Agentur der Europäischen Union für Cybersicherheit über den erheblichen Sicherheitsvorfall zu unterrichten, wobei die Art der gemäß § 32 Absatz 2 erhaltenen Informationen mitzuteilen und das wirtschaftliche Interesse der Einrichtung sowie die Vertraulichkeit der bereitgestellten Informationen zu wahren ist.
(5) Während eines erheblichen Sicherheitsvorfalls gemäß § 32 Absatz 1 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 eines erheblichen Sicherheitsvorfalls erforderlich ist.	(5) Während eines erheblichen Sicherheitsvorfalls gemäß § 32 Absatz 1 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 eines erheblichen Sicherheitsvorfalls erforderlich ist.
(6) Soweit im Rahmen dieser Vorschrift personenbezogene Daten verarbeitet werden, ist eine über die vorstehenden Absätze hinausgehende Verarbeitung zu anderen Zwecken unzulässig. § 8 Absatz 8 Satz 3 bis 9 ist entsprechend anzuwenden.	(6) Soweit im Rahmen dieser Vorschrift personenbezogene Daten verarbeitet werden, ist eine über die vorstehenden Absätze hinausgehende Verarbeitung zu anderen Zwecken unzulässig. § 8 Absatz 8 Satz 3 bis 9 ist entsprechend anzuwenden.

Entwurf	Beschlüsse des 4. Ausschusses
§ 41	§ 41
Untersagung des Einsatzes kritischer Komponenten	**Untersagung des Einsatzes kritischer Komponenten**
(1) Ein Betreiber kritischer Anlagen hat den geplanten erstmaligen Einsatz einer kritischen Komponente gemäß § 2 Nummer 23 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 der Einsatz nicht untersagt wurde.	(1) Das Bundesministerium des Innern und für Heimat kann gegenüber dem Betreiber kritischer Anlagen den Einsatz von kritischen Komponenten eines Herstellers im Benehmen mit dem Bundesministerium für Wirtschaft und Klimaschutz in den Sektoren Energie und Welt-raum, dem Bundesministerium für Digitales und Verkehr in den Sektoren Informations-technik und Telekommunikation sowie Transport und Verkehr, dem Bundesministerium für Gesundheit im Sektor Gesundheit, dem Bundesministerium für Ernährung und Landwirtschaft im Sektor Ernährung, dem Bundesministerium der Finanzen im Sektor Finanzwesen, dem Bundesministerium für Arbeit und Soziales im Sektor Sozialversicherungsträger sowie Grundsicherung für Arbeitssuchende und dem Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz in den Sektoren Wasser sowie Siedlungsabfallentsorgung, sowie dem Auswärtigen Amt untersagen oder Anordnungen erlassen, wenn der Einsatz die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigen.
(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 § 56 Absatz 4 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) Hat das Bundesministerium des Innern und für Heimat einem Betreiber kritischer Anlagen den Einsatz einer kritischen Komponente untersagt oder eine An-ordnung erlassen, kann das Bundesministerium des Innern und für Heimat im Benehmen mit dem in Absatz 1 genannten Bundesministerium

Entwurf	Beschlüsse des 4. Ausschusses
1. der Hersteller unmittelbar oder mittelbar von der Regierung, einschließlich sonstiger staatlicher Stellen oder Streitkräfte, eines Drittstaates kontrolliert wird,	1. dem Betreiber kritischer Anlagen auch den zukünftigen Einsatz weiterer kritischer Komponenten desselben Herstellers und desselben Komponententyps untersagen oder Anordnungen erlassen,
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	2. allen Betreibern kritischer Anlagen den Einsatz derselben kritischen Komponente desselben Herstellers sowie von weiteren kritischen Komponenten desselben Komponententyps desselben Herstellers untersagen oder Anordnungen erlassen.
3. der Einsatz der kritischen Komponente im Einklang mit den sicherheitspolitischen Zielen der Bundesrepublik Deutschland, der Europäischen Union oder des Nordatlantikvertrages steht.	
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.	Die Entscheidung nach Absatz 2 Nr. 2 ergeht als Allgemeinverfügung.

Entwurf	Beschlüsse des 4. Ausschusses
(3) Kritische Komponenten gemäß § 2 Nummer 23 dürfen nur eingesetzt werden, wenn der Hersteller eine Erklärung über seine Vertrauenswürdigkeit (Garantieerklärung) gegenüber dem Betreiber der kritischen Anlage abgegeben 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 Zweck von Sabotage, Spionage oder Terrorismus, auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der kritischen Anlage einwirken zu können. Das Bundesministerium des Innern und für Heimat legt die Einzelheiten der Mindestanforderungen an die Garantieerklärung im Einvernehmen mit den in § 56 Absatz 4 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 und Funktionsfähigkeit der kritischen Anlage 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 aus dessen Organisationsstruktur, stammen. Die Sätze 1 und 2 gelten erst ab der Bekanntmachung der Allgemeinverfügung nach Satz 4 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.	(3) Widerspruch und Klage gegen eine Untersagung oder Anordnung nach Absatz 1 und 2 haben keine aufschiebende Wirkung.

Entwurf	Beschlüsse des 4. Ausschusses
(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 § 56 Absatz 4 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) Bei der Prüfung einer voraussichtlichen Beeinträchtigung der öffentlichen Ordnung oder Sicherheit nach Absatz 1 kann insbesondere berücksichtigt werden, ob
	1. der Hersteller unmittelbar oder mittelbar von der Regierung, einschließlich sonstiger staatlicher Stellen oder Streitkräfte, eines Drittstaates kontrolliert wird oder zur Zusammenarbeit mit staatlichen Stellen oder Streitkräften eines Drittstaates verpflichtet ist oder von dem Drittstaat hierzu verpflichtet werden kann,
	2. der Hersteller an Aktivitäten beteiligt war oder ist, die geeignet waren oder sind, 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 zu haben,
	3. hinreichende Anhaltspunkte dafür bestehen, dass der Hersteller aus sonstigen Gründen nicht vertrauenswürdig ist,
	4. der Einsatz der kritischen Komponente im Einklang mit den sicherheitspolitischen Interessen der Bundesrepublik Deutschland, der Europäischen Union oder des Nordatlantikvertrages steht.
(5) Ein Hersteller einer kritischen Komponente kann insbesondere dann nicht vertrauenswürdig sein, wenn hinreichende Anhaltspunkte dafür bestehen, dass	(5) Der Betreiber kritischer Anlagen ist zur Mitwirkung bei der Ermittlung des Sachverhalts verpflichtet. Dafür hat er alle für das Verfahren erheblichen Tatsachen vollständig und wahrheitsgemäß offenzulegen und die ihm bekannten Beweismittel anzugeben.

Entwurf	Beschlüsse des 4. Ausschusses
1. er gegen die in der Garantieerklärung eingegangen Verpflichtungen verstoßen hat,	
2. in der Garantieerklärung angegebene Tatsachenbehauptungen unwahr sind,	
3. er Sicherheitsüberprüfungen und Penetrationsanalysen an seinem Produkt und in der Produktionsumgebung nicht im erforderlichen Umfang in angemessener Weise unterstützt,	
4. Schwachstellen oder Manipulationen an seinem Produkt nicht unverzüglich, nachdem er davon Kenntnis erlangt, beseitigt und dem Betreiber kritischer Anlagen meldet,	
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 Anlage einwirken zu können, oder	
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 Anlage einwirken zu können.	
(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 § 56 Absatz 4 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt	
1. den geplanten Einsatz weiterer kritischer Komponenten desselben Typs und desselben Herstellers untersagen und	
2. den weiteren Einsatz kritischer Komponenten desselben Typs und desselben Herstellers unter Einräumung einer angemessenen Frist untersagen.	

Entwurf	Beschlüsse des 4. Ausschusses
(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 § 56 Absatz 4 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt untersagen.	
§ 42	§ 42
Auskunftsverlangen	**Auskunftsverlangen**
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.	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.
Kapitel 3	Kapitel 3
Informationssicherheit der Einrichtungen der Bundesverwaltung	Informationssicherheit der Einrichtungen der Bundesverwaltung
§ 43	§ 43
Informationssicherheitsmanagement	**Informationssicherheitsmanagement**
(1) Die Leitung der Einrichtung der Bundesverwaltung ist dafür verantwortlich, unter Berücksichtigung der Belange des IT-Betriebs die Voraussetzungen zur Gewährleistung der Informationssicherheit zu schaffen.	(1) Die Leitung der Einrichtung der Bundesverwaltung ist dafür verantwortlich, unter Berücksichtigung der Belange des IT-Betriebs die Voraussetzungen zur Gewährleistung der Informationssicherheit zu schaffen.
(2) Die Leitung der Einrichtung der Bundesverwaltung muss regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Informationssicherheit zu erlangen sowie die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.	(2) Die Leitung der Einrichtung der Bundesverwaltung muss regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Informationssicherheit zu erlangen sowie die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.

Entwurf	Beschlüsse des 4. Ausschusses
(3) Soweit öffentlich-rechtlich oder privatrechtlich organisierte Stellen mit Leistungen für Informationstechnik des Bundes beauftragt werden, ist vertraglich sicherzustellen, dass sie 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 Leitung der Einrichtung der Bundesverwaltung nach Absatz 1 bleiben hiervon unberührt.	(3) Soweit öffentlich-rechtlich oder privatrechtlich organisierte Stellen mit Leistungen für Informationstechnik des Bundes beauftragt werden, ist vertraglich sicherzustellen, dass sie 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 Leitung der Einrichtung der Bundesverwaltung nach Absatz 1 bleiben hiervon unberührt.
(4) Die Registrierung von Einrichtungen der Bundesverwaltung nach § 33 obliegt der Leitung der Einrichtung der Bundesverwaltung. Die Einrichtungen der Bundesverwaltung weisen dem Bundesamt die Erfüllung der Anforderungen nach Absatz 1 spätestens fünf Jahre nach Inkrafttreten dieses Gesetzes und anschließend regelmäßig nach seinen Vorgaben nach.	(4) Die Registrierung von Einrichtungen der Bundesverwaltung nach § 33 obliegt der Leitung der Einrichtung der Bundesverwaltung. Die Einrichtungen der Bundesverwaltung weisen dem Bundesamt die Erfüllung der Anforderungen nach Absatz 1 spätestens fünf Jahre nach Inkrafttreten dieses Gesetzes und anschließend regelmäßig nach seinen Vorgaben nach.
(5) Werden, über die sich aus § 32 ergebenden Meldepflichten hinaus, Einrichtungen der Bundesverwaltung Informationen nach § 4 Absatz 2 Nummer 1 bekannt, die für die Erfüllung von Aufgaben oder für die Sicherheit der Kommunikationstechnik des Bundes von Bedeutung sind, unterrichten die Einrichtungen der Bundesverwaltung das Bundesamt hierüber unverzüglich, soweit andere Vorschriften dem nicht entgegenstehen. Ausgenommen von den Meldepflichten für Einrichtungen der Bundesverwaltung nach § 32 sowie nach Satz 1 dieses Absatzes 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. Ausgenommen von der Pflicht nach Absatz 5 Satz 3 sind der Bundesnachrichtendienst und das Bundesamt für Verfassungsschutz.	(5) Werden, über die sich aus § 32 ergebenden Meldepflichten hinaus, Einrichtungen der Bundesverwaltung Informationen nach § 4 Absatz 2 Nummer 1 bekannt, die für die Erfüllung von Aufgaben oder für die Sicherheit der Kommunikationstechnik des Bundes von Bedeutung sind, unterrichten die Einrichtungen der Bundesverwaltung das Bundesamt hierüber unverzüglich, soweit andere Vorschriften dem nicht entgegenstehen. Ausgenommen von den Meldepflichten für Einrichtungen der Bundesverwaltung nach § 32 sowie nach Satz 1 dieses Absatzes 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. Ausgenommen von der Pflicht nach Absatz 5 Satz 3 sind der Bundesnachrichtendienst und das Bundesamt für Verfassungsschutz.

Entwurf	Beschlüsse des 4. Ausschusses
(6) Das Bundesministerium des Innern und für Heimat erlässt im Einvernehmen mit den Ressorts allgemeine Verwaltungsvorschriften zur Durchführung des Absatzes 5.	(6) Das Bundesministerium des Innern und für Heimat erlässt im Einvernehmen mit den Ressorts allgemeine Verwaltungsvorschriften zur Durchführung des Absatzes 5. (7) Werden, über die sich aus § 32 ergebenden Meldepflichten hinaus, Einrichtungen der Bundesverwaltung Informationen nach § 4 Absatz 2 Nummer 1 bekannt, unterrichten die Einrichtungen der Bundesverwaltung das Bundesamt hierüber unverzüglich, soweit andere gesetzliche Regelungen dem nicht entgegenstehen.
§ 44	§ 44
Vorgaben des Bundesamtes	**Vorgaben des Bundesamtes**
(1) Die Einrichtungen der Bundesverwaltung müssen die jeweils geltenden Fassungen der Mindeststandards für die Sicherheit in der Informationstechnik des Bundes (Mindeststandards) als Mindestanforderungen zum Schutz der in der Bundesverwaltung verarbeiteten Informationen erfüllen. Die Mindeststandards werden vom Bundesamt im Benehmen mit den Ressorts und weiteren obersten Bundesbehörden festgelegt und auf der Internetseite des Bundesamtes veröffentlicht. Abweichungen von den Mindeststandards sind nur in sachlich gerechtfertigten Fällen zulässig, sie sind zu dokumentieren und zu begründen. Für die in § 2 Nummer 21 genannten Gerichte und Verfassungsorgane haben die Vorschriften nach Satz 1 empfehlenden Charakter. Für die Verpflichtung nach Satz 1 gelten die Ausnahmen nach § 7 Absatz 6 und 7 entsprechend.	(1) Die Einrichtungen der Bundesverwaltung müssen die jeweils geltenden Fassungen der Mindeststandards für die Sicherheit in der Informationstechnik des Bundes (Mindeststandards) als Mindestanforderungen zum Schutz der in der Bundesverwaltung verarbeiteten Informationen erfüllen. Die Mindeststandards werden vom Bundesamt im Benehmen mit den Ressorts und weiteren obersten Bundesbehörden festgelegt und auf der Internetseite des Bundesamtes veröffentlicht. Abweichungen von den Mindeststandards sind nur in sachlich gerechtfertigten Fällen zulässig, sie sind zu dokumentieren und zu begründen. Für die in § 2 Nummer 21 genannten Gerichte und Verfassungsorgane haben die Vorschriften nach Satz 1 empfehlenden Charakter. Für die Verpflichtung nach Satz 1 gelten die Ausnahmen nach § 7 Absatz 6 und 7 entsprechend.

Entwurf	Beschlüsse des 4. Ausschusses
(2) Das Bundeskanzleramt und die Bundesministerien müssen als zusätzliche Mindestanforderungen die BSI-Standards und das IT-Grundschutz-Kompendium des Bundesamtes (IT-Grundschutz) in den jeweils geltenden Fassungen einhalten. Die jeweils geltenden Fassungen werden auf der Internetseite des Bundesamtes veröffentlicht. Der IT-Grundschutz wird durch das Bundesamt regelmäßig evaluiert und entsprechend dem Stand der Technik sowie unter Berücksichtigung der Erfahrungen aus der Praxis und aus der Beratung und Unterstützung nach Absatz 4 fortentwickelt; dabei wird der Umsetzungsaufwand soweit möglich minimiert. Das Bundesamt wird den IT-Grundschutz bis zum 1. Januar 2026 modernisieren und fortentwickeln. Für die Verpflichtung nach Satz 1 gelten die Ausnahmen nach § 7 Absatz 6 und 7 entsprechend.	(2) Das Bundeskanzleramt und die Bundesministerien müssen als zusätzliche Mindestanforderungen die BSI-Standards und das IT-Grundschutz-Kompendium des Bundesamtes (IT-Grundschutz) in den jeweils geltenden Fassungen einhalten. Die jeweils geltenden Fassungen werden auf der Internetseite des Bundesamtes veröffentlicht. Der IT-Grundschutz wird durch das Bundesamt regelmäßig evaluiert und entsprechend dem Stand der Technik sowie unter Berücksichtigung der Erfahrungen aus der Praxis und aus der Beratung und Unterstützung nach Absatz 4 fortentwickelt; dabei wird der Umsetzungsaufwand soweit möglich minimiert. Das Bundesamt wird den IT-Grundschutz bis zum 1. Januar 2026 modernisieren und fortentwickeln. Für die Verpflichtung nach Satz 1 gelten die Ausnahmen nach § 7 Absatz 6 und 7 entsprechend.
(3) Durch die Umsetzung der Mindestanforderungen nach Absatz 1 Satz 1 und Absatz 2 Satz 1ist die Erfüllung der Vorgaben nach § 30 gewährleistet, soweit nicht die Europäische Kommission einen Durchführungsrechtsakt gemäß Artikel 21 Absatz 5 Unterabsatz 2 der NIS-2-Richtlinie erlässt, in dem die technischen und methodischen Anforderungen über die Mindestanforderungen aus Absatz 1 Satz 1 und Absatz 2 Satz 1 hinausgehen. Falls eine Einrichtung des Bundes gleichzeitig ein Betreiber kritischer Anlagen ist und die Anforderungen des IT-Grundschutzes und der Mindeststandards den Anforderungen nach § 30 Absatz 9 und § 31 widersprechen, genießen letztere Vorrang.	(3) Durch die Umsetzung der Mindestanforderungen nach Absatz 1 Satz 1 und Absatz 2 Satz 1ist die Erfüllung der Vorgaben nach § 30 gewährleistet, soweit nicht die Europäische Kommission einen Durchführungsrechtsakt gemäß Artikel 21 Absatz 5 Unterabsatz 2 der NIS-2-Richtlinie erlässt, in dem die technischen und methodischen Anforderungen über die Mindestanforderungen aus Absatz 1 Satz 1 und Absatz 2 Satz 1 hinausgehen. Falls eine Einrichtung des Bundes gleichzeitig ein Betreiber kritischer Anlagen ist und die Anforderungen des IT-Grundschutzes und der Mindeststandards den Anforderungen nach § 30 Absatz 9 und § 31 widersprechen, genießen letztere Vorrang.
(4) Das Bundesamt berät die Einrichtungen der Bundesverwaltung auf Ersuchen bei der Umsetzung und Einhaltung der Mindestanforderungen nach Absatz 1 Satz 1 und Absatz 2 Satz 1, stellt Hilfsmittel zur Verfügung und unterstützt die Bereitstellung entsprechender Lösungen durch die IT-Dienstleister des Bundes über den gesamten Lebenszyklus.	(4) Das Bundesamt berät die Einrichtungen der Bundesverwaltung auf Ersuchen bei der Umsetzung und Einhaltung der Mindestanforderungen nach Absatz 1 Satz 1 und Absatz 2 Satz 1, stellt Hilfsmittel zur Verfügung und unterstützt die Bereitstellung entsprechender Lösungen durch die IT-Dienstleister des Bundes über den gesamten Lebenszyklus.

Entwurf	Beschlüsse des 4. Ausschusses
(5) Das Bundesamt stellt im Rahmen seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 10 technische Richtlinien und Referenzarchitekturen bereit, die von den Einrichtungen der Bundesverwaltung als Rahmen für die Entwicklung sachgerechter Anforderungen an Auftragnehmer – im Sinne einer Eignung – und IT-Produkte – im Sinne einer Spezifikation – für die Durchführung von Vergabeverfahren berücksichtigt werden. Die Vorschriften des Vergaberechts und des Geheimschutzes bleiben unberührt.	(5) Das Bundesamt stellt im Rahmen seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 10 technische Richtlinien und Referenzarchitekturen bereit, die von den Einrichtungen der Bundesverwaltung als Rahmen für die Entwicklung sachgerechter Anforderungen an Auftragnehmer – im Sinne einer Eignung – und IT-Produkte – im Sinne einer Spezifikation – für die Durchführung von Vergabeverfahren berücksichtigt werden. Die Vorschriften des Vergaberechts und des Geheimschutzes bleiben unberührt.
(6) Für die Einrichtungen der Bundesverwaltung kann das Bundesministerium des Innern und für Heimat im Einvernehmen mit den anderen Ressorts festlegen, dass sie verpflichtet sind, nach § 19 bereitgestellte IT-Sicherheitsprodukte beim Bundesamt abzurufen. Eigenbeschaffungen der Einrichtungen der Bundesverwaltung sind in diesem Fall nur zulässig, wenn das spezifische Anforderungsprofil den Einsatz abweichender Produkte erfordert. Dies gilt nicht für die in § 2 Nummer 21 genannten Gerichte und Verfassungsorgane sowie die Auslandsinformations- und -kommunikationstechnik gemäß § 7 Absatz 6.	(6) Für die Einrichtungen der Bundesverwaltung kann das Bundesministerium des Innern und für Heimat im Einvernehmen mit den anderen Ressorts festlegen, dass sie verpflichtet sind, nach § 19 bereitgestellte IT-Sicherheitsprodukte beim Bundesamt abzurufen. Eigenbeschaffungen der Einrichtungen der Bundesverwaltung sind in diesem Fall nur zulässig, wenn das spezifische Anforderungsprofil den Einsatz abweichender Produkte erfordert. Dies gilt nicht für die in § 2 Nummer 21 genannten Gerichte und Verfassungsorgane sowie die Auslandsinformations- und -kommunikationstechnik gemäß § 7 Absatz 6.
§ 45	§ 45
Informationssicherheitsbeauftragte der Einrichtungen der Bundesverwaltung	**Informationssicherheitsbeauftragte der Einrichtungen der Bundesverwaltung**
(1) Jede Leitung einer Einrichtung der Bundesverwaltung bestellt für ihre Einrichtung eine Informationssicherheitsbeauftragte oder einen Informationssicherheitsbeauftragten und bestimmt mindestens eine zur Vertretung berechtigte Person.	(1) Jede Leitung einer Einrichtung der Bundesverwaltung bestellt für ihre Einrichtung eine Informationssicherheitsbeauftragte oder einen Informationssicherheitsbeauftragten und bestimmt mindestens eine zur Vertretung berechtigte Person.

Entwurf	Beschlüsse des 4. Ausschusses
(2) Für die Erfüllung ihrer Aufgaben ist eine zielgerichtete Befähigung der Informationssicherheitsbeauftragten der Einrichtungen der Bundesverwaltung notwendig. Die Informationssicherheitsbeauftragten der Einrichtungen sowie ihre Vertreter müssen die zur Erfüllung ihrer Aufgaben erforderliche Fachkunde erwerben. Sie sowie ihre Vertreter unterstehen der Fachaufsicht des oder der Informationssicherheitsbeauftragten des jeweils zuständigen Ressorts.	(2) Für die Erfüllung ihrer Aufgaben ist eine zielgerichtete Befähigung der Informationssicherheitsbeauftragten der Einrichtungen der Bundesverwaltung notwendig. Die Informationssicherheitsbeauftragten der Einrichtungen sowie ihre Vertreter müssen die zur Erfüllung ihrer Aufgaben erforderliche Fachkunde erwerben. Sie sowie ihre Vertreter unterstehen der Fachaufsicht des oder der Informationssicherheitsbeauftragten des jeweils zuständigen Ressorts.
(3) Die Informationssicherheitsbeauftragten der Einrichtungen der Bundesverwaltung sind für den Aufbau und die Aufrechterhaltung des Informationssicherheitsprozesses ihrer Einrichtung zuständig. Sie erstellen ein Informationssicherheitskonzept, das mindestens die Vorgaben des Bundesamtes nach § 44 Absatz 1 erfüllt. Sie wirken auf die operative Umsetzung des Informationssicherheitskonzepts hin und kontrollieren die Umsetzung innerhalb der Einrichtung. Die Informationssicherheitsbeauftragten beraten die Leitung der Einrichtung der Bundesverwaltung in allen Fragen der Informationssicherheit und unterrichten die Leitung der Einrichtung der Bundesverwaltung sowie den oder die jeweils zuständige Informationssicherheitsbeauftragte des Ressorts regelmäßig sowie anlassbezogen über ihre Tätigkeit, über den Stand der Informationssicherheit innerhalb der Einrichtung, über die Mittel- und Personalausstattung sowie über Sicherheitsvorfälle. Ihre Berichts- und Beratungsaufgaben erfüllen sie unabhängig und weisungsfrei.	(3) Die Informationssicherheitsbeauftragten der Einrichtungen der Bundesverwaltung sind für den Aufbau und die Aufrechterhaltung des Informationssicherheitsprozesses ihrer Einrichtung zuständig. Sie erstellen ein Informationssicherheitskonzept, das mindestens die Vorgaben des Bundesamtes nach § 44 Absatz 1 erfüllt. Sie wirken auf die operative Umsetzung des Informationssicherheitskonzepts hin und kontrollieren die Umsetzung innerhalb der Einrichtung. Die Informationssicherheitsbeauftragten beraten die Leitung der Einrichtung der Bundesverwaltung in allen Fragen der Informationssicherheit und unterrichten die Leitung der Einrichtung der Bundesverwaltung sowie den oder die jeweils zuständige Informationssicherheitsbeauftragte des Ressorts regelmäßig sowie anlassbezogen über ihre Tätigkeit, über den Stand der Informationssicherheit innerhalb der Einrichtung, über die Mittel- und Personalausstattung sowie über Sicherheitsvorfälle. Ihre Berichts- und Beratungsaufgaben erfüllen sie unabhängig und weisungsfrei.
(4) Die Informationssicherheitsbeauftragten der Einrichtungen sind bei allen Maßnahmen zu beteiligen, die die Informationssicherheit der Einrichtung betreffen. Sie haben ein unmittelbares Vortragsrecht bei der jeweiligen Leitung ihrer Einrichtung sowie bei dem oder der Informationssicherheitsbeauftragten des jeweils zuständigen Ressorts. Sie dürfen von ihrer jeweiligen Einrichtung wegen der Erfüllung ihrer Aufgaben nicht abberufen oder benachteiligt werden.	(4) Die Informationssicherheitsbeauftragten der Einrichtungen sind bei allen Maßnahmen zu beteiligen, die die Informationssicherheit der Einrichtung betreffen. Sie haben ein unmittelbares Vortragsrecht bei der jeweiligen Leitung ihrer Einrichtung sowie bei dem oder der Informationssicherheitsbeauftragten des jeweils zuständigen Ressorts. Sie dürfen von ihrer jeweiligen Einrichtung wegen der Erfüllung ihrer Aufgaben nicht abberufen oder benachteiligt werden.

Entwurf	Beschlüsse des 4. Ausschusses
§ 46	§ 46
Informationssicherheitsbeauftragte der Ressorts	**Informationssicherheitsbeauftragte der Ressorts**
(1) Die Leitungen der einzelnen Ressorts sowie die Leitungen weiterer oberster Bundesbehörden bestellen jeweils eine Informationssicherheitsbeauftragte oder einen Informationssicherheitsbeauftragten des Ressorts, der oder dem unter Berücksichtigung der Belange des IT-Betriebs die Steuerung und Überwachung des Informationssicherheitsmanagements innerhalb des Ressorts beziehungsweise innerhalb der obersten Bundesbehörde und ihres Geschäftsbereichs obliegt, und bestimmen mindestens eine zur Vertretung berechtigte Person. Der oder die Informationssicherheitsbeauftragte des Ressorts wirkt auf die Umsetzung der Informationssicherheit in ihrem oder seinem Ressort hin.	(1) Die Leitungen der einzelnen Ressorts sowie die Leitungen weiterer oberster Bundesbehörden bestellen jeweils eine Informationssicherheitsbeauftragte oder einen Informationssicherheitsbeauftragten des Ressorts, der oder dem unter Berücksichtigung der Belange des IT-Betriebs die Steuerung und Überwachung des Informationssicherheitsmanagements innerhalb des Ressorts beziehungsweise innerhalb der obersten Bundesbehörde und ihres Geschäftsbereichs obliegt, und bestimmen mindestens eine zur Vertretung berechtigte Person. Der oder die Informationssicherheitsbeauftragte des Ressorts wirkt auf die Umsetzung der Informationssicherheit in ihrem oder seinem Ressort hin.
(2) Für die Erfüllung ihrer Aufgaben ist eine zielgerichtete Befähigung der Informationssicherheitsbeauftragten der Ressorts notwendig. Der oder die Informationssicherheitsbeauftragte des Ressorts muss die zur Erfüllung seiner oder ihrer Aufgaben erforderliche Fachkunde erwerben.	(2) Für die Erfüllung ihrer Aufgaben ist eine zielgerichtete Befähigung der Informationssicherheitsbeauftragten der Ressorts notwendig. Der oder die Informationssicherheitsbeauftragte des Ressorts muss die zur Erfüllung seiner oder ihrer Aufgaben erforderliche Fachkunde erwerben.
(3) Die Informationssicherheitsbeauftragten der Ressorts koordinieren jeweils die Fortschreibung von Informationssicherheitsleitlinien für ihr Ressort. Sie unterrichten die Ressortleitung über ihre Tätigkeit und über den Stand der Informationssicherheit innerhalb des Ressorts, über die Mittel- und Personalausstattung sowie über Sicherheitsvorfälle. Ihre Berichts- und Beratungsaufgaben erfüllen sie unabhängig und weisungsfrei.	(3) Die Informationssicherheitsbeauftragten der Ressorts koordinieren jeweils die Fortschreibung von Informationssicherheitsleitlinien für ihr Ressort. Sie unterrichten die Ressortleitung über ihre Tätigkeit und über den Stand der Informationssicherheit innerhalb des Ressorts, über die Mittel- und Personalausstattung sowie über Sicherheitsvorfälle. Ihre Berichts- und Beratungsaufgaben erfüllen sie unabhängig und weisungsfrei.
(4) In begründeten Einzelfällen kann der oder die 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. Über eine Untersagung ist das Bundesamt zu unterrichten.	(4) In begründeten Einzelfällen kann der oder die 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. Über eine Untersagung ist das Bundesamt zu unterrichten.

Entwurf	Beschlüsse des 4. Ausschusses
(5) Der oder die Informationssicherheitsbeauftragte des Ressorts kann im Benehmen mit dem Bundesamt Einrichtungen der Bundesverwaltung innerhalb des Ressorts von Verpflichtungen nach diesem Teil teilweise oder insgesamt durch Erteilung eines Ausnahmebescheides befreien. Voraussetzung hierfür ist, dass sachliche Gründe für die Erteilung eines Ausnahmebescheids vorliegen und durch die Befreiung keine nachteiligen Auswirkungen für die Informationssicherheit des Bundes zu befürchten sind. Über erteilte Ausnahmebescheide ist das Bundesamt zu unterrichten. Satz 1 gilt nicht, wenn die jeweilige Einrichtung der Bundesverwaltung die Voraussetzungen des § 28 Absatz 1 Satz 1 oder § 28 Absatz 2 Satz 1 erfüllt.	(5) Der oder die Informationssicherheitsbeauftragte des Ressorts kann im Benehmen mit dem Bundesamt Einrichtungen der Bundesverwaltung innerhalb des Ressorts von Verpflichtungen nach diesem Teil teilweise oder insgesamt durch Erteilung eines Ausnahmebescheides befreien. Voraussetzung hierfür ist, dass sachliche Gründe für die Erteilung eines Ausnahmebescheids vorliegen und durch die Befreiung keine nachteiligen Auswirkungen für die Informationssicherheit des Bundes zu befürchten sind. Über erteilte Ausnahmebescheide ist das Bundesamt zu unterrichten. Satz 1 gilt nicht, wenn die jeweilige Einrichtung der Bundesverwaltung die Voraussetzungen des § 28 Absatz 1 Satz 1 oder § 28 Absatz 2 Satz 1 erfüllt.
(6) Der oder die Informationssicherheitsbeauftragte des Ressorts ist bei allen Gesetzes-, Verordnungs- und sonstigen wichtigen Vorhaben innerhalb des Ressorts zu beteiligen, soweit die Vorhaben Fragen der Informationssicherheit berühren. Er oder sie hat ein unmittelbares Vortragsrecht bei der jeweiligen Leitung des Ressorts. Sie dürfen von ihrer jeweiligen Einrichtung wegen der Erfüllung ihrer Aufgaben nicht abberufen oder benachteiligt werden.	(6) Der oder die Informationssicherheitsbeauftragte des Ressorts ist bei allen Gesetzes-, Verordnungs- und sonstigen wichtigen Vorhaben innerhalb des Ressorts zu beteiligen, soweit die Vorhaben Fragen der Informationssicherheit berühren. Er oder sie hat ein unmittelbares Vortragsrecht bei der jeweiligen Leitung des Ressorts. Sie dürfen von ihrer jeweiligen Einrichtung wegen der Erfüllung ihrer Aufgaben nicht abberufen oder benachteiligt werden.
§ 47	§ 47
Wesentliche Digitalisierungsvorhaben und Kommunikationsinfrastrukturen des Bundes	**Wesentliche Digitalisierungsvorhaben und Kommunikationsinfrastrukturen des Bundes**
(1) Für die Planung und Umsetzung von wesentlichen Digitalisierungsvorhaben und Kommunikationsinfrastrukturen des Bundes sind eigene Informationssicherheitsbeauftragte nach § 45 zu bestellen.	(1) Für die Planung und Umsetzung von wesentlichen Digitalisierungsvorhaben und Kommunikationsinfrastrukturen des Bundes sind eigene Informationssicherheitsbeauftragte nach § 45 zu bestellen.
(2) 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.	(2) 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.

Entwurf	Beschlüsse des 4. Ausschusses
(3) In der Regel bestellt diejenige Einrichtung den Informationssicherheitsbeauftragten nach Satz 1, die für die Steuerung des Digitalisierungsvorhabens oder der Kommunikationsinfrastrukturen des Bundes verantwortlich ist. Wenn bei ressortübergreifenden Digitalisierungsvorhaben oder Kommunikationsinfrastrukturen eine Bestellung durch Einrichtungen in verschiedenen beteiligten Ressorts und weiteren obersten Bundesbehörden in Betracht kommt und nicht innerhalb einer angemessenen Frist Einvernehmen darüber hergestellt werden kann, durch welche Einrichtung die Bestellung erfolgt, so entscheidet das Bundesministerium des Innern und für Heimat.	(3) In der Regel bestellt diejenige Einrichtung den Informationssicherheitsbeauftragten nach Satz 1, die für die Steuerung des Digitalisierungsvorhabens oder der Kommunikationsinfrastrukturen des Bundes verantwortlich ist. Wenn bei ressortübergreifenden Digitalisierungsvorhaben oder Kommunikationsinfrastrukturen eine Bestellung durch Einrichtungen in verschiedenen beteiligten Ressorts und weiteren obersten Bundesbehörden in Betracht kommt und nicht innerhalb einer angemessenen Frist Einvernehmen darüber hergestellt werden kann, durch welche Einrichtung die Bestellung erfolgt, so entscheidet das Bundesministerium des Innern und für Heimat.
(4) Die Informationssicherheitsbeauftragten nach Satz 1 unterstehen entweder der Leitung der Einrichtung oder dem oder der jeweils zuständigen Informationssicherheitsbeauftragten des Ressorts.	(4) Die Informationssicherheitsbeauftragten nach Satz 1 unterstehen entweder der Leitung der Einrichtung oder dem oder der jeweils zuständigen Informationssicherheitsbeauftragten des Ressorts.
(5) Zur Gewährleistung der Informationssicherheit bei der Planung und Umsetzung von wesentlichen Digitalisierungsvorhaben soll die jeweils verantwortliche Einrichtung das Bundesamt frühzeitig beteiligen und dem Bundesamt Gelegenheit zur Stellungnahme geben.	(5) Zur Gewährleistung der Informationssicherheit bei der Planung und Umsetzung von wesentlichen Digitalisierungsvorhaben soll die jeweils verantwortliche Einrichtung das Bundesamt frühzeitig beteiligen und dem Bundesamt Gelegenheit zur Stellungnahme geben.

Entwurf	Beschlüsse des 4. Ausschusses
§ 48	§ 48
Amt des Koordinators für Informationssicherheit	**Amt des Koordinators für Informationssicherheit**

Die Bundesregierung bestellt eine Koordinatorin oder einen Koordinator für Informationssicherheit.	(1) Die Leitung des Bundesamtes nimmt die Aufgaben der Koordinatorin oder des Koordinators für Informationssicherheit wahr. Sie wird durch eine Stellvertreterin oder einen Stellvertreter unterstützt. Die Koordinatorin oder der Koordinator sowie die Stellvertreterin oder der Stellvertreter müssen über die für die Erfüllung ihrer Aufgaben und Ausübung ihrer Befugnisse erforderliche Qualifikation, Erfahrung und Sachkunde insbesondere im Bereich der Informationssicherheit verfügen. (2) Die Koordinatorin oder der Koordinator nimmt die in Teil 2 Kapitel 1 genannten Aufgaben und Durchsetzungsbefugnisse des Bundesamts als zentrale Aufsichtsbehörde operativ unabhängig und weisungsfrei wahr, einschließlich der Inkraftsetzung von Mindestsicherheitsstandards für die Bundesverwaltung gemäß § 44 und der Überwachung von Risiken in der Informationssicherheit des Bundes mittels Kontrollen nach § 7. (3) Auf Basis der durch das Bundesamt erhaltenen Informationen im Rahmen der Rolle als zentrale Meldestelle nach § 4, des Informationsaustauschs nach § 6, der Kontrollen nach § 7, der Abwehr von Schadprogrammen nach § 8, der Verarbeitung von Protokollierungsdaten nach § 9, oder aus der weiteren Zusammenarbeit mit Einrichtungen der Bundesverwaltung, wahrt die Koordinatorin oder der Koordinator den Überblick über die Informationssicherheitslage in der Bundesverwaltung. Auf dieser Grundlage hat sie oder er die Befugnis, Anordnungen zur Umsetzung von Verbesserungsvorschlägen nach § 7 oder zur Abwendung oder Behebung von Sicherheitsvorfällen nach § 10 zu erteilen. (4) Die Koordinatorin oder der Koordinator unterstützt die Ressorts bei der Umsetzung der Vorgaben nach diesem Gesetz. Dabei wirkt sie oder er gemeinsam mit dem Beauftragten der Bundesregierung für Informationstechnik auf ein angemessenes Verhältnis zwischen dem Einsatz von Informationstechnik und Informationssicherheit hin. (5) Die Koordinatorin oder der Koordinator wird bei allen Gesetzes-, Verordnungs- und sonstigen wichtigen Vorhaben beteiligt soweit sie Fragen der Informations-

Entwurf	Beschlüsse des 4. Ausschusses
	sicherheit berühren. Wenn in ressortübergreifenden oder föderalen Gremien Fragen der Informationssicherheit behandelt werden, wird er oder sie eingebunden. (6) Die Koordinatorin oder der Koordinator unterrichtet den Haushaltsausschuss des Deutschen Bundestages kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres über die Anwendung des § 7.
Teil 4	Teil 4
Datenbanken der Domain-Name-Registrierungsdaten	Datenbanken der Domain-Name-Registrierungsdaten
§ 49	§ 49
Pflicht zum Führen einer Datenbank	**Pflicht zum Führen einer Datenbank**
(1) Um einen Beitrag zur Sicherheit, Stabilität und Resilienz des Domain Name Systems zu leisten, haben Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister genaue und vollständige Domain-Namen-Registrierungsdaten in einer eigenen Datenbank mit der gebotenen Sorgfalt zu sammeln und zu pflegen.	(1) Um einen Beitrag zur Sicherheit, Stabilität und Resilienz des Domain Name Systems zu leisten, haben Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister genaue und vollständige Domain-Namen-Registrierungsdaten in einer eigenen Datenbank mit der gebotenen Sorgfalt zu sammeln und zu pflegen.
(2) Die Datenbank 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:	(2) Die Datenbank 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:
1. den Domain-Namen;	1. den Domain-Namen;
2. das Datum der Registrierung;	2. das Datum der Registrierung;
3. den Namen des Domain-Inhabers, seine E-Mail-Adresse und Telefonnummer;	3. den Namen des Domain-Inhabers, seine E-Mail-Adresse und Telefonnummer;

Entwurf	Beschlüsse des 4. Ausschusses
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.	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.
(3) Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister haben Vorgaben und Verfahren, einschließlich Überprüfungsverfahren, vorzuhalten, mit denen sichergestellt wird, dass die Datenbank genaue und vollständige Angaben enthält. Sie haben diese Vorgaben und Verfahren bis zum … [*einfügen: Datum, drei Monate nach Inkrafttreten*] öffentlich zugänglich zu machen.	(3) Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister haben Vorgaben und Verfahren, einschließlich Überprüfungsverfahren, vorzuhalten, mit denen sichergestellt wird, dass die Datenbank genaue und vollständige Angaben enthält. Sie haben diese Vorgaben und Verfahren bis zum … [*einfügen: Datum, drei Monate nach Inkrafttreten*] öffentlich zugänglich zu machen.
(4) Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister haben unverzüglich nach der Registrierung eines Domain-Namens die nicht personenbezogenen Domain-Namen-Registrierungsdaten öffentlich zugänglich zu machen.	(4) Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister haben unverzüglich nach der Registrierung eines Domain-Namens die nicht personenbezogenen Domain-Namen-Registrierungsdaten öffentlich zugänglich zu machen.
(5) Das Bundesamt kann die Erfüllung der Vorgaben überprüfen.	(5) Das Bundesamt kann die Erfüllung der Vorgaben überprüfen.
§ 50	§ 50
Verpflichtung zur Zugangsgewährung	**Verpflichtung zur Zugangsgewährung**
(1) Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister haben einem berechtigten Zugangsnachfrager auf begründeten Antrag unter Darlegung eines berechtigten Interesses und soweit dies für die Erfüllung von deren Aufgaben erforderlich ist unverzüglich und in jedem Fall innerhalb von 72 Stunden nach Eingang des Antrags Zugang zu den Domain-Namen-Registrierungsdaten zu gewähren. Liegen die angefragten Informationen nicht vor, so ist dies innerhalb von 24 Stunden nach Eingang des Antrags auf Zugang mitzuteilen.	(1) Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister haben einem berechtigten Zugangsnachfrager auf begründeten Antrag unter Darlegung eines berechtigten Interesses und soweit dies für die Erfüllung von deren Aufgaben erforderlich ist unverzüglich und in jedem Fall innerhalb von 72 Stunden nach Eingang des Antrags Zugang zu den Domain-Namen-Registrierungsdaten zu gewähren. Liegen die angefragten Informationen nicht vor, so ist dies innerhalb von 24 Stunden nach Eingang des Antrags auf Zugang mitzuteilen.

Entwurf	Beschlüsse des 4. Ausschusses
(2) Die Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister haben die Vorgaben und Verfahren im Hinblick auf die Offenlegung der Domain-Namen-Registrierungsdaten bis zum … [*einfügen: Datum, drei Monate nach Inkrafttreten*] öffentlich zugänglich zu machen.	(2) Die Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister haben die Vorgaben und Verfahren im Hinblick auf die Offenlegung der Domain-Namen-Registrierungsdaten bis zum … [*einfügen: Datum, drei Monate nach Inkrafttreten*] öffentlich zugänglich zu machen.
(3) Das Auskunftsverfahren bei Bestandsdaten gemäß § 22 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes bleibt unberührt.	(3) Das Auskunftsverfahren bei Bestandsdaten gemäß § 22 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes bleibt unberührt.
(4) Das Bundesamt kann die Erfüllung der Vorgaben überprüfen.	(4) Das Bundesamt kann die Erfüllung der Vorgaben überprüfen.
§ 51	§ 51
Kooperationspflicht	**Kooperationspflicht**
Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister sind zur Kooperation verpflichtet, um die in den §§ 49 und 50 festgelegten Verpflichtungen zu erfüllen und insbesondere eine doppelte Erhebung von Domain-Namen-Registrierungsdaten vom Domaininhaber auszuschließen.	Top Level Domain Name Registries und Domain-Name-Registry-Dienstleister sind zur Kooperation verpflichtet, um die in §§ 49 und § 50 festgelegten Verpflichtungen zu erfüllen und insbesondere eine doppelte Erhebung von Domain-Namen-Registrierungsdaten vom Domaininhaber auszuschließen.
Teil 5	Teil 5
Zertifizierung, Konformitätserklärung und Kennzeichen	Zertifizierung, Konformitätserklärung und Kennzeichen
§ 52	§ 52
Zertifizierung	**Zertifizierung**
(1) Das Bundesamt ist nationale Zertifizierungsstelle der Bundesverwaltung für IT-Sicherheit.	(1) Das Bundesamt ist nationale Zertifizierungsstelle der Bundesverwaltung für IT-Sicherheit.

Entwurf	Beschlüsse des 4. Ausschusses
(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 Anzahl 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 diejenigen Unterlagen vorzulegen und die Auskünfte zu erteilen, deren Kenntnis für die Prüfung und Bewertung der Produkte und Leistungen oder der Eignung der Person sowie für die Erteilung des Zertifikats erforderlich ist. Ein Zertifikat nach Satz 1 darf nur dann für ein Produkt, eine Leistung, eine Person oder einen IT-Sicherheitsdienstleister verwendet werden, wenn das Bundesamt ein entsprechendes Zertifikat erteilt hat und dieses nicht aufgehoben wurde oder auf andere Weise ungültig geworden 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 Anzahl 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 diejenigen Unterlagen vorzulegen und die Auskünfte zu erteilen, deren Kenntnis für die Prüfung und Bewertung der Produkte und Leistungen oder der Eignung der Person sowie für die Erteilung des Zertifikats erforderlich ist. Ein Zertifikat nach Satz 1 darf nur dann für ein Produkt, eine Leistung, eine Person oder einen IT-Sicherheitsdienstleister verwendet werden, wenn das Bundesamt ein entsprechendes Zertifikat erteilt hat und dieses nicht aufgehoben wurde oder auf andere Weise ungültig geworden ist.
(3) Die Prüfung und Bewertung können durch vom Bundesamt nach Absatz 7 anerkannte sachverständige Stellen erfolgen.	(3) Die Prüfung und Bewertung können durch vom Bundesamt nach Absatz 7 anerkannte sachverständige Stellen erfolgen.
(4) Das Sicherheitszertifikat wird erteilt, wenn	(4) Das Sicherheitszertifikat wird erteilt, wenn
1. die informationstechnischen Systeme, Komponenten, Produkte oder Schutzprofile den vom Bundesamt festgelegten Kriterien entsprechen und	1. die informationstechnischen Systeme, Komponenten, Produkte oder Schutzprofile den vom Bundesamt festgelegten Kriterien entsprechen und
2. das Bundesministerium des Innern und für Heimat die Erteilung des Zertifikats nicht nach Absatz 5 untersagt hat.	2. das Bundesministerium des Innern und für Heimat die Erteilung des Zertifikats nicht nach Absatz 5 untersagt hat.
Vor Erteilung des Sicherheitszertifikats legt das Bundesamt den Vorgang dem Bundesministerium des Innern und für Heimat zur Prüfung nach Absatz 5 vor.	Vor Erteilung des Sicherheitszertifikats legt das Bundesamt den Vorgang dem Bundesministerium des Innern und für Heimat zur Prüfung nach Absatz 5 vor.

Entwurf	Beschlüsse des 4. Ausschusses
(5) Das Bundesministerium des Innern und für Heimat kann die Erteilung eines Zertifikats nach Absatz 4 im Einzelfall untersagen, wenn überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung entgegenstehen.	(5) Das Bundesministerium des Innern und für Heimat kann die Erteilung eines Zertifikats nach Absatz 4 im Einzelfall untersagen, wenn überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung entgegenstehen.
(6) Für die Zertifizierung von Personen und IT-Sicherheitsdienstleistern gilt Absatz 4 entsprechend.	(6) Für die Zertifizierung von Personen und IT-Sicherheitsdienstleistern gilt Absatz 4 entsprechend.
(7) Eine Stelle wird als sachverständig im Sinne des Absatzes 3 anerkannt, wenn	(7) Eine Stelle wird als sachverständig im Sinne des Absatz 3 anerkannt, wenn
1. die sachliche und personelle Ausstattung sowie die fachliche Qualifikation und Zuverlässigkeit der Konformitätsbewertungsstelle den vom Bundesamt festgelegten Kriterien entsprechen und	1. die sachliche und personelle Ausstattung sowie die fachliche Qualifikation und Zuverlässigkeit der Konformitätsbewertungsstelle den vom Bundesamt festgelegten Kriterien entsprechen und
2. das Bundesministerium des Innern und für 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.
Das Bundesamt stellt durch die notwendigen Maßnahmen sicher, dass das Fortbestehen der Voraussetzungen nach Satz 1 regelmäßig überprüft wird.	Das Bundesamt stellt durch die notwendigen Maßnahmen sicher, dass das Fortbestehen der Voraussetzungen nach Satz 1 regelmäßig überprüft wird.
(8) Sicherheitszertifikate anderer anerkannter Zertifizierungsstellen aus dem Bereich der Europäischen Union werden vom Bundesamt anerkannt, sofern sie eine den Sicherheitszertifikaten des Bundesamtes gleichwertige Sicherheit ausweisen und die Gleichwertigkeit vom Bundesamt festgestellt worden ist.	(8) Sicherheitszertifikate anderer anerkannter Zertifizierungsstellen aus dem Bereich der Europäischen Union werden vom Bundesamt anerkannt, sofern sie eine den Sicherheitszertifikaten des Bundesamtes gleichwertige Sicherheit ausweisen und die Gleichwertigkeit vom Bundesamt festgestellt worden ist.

Entwurf	Beschlüsse des 4. Ausschusses
§ 53	§ 53
Konformitätsbewertung und Konformitätserklärung	**Konformitätsbewertung und Konformitätserklärung**
(1) Das Bundesamt kann für die vom Bundesamt in einer Technischen Richtlinie festgelegten Anforderungen und Vorgaben zulassen, dass ein Hersteller oder Anbieter von IKT-Produkten, IKT-Diensten und IKT-Prozessen, die keine Verbraucherprodukte nach § 55 sind, sowie eine Person oder ein IT-Sicherheitsdienstleister eine Selbstbewertung seiner oder ihrer Konformität vornehmen. Der Hersteller oder Anbieter von IKT-Produkten, IKT-Diensten und IKT-Prozessen, die Person oder der IT-Sicherheitsdienstleister kann unter den Voraussetzungen von Satz 1 eine Konformitätserklärung ausstellen, die bestätigt, dass er oder sie die in der Technischen Richtlinie festgelegten Anforderungen erfüllt. Durch die Ausstellung der Konformitätserklärung übernimmt der Hersteller oder Anbieter der IKT-Produkte, IKT-Dienste und IKT-Prozesse, die Person oder der IT-Sicherheitsdienstleister (Aussteller) die Verantwortung dafür, dass das IKT-Produkt, der IKT-Dienst, der IKT-Prozess, die Person oder die IT-Sicherheitsdienstleistung den in der Technischen Richtlinie festgelegten Anforderungen entspricht. Eine Erklärung nach Satz 3 darf nur dann für ein IKT-Produkt, einen IKT-Dienst und IKT-Prozess, eine Person oder einen IT-Sicherheitsdienstleister verwendet werden, wenn der Hersteller, der Anbieter, die Person oder der IT-Sicherheitsdienstleister diese ausgestellt hat und sie weder widerrufen noch nach Absatz 5 Nummer 3 für ungültig erklärt wurde.	(1) Das Bundesamt kann für die vom Bundesamt in einer Technischen Richtlinie festgelegten Anforderungen und Vorgaben zulassen, dass ein Hersteller oder Anbieter von IKT-Produkten, IKT-Diensten und IKT-Prozessen, die keine Verbraucherprodukte nach § 55 sind, sowie eine Person oder ein IT-Sicherheitsdienstleister eine Selbstbewertung seiner oder ihrer Konformität vornehmen. Der Hersteller oder Anbieter von IKT-Produkten, IKT-Diensten und IKT-Prozessen, die Person oder der IT-Sicherheitsdienstleister kann unter den Voraussetzungen von Satz 1 eine Konformitätserklärung ausstellen, die bestätigt, dass er oder sie die in der Technischen Richtlinie festgelegten Anforderungen erfüllt. Durch die Ausstellung der Konformitätserklärung übernimmt der Hersteller oder Anbieter der IKT-Produkte, IKT-Dienste und IKT-Prozesse, die Person oder der IT-Sicherheitsdienstleister (Aussteller) die Verantwortung dafür, dass das IKT-Produkt, der IKT-Dienst, der IKT-Prozess, die Person oder die IT-Sicherheitsdienstleistung den in der Technischen Richtlinie festgelegten Anforderungen entspricht. Eine Erklärung nach Satz 3 darf nur dann für ein IKT-Produkt, einen IKT-Dienst und IKT-Prozess, eine Person oder einen IT-Sicherheitsdienstleister verwendet werden, wenn der Hersteller, der Anbieter, die Person oder der IT-Sicherheitsdienstleister diese ausgestellt hat und sie weder widerrufen noch nach Absatz 5 Nummer 3 für ungültig erklärt wurde.
(2) Die Technische Richtlinie nach Absatz 1 kann insbesondere Vorgaben enthalten über	(2) Die Technische Richtlinie nach Absatz 1 kann insbesondere Vorgaben enthalten über
1. den Inhalt und das Format der Konformitätserklärung,	1. den Inhalt und das Format der Konformitätserklärung,
2. Nachweise und Verfahren, die die Angaben der Konformitätserklärung belegen,	2. Nachweise und Verfahren, die die Angaben der Konformitätserklärung belegen,

Entwurf	Beschlüsse des 4. Ausschusses
3. die Bedingungen für die Aufrechterhaltung, Fortführung und Verlängerung der Konformitätserklärung,	3. die Bedingungen für die Aufrechterhaltung, Fortführung und Verlängerung der Konformitätserklärung,
4. die Verwendung eines vom Bundesamt bereitgestellten Kennzeichens und Siegels sowie die Bedingungen für deren Verwendung,	4. die Verwendung eines vom Bundesamt bereitgestellten Kennzeichens und Siegels sowie die Bedingungen für deren Verwendung,
5. die Meldung und Behandlung erkannter Schwachstellen des IKT-Produktes, IKT-Dienstes oder IKT-Prozesses oder der IT-Sicherheitsdienstleistung,	5. die Meldung und Behandlung erkannter Schwachstellen des IKT-Produktes, IKT-Dienstes oder IKT-Prozesses oder der IT-Sicherheitsdienstleistung,
6. die Bereitstellung von Informationen auf der Internetseite des Bundesamtes über die Konformitätserklärung, dessen Aussteller und das IKT-Produkt, den IKT-Dienst, den IKT-Prozess, die Person oder die IT-Sicherheitsdienstleistung oder	6. die Bereitstellung von Informationen auf der Internetseite des Bundesamtes über die Konformitätserklärung, dessen Aussteller und das IKT-Produkt, den IKT-Dienst, den IKT-Prozess, die Person oder die IT-Sicherheitsdienstleistung oder
7. die Befristung der Geltungsdauer der Konformitätserklärung.	7. die Befristung der Geltungsdauer der Konformitätserklärung.
(3) Wird in den Vorgaben nach Absatz 2 festgelegt, dass die Angaben der Konformitätserklärung nur durch eine akkreditierte Konformitätsbewertungsstelle nachgewiesen werden können, so kann das Bundesamt auf Antrag Konformitätsbewertungsstellen, die beabsichtigen, im Anwendungsbereich dieses Paragraphen tätig zu werden, eine Befugnis erteilen, wenn die maßgeblichen Voraussetzungen der Technischen Richtlinie erfüllt sind. Ohne eine Befugniserteilung durch das Bundesamt dürfen Konformitätsbewertungsstellen im Anwendungsbereich dieses Paragraphen nicht tätig werden.	(3) Wird in den Vorgaben nach Absatz 2 festgelegt, dass die Angaben der Konformitätserklärung nur durch eine akkreditierte Konformitätsbewertungsstelle nachgewiesen werden können, so kann das Bundesamt auf Antrag Konformitätsbewertungsstellen, die beabsichtigen, im Anwendungsbereich dieses Paragraphen tätig zu werden, eine Befugnis erteilen, wenn die maßgeblichen Voraussetzungen der Technischen Richtlinie erfüllt sind. Ohne eine Befugniserteilung durch das Bundesamt dürfen Konformitätsbewertungsstellen im Anwendungsbereich dieses Paragraphen nicht tätig werden.
(4) Der Aussteller hält die Konformitätserklärung, die technische Dokumentation und alle weiteren einschlägigen Informationen in Bezug auf die Konformität der IKT-Produkte, IKT-Dienste und IKT-Prozesse, der Person oder der IT-Sicherheitsdienstleistung mit den festgelegten Kriterien während eines Zeitraums, der vom Bundesamt in der Technischen Richtlinie nach Absatz 1 festgelegt wurde, für das Bundesamt bereit. Eine Kopie der Konformitätserklärung ist dem Bundesamt vorzulegen.	(4) Der Aussteller hält die Konformitätserklärung, die technische Dokumentation und alle weiteren einschlägigen Informationen in Bezug auf die Konformität der IKT-Produkte, IKT-Dienste und IKT-Prozesse, der Person oder der IT-Sicherheitsdienstleistung mit den festgelegten Kriterien während eines Zeitraums, der vom Bundesamt in der Technischen Richtlinie nach Absatz 1 festgelegt wurde, für das Bundesamt bereit. Eine Kopie der Konformitätserklärung ist dem Bundesamt vorzulegen.

Entwurf	Beschlüsse des 4. Ausschusses
(5) Das Bundesamt kann geeignete Maßnahmen ergreifen, um sicherzustellen, dass die Aussteller von Konformitätserklärungen den Anforderungen des Schemas und den Vorgaben dieses Paragraphen genügen und insbesondere	(5) Das Bundesamt kann geeignete Maßnahmen ergreifen, um sicherzustellen, dass die Aussteller von Konformitätserklärungen den Anforderungen des Schemas und den Vorgaben dieses Paragraphen genügen und insbesondere
1. Aussteller von Konformitätserklärungen auffordern, ihm sämtliche Auskünfte zu erteilen, die es für die Erfüllung ihrer Aufgaben benötigt,	1. Aussteller von Konformitätserklärungen auffordern, ihm sämtliche Auskünfte zu erteilen, die es für die Erfüllung ihrer Aufgaben benötigt,
2. Untersuchungen in Form von Testkäufen oder Audits bei den Ausstellern von Konformitätserklärungen durchführen, um deren Einhaltung der in der Technischen Richtlinie festgelegten Anforderungen und Vorgaben nach Absatz 1 zu überprüfen und	2. Untersuchungen in Form von Testkäufen oder Audits bei den Ausstellern von Konformitätserklärungen durchführen, um deren Einhaltung der in der Technischen Richtlinie festgelegten Anforderungen und Vorgaben nach Absatz 1 zu überprüfen und
3. Konformitätserklärungen nach Absatz 1 für ungültig erklären.	3. Konformitätserklärungen nach Absatz 1 für ungültig erklären.
(6) Für Maßnahmen nach Absatz 4 kann das Bundesamt Gebühren erheben, sofern es auf Grund von Anhaltspunkten tätig geworden ist, die berechtigte Zweifel an der Einhaltung der Anforderungen der Technischen Richtlinie oder dieses Paragraphen begründeten.	(6) Für Maßnahmen nach Absatz 4 kann das Bundesamt Gebühren erheben, sofern es auf Grund von Anhaltspunkten tätig geworden ist, die berechtigte Zweifel an der Einhaltung der Anforderungen der Technischen Richtlinie oder dieses Paragraphen begründeten.
§ 54	§ 54
Nationale Behörde für die Cybersicherheitszertifizierung	**Nationale Behörde für die Cybersicherheitszertifizierung**
(1) Das Bundesamt ist die nationale Behörde für die Cybersicherheitszertifizierung nach Artikel 58 Absatz 1 der Verordnung (EU) 2019/881.	(1) Das Bundesamt ist die nationale Behörde für die Cybersicherheitszertifizierung nach Artikel 58 Absatz 1 der Verordnung (EU) 2019/881.

Entwurf	Beschlüsse des 4. Ausschusses
(2) Das Bundesamt kann auf Antrag Konformitätsbewertungsstellen, die im Anwendungsbereich der Verordnung (EU) 2019/881 sowie des § 52 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 § 52 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 § 52 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 § 52 dieses Gesetzes erfüllt sind. Ohne eine Befugniserteilung durch das Bundesamt dürfen Konformitätsbewertungsstellen im Anwendungsbereich der Verordnung (EU) 2019/881 nicht tätig werden.
(3) Soweit dies zur Erfüllung seiner Aufgaben nach Artikel 58 Absatz 7 der Verordnung (EU) 2019/881 und nach § 52 dieses Gesetzes erforderlich ist, kann das Bundesamt von Konformitätsbewertungsstellen, denen eine Befugnis nach Absatz 2 erteilt wurde, von Inhabern europäischer Cybersicherheitszertifikate und 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.	(3) Soweit dies zur Erfüllung seiner Aufgaben nach Artikel 58 Absatz 7 der Verordnung (EU) 2019/881 und nach § 52 dieses Gesetzes erforderlich ist, kann das Bundesamt von Konformitätsbewertungsstellen, denen eine Befugnis nach Absatz 2 erteilt wurde, von Inhabern europäischer Cybersicherheitszertifikate und 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.
(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.

Entwurf	Beschlüsse des 4. Ausschusses
(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 dort befindliche Unterlagen und Muster 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.	(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 dort befindliche Unterlagen und Muster 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.
(6) Das Bundesamt kann von ihm ausgestellte Cybersicherheitszertifikate oder durch eine Konformitätsbewertungsstelle, der eine Befugnis nach 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,	(6) Das Bundesamt kann von ihm ausgestellte Cybersicherheitszertifikate oder durch eine Konformitätsbewertungsstelle, der eine Befugnis nach 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,
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
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 er 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 er das Bundesamt bei der Wahrnehmung seiner Befugnisse nach Absatz 4 oder im Falle eines Inhabers eines europäischen Cybersicherheitszertifikats auch nach Absatz 5 behindert hat.

Entwurf	Beschlüsse des 4. Ausschusses
Widerrufene Cybersicherheitszertifikate oder für ungültig erklärte EU-Konformitätserklärungen nach Satz 1 dürfen nicht verwendet werden.	Widerrufene Cybersicherheitszertifikate oder für ungültig erklärte EU-Konformitätserklärungen nach Satz 1 dürfen nicht verwendet werden.
(7) Das Bundesamt kann von ihm erteilte Befugnisse nach Absatz 2 widerrufen,	(7) Das Bundesamt kann von ihm erteilte Befugnisse nach Absatz 2 widerrufen,
1. sofern die Voraussetzungen des maßgeblichen europäischen Schemas für die Cybersicherheitszertifizierung nach Artikel 54 der Verordnung (EU) 2019/881 oder des § 52 dieses Gesetzes nicht erfüllt sind oder	1. sofern die Voraussetzungen des maßgeblichen europäischen Schemas für die Cybersicherheitszertifizierung nach Artikel 54 der Verordnung (EU) 2019/881 oder des § 52 dieses Gesetzes nicht erfüllt sind oder
2. wenn das Bundesamt die Erfüllung dieser Voraussetzungen nicht feststellen kann, weil die Konformitätsbewertungsstelle ihren Mitwirkungspflichten nach Absatz 3 nicht nachgekommen ist oder weil sie 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 sie das Bundesamt bei der Wahrnehmung seiner Befugnisse nach den Absätzen 4 und 5 behindert hat.
§ 55	§ 55
Freiwilliges IT-Sicherheitskennzeichen	**Freiwilliges IT-Sicherheitskennzeichen**
(1) Das Bundesamt führt zur Information von Verbrauchern über die IT-Sicherheit von Produkten bestimmter vom Bundesamt festgelegter Produktkategorien ein einheitliches IT-Sicherheitskennzeichen ein. Das IT-Sicherheitskennzeichen trifft keine Aussage über die den Datenschutz betreffenden Eigenschaften eines Produktes.	(1) Das Bundesamt führt zur Information von Verbrauchern über die IT-Sicherheit von Produkten bestimmter vom Bundesamt festgelegter Produktkategorien ein einheitliches IT-Sicherheitskennzeichen ein. Das IT-Sicherheitskennzeichen trifft keine Aussage über die den Datenschutz betreffenden Eigenschaften eines Produktes.
(2) Das IT-Sicherheitskennzeichen besteht aus	(2) Das IT-Sicherheitskennzeichen besteht aus
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
2. einer Information des Bundesamtes über sicherheitsrelevante IT-Eigenschaften des Produktes (Sicherheitsinformation).	2. einer Information des Bundesamtes über sicherheitsrelevante IT-Eigenschaften des Produktes (Sicherheitsinformation).

Entwurf	Beschlüsse des 4. Ausschusses
(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 § 56 Absatz 2 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, 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.	(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 § 56 Absatz 2 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, 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.
(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.

Entwurf	Beschlüsse des 4. Ausschusses
(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
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,
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
3. die gegebenenfalls erhobene Verwaltungsgebühr beglichen wurde.	3. die gegebenenfalls erhobene Verwaltungsgebühr beglichen wurde.
Die Erteilung der Freigabe erfolgt schriftlich und innerhalb einer angemessenen Frist, die in der Rechtsverordnung nach § 56 Absatz 2 bestimmt wird. Den genauen Ablauf des Antragsverfahrens und die beizufügenden Unterlagen regelt die Rechtsverordnung nach § 56 Absatz 2.	Die Erteilung der Freigabe erfolgt schriftlich und innerhalb einer angemessenen Frist, die in der Rechtsverordnung nach § 56 Absatz 2 bestimmt wird. Den genauen Ablauf des Antragsverfahrens und die beizufügenden Unterlagen regelt die Rechtsverordnung nach § 56 Absatz 2.
(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 § 56 Absatz 2 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 § 56 Absatz 2 festzulegen.
(7) Nach Ablauf der festgelegten Dauer, für die der Hersteller oder Diensteanbieter die Erfüllung der IT-Sicherheitsanforderungen zusichert, 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, für die der Hersteller oder Diensteanbieter die Erfüllung der IT-Sicherheitsanforderungen zusichert, 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.

Entwurf	Beschlüsse des 4. Ausschusses
(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 geeigneten Maßnahmen zum Schutz des Vertrauens der Verbraucher in das IT-Sicherheitskennzeichen treffen, insbesondere	(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 geeigneten Maßnahmen zum Schutz des Vertrauens der Verbraucher in das IT-Sicherheitskennzeichen treffen, insbesondere
1. Informationen über die Abweichungen oder Schwachstellen in geeigneter Weise in der Sicherheitsinformation veröffentlichen oder	1. Informationen über die Abweichungen oder Schwachstellen in geeigneter Weise in der Sicherheitsinformation veröffentlichen oder
2. die Freigabe des IT-Sicherheitskennzeichens widerrufen.	2. die Freigabe des IT-Sicherheitskennzeichens widerrufen.
Absatz 7 Satz 2 gilt entsprechend.	Absatz 7 Satz 2 gilt entsprechend.
(9) Bevor das Bundesamt eine Maßnahme nach Absatz 8 trifft, räumt es dem Hersteller oder Diensteanbieter die 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.	(9) Bevor das Bundesamt eine Maßnahme nach Absatz 8 trifft, räumt es dem Hersteller oder Diensteanbieter die 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.

Entwurf	Beschlüsse des 4. Ausschusses
Teil 6	Teil 6
Verordnungsermächtigungen, Grundrechtseinschränkungen und Berichtspflichten	Verordnungsermächtigungen, Grundrechtseinschränkungen und Berichtspflichten
§ 56	§ 56
Ermächtigung zum Erlass von Rechtsverordnungen	**Ermächtigung zum Erlass von Rechtsverordnungen**
(1) Das Bundesministerium des Innern und für Heimat bestimmt 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 § 52 und deren Inhalt.	(1) Das Bundesministerium des Innern und für Heimat bestimmt nach Anhörung der betroffenen Wirtschaftsverbände sowie Vertretern der Wissenschaft 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 § 52 und deren Inhalt.
(2) Das Bundesministerium des Innern und für Heimat bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, im Einvernehmen mit dem Bundesministerium für Wirtschaft und Klimaschutz und dem Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz die Einzelheiten der Gestaltung, des Inhalts und der Verwendung des IT-Sicherheitskennzeichens nach § 55, 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.	(2) Das Bundesministerium des Innern und für Heimat bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung der betroffenen Wirtschaftsverbände sowie Vertretern der Wissenschaft im Einvernehmen mit dem Bundesministerium für Wirtschaft und Klimaschutz und dem Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz die Einzelheiten der Gestaltung, des Inhalts und der Verwendung des IT-Sicherheitskennzeichens nach § 55, 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.

Entwurf	Beschlüsse des 4. Ausschusses
(3) Das Bundesministerium des Innern und für Heimat bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, im Einvernehmen mit dem Bundesministerium für Wirtschaft und Klimaschutz, dem Bundesministerium der Finanzen, dem Bundesministerium der Justiz, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium der Verteidigung, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Digitales und Verkehr, dem Bundesministerium für Bildung und Forschung und dem Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz, welche durch eine besonders wichtige Einrichtung oder eine wichtige Einrichtung eingesetzten Produkte, Dienste oder Prozesse gemäß § 30 Absatz 6 über eine Cybersicherheitszertifizierung verfügen müssen, da sie für die Erbringung der Dienste der Einrichtung maßgeblich sind und Art und Ausmaß der Risikoexposition der Einrichtung einen verpflichtenden Einsatz von zertifizierten Produkten, Diensten oder Prozessen in diesem Bereich erforderlich machen.	(3) Das Bundesministerium des Innern und für Heimat bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, im Einvernehmen mit dem Bundesministerium für Wirtschaft und Klimaschutz, dem Bundesministerium der Finanzen, dem Bundesministerium der Justiz, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium der Verteidigung, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Digitales und Verkehr, dem Bundesministerium für Bildung und Forschung und dem Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz, welche durch eine besonders wichtige Einrichtung oder eine wichtige Einrichtung eingesetzten Produkte, Dienste oder Prozesse gemäß § 30 Absatz 6 über eine Cybersicherheitszertifizierung verfügen müssen, da sie für die Erbringung der Dienste der Einrichtung maßgeblich sind und Art und Ausmaß der Risikoexposition der Einrichtung einen verpflichtenden Einsatz von zertifizierten Produkten, Diensten oder Prozessen in diesem Bereich erforderlich machen.

Entwurf	Beschlüsse des 4. Ausschusses
(4) Das Bundesministerium des Innern und für Heimat bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, im Einvernehmen mit dem Bundesministerium für Wirtschaft und Klimaschutz, dem Bundesministerium der Finanzen, dem Bundesministerium der Justiz, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium der Verteidigung, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Digitales und Verkehr und dem Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz unter Festlegung der in § 2 Nummer 24 genannten Sektoren wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrads, welche Anlagen als kritische Anlagen im Sinne dieses Gesetzes gelten. Der als bedeutend anzusehende Versorgungsgrad ist anhand branchenspezifischer Schwellenwerte für jede als kritisch anzusehende Dienstleistung zu bestimmen. Zugang zu Akten, die die Erstellung oder Änderung dieser Verordnung betreffen, wird nicht gewährt.	(4) 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 und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Klimaschutz, dem Bundesministerium der Finanzen, dem Bundesministerium der Justiz, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium der Verteidigung, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Digitales und Verkehr und dem Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz unter Festlegung der in § 2 Nummer 24 genannten Sektoren wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrads, welche Anlagen als kritische Anlagen im Sinne dieses Gesetzes gelten. Der als bedeutend anzusehende Versorgungsgrad ist anhand branchenspezifischer Schwellenwerte für jede als kritisch anzusehende Dienstleistung zu bestimmen. Zugang zu Akten, die die Erstellung oder Änderung dieser Verordnung betreffen, wird nicht gewährt.

Entwurf	Beschlüsse des 4. Ausschusses
(5) Das Bundesministerium des Innern und für Heimat kann im Einvernehmen mit dem mit dem Bundesministerium für Wirtschaft und Klimaschutz und im Benehmen mit 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 durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, bestimmen, wann ein Sicherheitsvorfall im Hinblick auf seine technischen oder organisatorischen Ursachen oder im Hinblick auf seine Auswirkungen auf die Einrichtung, den Staat, die Wirtschaft oder die Anzahl der von den Auswirkungen Betroffenen als erheblich im Sinne von § 2 Nummer 11 anzusehen ist. Das Bundesministerium kann diese Ermächtigung durch Rechtsverordnung auf das Bundesamt übertragen. Etwaige Durchführungsrechtsakte der Europäischen Kommission gemäß Artikel 23 Absatz 11 Unterabsatz 2 der NIS-2-Richtlinie, die die Voraussetzungen eines erheblichen Sicherheitsvorfalls bestimmen, gehen der Rechtsverordnung nach den Sätzen 1 und 2 insoweit vor.	(5) Das Bundesministerium des Innern und für Heimat kann im Einvernehmen mit dem mit dem Bundesministerium für Wirtschaft und Klimaschutz und im Benehmen mit 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 durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung von Vertretern der Wissenschaft und der betroffenen Wirtschaftsverbände bestimmen, wann ein Sicherheitsvorfall im Hinblick auf seine technischen oder organisatorischen Ursachen oder im Hinblick auf seine Auswirkungen auf die Einrichtung, den Staat, die Wirtschaft oder die Anzahl der von den Auswirkungen Betroffenen als erheblich im Sinne von § 2 Nummer 11 anzusehen ist. Das Bundesministerium kann diese Ermächtigung durch Rechtsverordnung auf das Bundesamt übertragen. Etwaige Durchführungsrechtsakte der Europäischen Kommission gemäß Artikel 23 Absatz 11 Unterabsatz 2 der NIS-2-Richtlinie, die die Voraussetzungen eines erheblichen Sicherheitsvorfalls bestimmen, gehen der Rechtsverordnung nach den Sätzen 1 und 2 insoweit vor.
(6) Das Bundesministerium des Innern und für Heimat kann durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, im Einvernehmen mit dem Bundesministerium für Gesundheit bestimmen, dass das Bundesamt gegenüber zugelassenen Krankenhäusern nach § 108 des Fünften Buches Sozialgesetzbuch zu einem früheren als dem in § 61 Absatz 3 Satz 5 genannten Zeitpunkt die Vorlage von Nachweisen über die Erfüllung einzelner oder aller der in § 61 Absatz 1 genannten Verpflichtungen anordnen kann.	(6) Das Bundesministerium des Innern und für Heimat kann durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, im Einvernehmen mit dem Bundesministerium für Gesundheit bestimmen, dass das Bundesamt gegenüber zugelassenen Krankenhäusern nach § 108 des Fünften Buches Sozialgesetzbuch zu einem früheren als dem in § 61 Absatz 3 Satz 5 genannten Zeitpunkt die Vorlage von Nachweisen über die Erfüllung einzelner oder aller der in § 61 Absatz 1 genannten Verpflichtungen anordnen kann.

Entwurf	Beschlüsse des 4. Ausschusses
	(7) Das Bundesministerium des Innern und für Heimat kann durch Rechtsverordnungen, die nicht der Zustimmung des Bundesrates bedürfen, für jeweils ei-nen der in § 2 Nr. 24 aufgeführten Sektoren im Einvernehmen mit dem in § 41 Absatz 1 für den jeweiligen Sektor genannten Bundesministerium kritische Komponenten i.S.d. § 2 Nr. 23 bestimmen. In der Rechtsverordnung kann eine Komponente als kritische Komponente bestimmt werden, wenn
	1. es sich bei der Komponente um ein IKT-Produkt handelt,
	2. die Komponente in kritischen Anlagen eingesetzt wird,
	3. die Komponente eine kritische Funktion realisiert und
	4. eine Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit der Komponente zu einer Beeinträchtigung der Funktionsfähigkeit kriti-scher Anlagen oder zu anderen Beeinträchtigungen der öffentlichen Ordnung oder Sicherheit führen könnte.
	Die in § 41 Absatz 1 genannten Bundesministerien können dem Bundesministerium des Innern und für Heimat einen Vorschlag für den Erlass einer Rechtsverordnung nach Satz 1 vorlegen. Das Vorschlagsrecht betrifft nur den Sektor im Sinne des § 2 Nr. 24, für den das jeweilige Bundesministerium in § 41 Absatz 1 genannt wird.
§ 57	§ 57
Einschränkung von Grundrechten	**Einschränkung von Grundrechten**
Das Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) wird durch die §§ 7, 8, 9, 11, 12, 15 und 16 eingeschränkt.	Das Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) wird durch die §§ 7, 8, 9, 11, 12, 15 und 16 eingeschränkt.

Entwurf	Beschlüsse des 4. Ausschusses
§ 58	§ 58
Berichtspflichten des Bundesamtes	**Berichtspflichten des Bundesamtes**
(1) Das Bundesamt unterrichtet das Bundesministerium des Innern und für Heimat über seine Tätigkeit.	(1) Das Bundesamt unterrichtet das Bundesministerium des Innern und für Heimat über seine Tätigkeit.
(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. § 13 Absatz 2 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. § 13 Absatz 2 ist entsprechend anzuwenden.
(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.	(3) Das Bundesministerium des Innern und für Heimat unterrichtet kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres den zuständigen Ausschuss des Deutschen Bundestages über die Anwendung dieses Gesetzes, insbesondere auch über die Anwendung des § 1 Satz 4 sowie begründet zu Einzelweisungen von erheblicher Bedeutung an das Bundesamt. Es geht dabei auch auf die Fortentwicklung des maßgeblichen Unionsrechts ein.
(4) Das Bundesamt legt der Agentur der Europäischen Union für Cybersicherheit erstmals zum 18. Januar 2025 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 § 5 Absatz 2 und § 32 gemeldet wurden.	(4) Das Bundesamt legt der Agentur der Europäischen Union für Cybersicherheit erstmals zum 18. Januar 2025 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 § 5 Absatz 2 und § 32 gemeldet wurden.
(5) Das Bundesamt übermittelt erstmals zum 17. April 2025 und in der Folge alle zwei Jahre	(5) Das Bundesamt übermittelt erstmals zum 17. April 2025 und in der Folge alle zwei Jahre
1. der Europäischen Kommission und der Kooperationsgruppe nach Artikel 14 der NIS-2-Richtlinie für jeden Sektor und Teilsektor gemäß Anhang I oder II der NIS-2-Richtlinie die Anzahl der besonders wichtigen Einrichtungen und wichtigen Einrichtungen, die gemäß § 33 Absatz 1 registriert wurden, und	1. der Europäischen Kommission und der Kooperationsgruppe nach Artikel 14 der NIS-2-Richtlinie für jeden Sektor und Teilsektor gemäß Anhang I oder II der NIS-2-Richtlinie die Anzahl der besonders wichtigen Einrichtungen und wichtigen Einrichtungen, die gemäß § 33 Absatz 1 registriert wurden, und

Entwurf	Beschlüsse des 4. Ausschusses
2. der Europäischen Kommission sachdienliche Informationen über die Anzahl der kritischen Anlagen, über den Sektor und den Teilsektor gemäß Anhang I oder II der 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.	2. der Europäischen Kommission sachdienliche Informationen über die Anzahl der kritischen Anlagen, über den Sektor und den Teilsektor gemäß Anhang I oder II der 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.
Teil 7	Teil 7
Aufsicht	Aufsicht
§ 59	§ 59
Zuständigkeit des Bundesamtes	**Zuständigkeit des Bundesamtes**
Das Bundesamt ist zuständige Aufsichtsbehörde für die Einhaltung der Vorschriften in Teil 3	Das Bundesamt ist zuständige Aufsichtsbehörde für die Einhaltung der Vorschriften in Teil 3
1. durch wichtige und besonders wichtige Einrichtungen, die in der Bundesrepublik Deutschland niedergelassen sind,	1. durch wichtige und besonders wichtige Einrichtungen, die in der Bundesrepublik Deutschland niedergelassen sind,
2. durch Betreiber kritischer Anlagen, deren kritische Anlagen sich auf dem Hoheitsgebiet der Bundesrepublik Deutschland befinden, und	2. durch Betreiber kritischer Anlagen, deren kritische Anlagen sich auf dem Hoheitsgebiet der Bundesrepublik Deutschland befinden, und
3. durch Einrichtungen der Bundesverwaltung.	3. durch Einrichtungen der Bundesverwaltung.

Entwurf	Beschlüsse des 4. Ausschusses
§ 60	§ 60
Zentrale Zuständigkeit in der Europäischen Union für bestimmte Einrichtungsarten	**Zentrale Zuständigkeit in der Europäischen Union für bestimmte Einrichtungsarten**
(1) Abweichend von § 59 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 für Anbieter von 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 haben. Ist dies der Fall, so ist das Bundesamt für die Einrichtung in der gesamten Europäischen Union zentral zuständig.	(1) Abweichend von § 59 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 für Anbieter von 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 haben. Ist dies der Fall, so ist das Bundesamt für die Einrichtung in der gesamten Europäischen Union zentral zuständig.
(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.	(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.

Entwurf	Beschlüsse des 4. Ausschusses
(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, so ist sie verpflichtet, einen Vertreter zu benennen. Der Vertreter muss in einem Mitgliedstaat der Europäischen Union niedergelassen sein, in der die Einrichtung die Dienste anbietet. Ist der Vertreter in der Bundesrepublik Deutschland niedergelassen, ist das Bundesamt für die Einrichtung zuständig. Hat eine Einrichtung der in Absatz 1 Satz 1 genannten Einrichtungsart in der Europäischen Union keinen Vertreter im Sinne dieses Absatzes benannt, so kann das Bundesamt sich für die betreffende Einrichtung zuständig erklären.	(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, so ist sie verpflichtet, einen Vertreter zu benennen. Der Vertreter muss in einem Mitgliedstaat der Europäischen Union niedergelassen sein, in der die Einrichtung die Dienste anbietet. Ist der Vertreter in der Bundesrepublik Deutschland niedergelassen, ist das Bundesamt für die Einrichtung zuständig. Hat eine Einrichtung der in Absatz 1 Satz 1 genannten Einrichtungsart in der Europäischen Union keinen Vertreter im Sinne dieses Absatzes benannt, so kann das Bundesamt sich für die betreffende Einrichtung zuständig erklären.
(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.	(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.
(5) Hat das Bundesamt ein Amtshilfeersuchen eines anderen Mitgliedstaats der Europäischen Union zu einer Einrichtung der in Absatz 1 Satz 1 genannten Einrichtungsart erhalten, so ist das Bundesamt befugt, 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, eine informationstechnische Komponente oder einen informationstechnischen Prozess betreibt. Satz 1 gilt entsprechend bei Amtshilfeersuchen eines anderen Mitgliedstaats der Europäischen Union, der für eine Einrichtung in der gesamten Europäischen Union zuständig ist, wenn die Einrichtung in der Bundesrepublik Deutschland Dienste anbietet oder ein informationstechnisches System, eine informationstechnische Komponente oder einen informationstechnischen Prozess betreibt.	(5) Hat das Bundesamt ein Amtshilfeersuchen eines anderen Mitgliedstaats der Europäischen Union zu einer Einrichtung der in Absatz 1 Satz 1 genannten Einrichtungsart erhalten, so ist das Bundesamt befugt, 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, eine informationstechnische Komponente oder einen informationstechnischen Prozess betreibt. Satz 1 gilt entsprechend bei Amtshilfeersuchen eines anderen Mitgliedstaats der Europäischen Union, der für eine Einrichtung in der gesamten Europäischen Union zuständig ist, wenn die Einrichtung in der Bundesrepublik Deutschland Dienste anbietet oder ein informationstechnisches System, eine informationstechnische Komponente oder einen informationstechnischen Prozess betreibt.

Entwurf	Beschlüsse des 4. Ausschusses
§ 61	§ 61
Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtige Einrichtungen	**Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtige Einrichtungen**
(1) Das Bundesamt kann gegenüber einzelnen besonders wichtigen Einrichtungen anordnen, Audits, Prüfungen oder Zertifizierungen von unabhängigen Stellen zur Prüfung der Erfüllung der Verpflichtungen nach § 30 Absatz 1 Satz 1, auch in Verbindung mit § 31 Absatz 1 und 2 Satz 1 und § 32 Absatz 1 bis 3 sowie § 38 Absatz 3 durchführen zu lassen.	(1) Das Bundesamt kann gegenüber einzelnen besonders wichtigen Einrichtungen anordnen, Audits, Prüfungen oder Zertifizierungen von unabhängigen Stellen zur Prüfung der Erfüllung der Verpflichtungen nach § 30 Absatz 1 Satz 1, auch in Verbindung mit § 31 Absatz 1 und 2 Satz 1 und § 32 Absatz 1 bis 3 sowie § 38 Absatz 3 durchführen zu lassen.
(2) Das Bundesamt kann nach Anhörung der betroffenen Einrichtungen und Wirtschaftsverbände fachliche und organisatorische Anforderungen für die prüfenden Stellen festlegen. Die Festlegung nach Satz 1 erfolgt durch eine öffentliche Mitteilung auf der Internetseite des Bundesamtes.	(2) Das Bundesamt kann nach Anhörung der betroffenen Einrichtungen und Wirtschaftsverbände fachliche und organisatorische Anforderungen für die prüfenden Stellen festlegen. Die Festlegung nach Satz 1 erfolgt durch eine öffentliche Mitteilung auf der Internetseite des Bundesamtes.

Entwurf	Beschlüsse des 4. Ausschusses
(3) Das Bundesamt kann auch gegenüber anderen besonders wichtigen Einrichtungen frühestens drei Jahre nach Inkrafttreten dieses Gesetzes die Vorlage von Nachweisen über die Erfüllung einzelner oder aller der in Absatz 1 genannten Verpflichtungen anordnen. Soweit das Bundesamt von seinem Recht nach Absatz 1 Gebrauch gemacht hat, kann es hierbei auch die Übermittlung der Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel sowie die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen. Es kann bei Sicherheitsmängeln die Vorlage eines geeigneten Mängelbeseitigungsplans im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder der sonst zuständigen Aufsichtsbehörde verlangen. Das Bundesamt kann die Vorlage eines geeigneten Nachweises über die erfolgte Mängelbeseitigung verlangen. Abweichend von Satz 1 kann das Bundesamt gegenüber zugelassenen Krankenhäusern nach § 108 des Fünften Buches Sozialgesetzbuch frühestens fünf Jahre nach Inkrafttreten dieses Gesetzes die Vorlage von Nachweisen über die Erfüllung einzelner oder aller der in Absatz 1 genannten Verpflichtungen anordnen, soweit nicht durch Rechtsverordnung nach § 56 Absatz 6 ein früherer Zeitpunkt bestimmt wird.	(3) Das Bundesamt kann auch gegenüber anderen besonders wichtigen Einrichtungen frühestens drei Jahre nach Inkrafttreten dieses Gesetzes die Vorlage von Nachweisen über die Erfüllung einzelner oder aller der in Absatz 1 genannten Verpflichtungen anordnen. Soweit das Bundesamt von seinem Recht nach Absatz 1 Gebrauch gemacht hat, kann es hierbei auch die Übermittlung der Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel sowie die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen. Es kann bei Sicherheitsmängeln die Vorlage eines geeigneten Mängelbeseitigungsplans im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder der sonst zuständigen Aufsichtsbehörde verlangen. Das Bundesamt kann die Vorlage eines geeigneten Nachweises über die erfolgte Mängelbeseitigung verlangen. Abweichend von Satz 1 kann das Bundesamt gegenüber zugelassenen Krankenhäusern nach § 108 des Fünften Buches Sozialgesetzbuch frühestens fünf Jahre nach Inkrafttreten dieses Gesetzes die Vorlage von Nachweisen über die Erfüllung einzelner oder aller der in Absatz 1 genannten Verpflichtungen anordnen, soweit nicht durch Rechtsverordnung nach § 56 Absatz 6 ein früherer Zeitpunkt bestimmt wird.
(4) Bei der Auswahl, von welchen Einrichtungen das Bundesamt nach Absatz 3 Nachweise anfordert, berücksichtigt das Bundesamt das Ausmaß der Risikoexposition, die Größe der Einrichtung sowie die Eintrittswahrscheinlichkeit und Schwere von möglichen Sicherheitsvorfällen sowie ihre möglichen gesellschaftlichen und wirtschaftlichen Auswirkungen.	(4) Bei der Auswahl, von welchen Einrichtungen das Bundesamt nach Absatz 3 Nachweise anfordert, berücksichtigt das Bundesamt das Ausmaß der Risikoexposition, die Größe der Einrichtung sowie die Eintrittswahrscheinlichkeit und Schwere von möglichen Sicherheitsvorfällen sowie ihre möglichen gesellschaftlichen und wirtschaftlichen Auswirkungen.

Entwurf	Beschlüsse des 4. Ausschusses
(5) 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 besonders wichtigen Einrichtung nur, sofern das Bundesamt auf Grund von Anhaltspunkten tätig geworden ist, die berechtigte Zweifel an der Einhaltung der Anforderungen nach § 30 Absatz 1 begründeten.	(5) 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 besonders wichtigen Einrichtung nur, sofern das Bundesamt auf Grund von Anhaltspunkten tätig geworden ist, die berechtigte Zweifel an der Einhaltung der Anforderungen nach § 30 Absatz 1 begründeten.
(6) Das Bundesamt kann gegenüber besonders wichtigen Einrichtungen im Benehmen mit der zuständigen Aufsichtsbehörde zur Verhütung oder Behebung eines Sicherheitsvorfalls oder eines Mangels erforderliche Maßnahmen nach § 30 Absatz 1 Satz 1 sowie die Vorlage eines geeigneten Mängelbeseitigungsplanes und eines geeigneten Nachweises über die erfolgte Mängelbeseitigung anordnen. Ein Benehmen mit der zuständigen Aufsichtsbehörde kann entfallen, sofern Gefahr im Verzug besteht. Ferner kann das Bundesamt die Berichterstattung zu den nach Satz 1 angeordneten Maßnahmen innerhalb einer angemessenen Frist verlangen.	(6) Das Bundesamt kann gegenüber besonders wichtigen Einrichtungen im Benehmen mit der zuständigen Aufsichtsbehörde zur Verhütung oder Behebung eines Sicherheitsvorfalls oder eines Mangels erforderliche Maßnahmen nach § 30 Absatz 1 Satz 1 sowie die Vorlage eines geeigneten Mängelbeseitigungsplanes und eines geeigneten Nachweises über die erfolgte Mängelbeseitigung anordnen. Ein Benehmen mit der zuständigen Aufsichtsbehörde kann entfallen, sofern Gefahr im Verzug besteht. Ferner kann das Bundesamt die Berichterstattung zu den nach Satz 1 angeordneten Maßnahmen innerhalb einer angemessenen Frist verlangen.
(7) Das Bundesamt kann gegenüber besonders wichtigen Einrichtungen im Benehmen mit der zuständigen Aufsichtsbehörde Anordnungen zur Umsetzung der in Absatz 1 genannten Verpflichtungen erlassen. Ein Benehmen mit der zuständigen Aufsichtsbehörde kann entfallen, sofern Gefahr im Verzug besteht. Es kann die Umsetzung von im Rahmen einer Sicherheitsprüfung formulierten konkreten Empfehlungen im Einzelfall innerhalb einer angemessenen Frist anordnen.	(7) Das Bundesamt kann gegenüber besonders wichtigen Einrichtungen im Benehmen mit der zuständigen Aufsichtsbehörde Anordnungen zur Umsetzung der in Absatz 1 genannten Verpflichtungen erlassen. Ein Benehmen mit der zuständigen Aufsichtsbehörde kann entfallen, sofern Gefahr im Verzug besteht. Es kann die Umsetzung von im Rahmen einer Sicherheitsprüfung formulierten konkreten Empfehlungen im Einzelfall innerhalb einer angemessenen Frist anordnen.

Entwurf	Beschlüsse des 4. Ausschusses
(8) Das Bundesamt kann gegenüber besonders wichtigen Einrichtungen anordnen,	(8) Das Bundesamt kann gegenüber besonders wichtigen Einrichtungen anordnen,
1. 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 diese Personen als Reaktion auf die Bedrohung ergreifen können, und	1. 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 diese Personen als Reaktion auf die Bedrohung ergreifen können, und
2. Informationen zu Verstößen gegen die in Absatz 1 genannten Verpflichtungen nach durch das Bundesamt bestimmten Vorgaben öffentlich bekannt zu machen.	2. Informationen zu Verstößen gegen die in Absatz 1 genannten Verpflichtungen nach durch das Bundesamt bestimmten Vorgaben öffentlich bekannt zu machen.
(9) Sofern besonders wichtige Einrichtungen den Anordnungen des Bundesamtes nach diesem Gesetz trotz Fristsetzung nicht nachkommen, kann das Bundesamt dies der jeweils zuständigen Aufsichtsbehörde mitteilen. Die zuständige Aufsichtsbehörde kann, wenn ein Zusammenhang zwischen Durchsetzungsmaßnahme und Anordnung besteht, als letztes Mittel	(9) Sofern besonders wichtige Einrichtungen den Anordnungen des Bundesamtes nach diesem Gesetz trotz Fristsetzung nicht nachkommen, kann das Bundesamt dies der jeweils zuständigen Aufsichtsbehörde mitteilen. Die zuständige Aufsichtsbehörde kann, wenn ein Zusammenhang zwischen Durchsetzungsmaßnahme und Anordnung besteht, als letztes Mittel
1. die dieser Einrichtung erteilte Genehmigung nach dem jeweiligen Fachrecht vorübergehend ganz oder teilweise aussetzen und	1. die dieser Einrichtung erteilte Genehmigung nach dem jeweiligen Fachrecht vorübergehend ganz oder teilweise aussetzen und
2. unzuverlässigen Geschäftsleitungen die Ausübung der Tätigkeit, zu der sie berufen sind (§ 2 Nummer 13), vorübergehend untersagen.	2. unzuverlässigen Geschäftsleitungen die Ausübung der Tätigkeit, zu der sie berufen sind (§ 2 Nummer 13), vorübergehend untersagen.
Die Aussetzung nach Satz 2 Nummer 1 und die Untersagung nach Satz 2 Nummer 2 sind nur solange zulässig, bis die besonders wichtige Einrichtung den Anordnungen des Bundesamtes nachkommt, wegen deren Nichtbefolgung sie ausgesprochen wurden.	Die Aussetzung nach Satz 2 Nummer 1 und die Untersagung nach Satz 2 Nummer 2 sind nur solange zulässig, bis die besonders wichtige Einrichtung den Anordnungen des Bundesamtes nachkommt, wegen deren Nichtbefolgung sie ausgesprochen wurden.

Entwurf	Beschlüsse des 4. Ausschusses
(10) Soweit das Bundesamt Maßnahmen gegenüber besonders wichtigen Einrichtungen durchführt, informiert es die zuständige Aufsichtsbehörde des Bundes darüber. Die Information hat unverzüglich zu erfolgen, wenn es sich um Maßnahmen nach Absatz 6 oder 7 handelt, die wegen Gefahr im Verzug ohne Benehmen der zuständigen Aufsichtsbehörde ergangen sind.	(10) Soweit das Bundesamt Maßnahmen gegenüber besonders wichtigen Einrichtungen durchführt, informiert es die zuständige Aufsichtsbehörde des Bundes darüber. Die Information hat unverzüglich zu erfolgen, wenn es sich um Maßnahmen nach Absatz 6 oder 7 handelt, die wegen Gefahr im Verzug ohne Benehmen der zuständigen Aufsichtsbehörde ergangen sind.
(11) Stellt das Bundesamt im Zuge der Beaufsichtigung einer Einrichtung oder Durchsetzung einer Maßnahme fest, dass ein Verstoß gegen die Verpflichtungen dieses Gesetzes eine offensichtliche Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Nummer 12 der Verordnung (EU) 2016/679 zur Folge hat, die gemäß Artikel 33 dieser Verordnung zu melden ist, unterrichtet es unverzüglich die zuständigen Aufsichtsbehörden.	(11) Stellt das Bundesamt im Zuge der Beaufsichtigung einer Einrichtung oder Durchsetzung einer Maßnahme fest, dass ein Verstoß gegen die Verpflichtungen dieses Gesetzes eine Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Nummer 12 der Verordnung (EU) 2016/679 zur Folge haben kann, die gemäß Artikel 33 dieser Verordnung zu melden ist, unterrichtet es unverzüglich die zuständigen Aufsichtsbehörden.
(12) Bei Einrichtungen, die in anderen Mitgliedstaaten der Europäischen Union Dienste erbringen, kann das Bundesamt auch auf Ersuchen der jeweils zuständigen Aufsichtsbehörden des Mitgliedstaats Maßnahmen nach den Absätzen 1 bis 11 ergreifen.	(12) Bei Einrichtungen, die in anderen Mitgliedstaaten der Europäischen Union Dienste erbringen, kann das Bundesamt auch auf Ersuchen der jeweils zuständigen Aufsichtsbehörden des Mitgliedstaats Maßnahmen nach den Absätzen 1 bis 11 ergreifen.
§ 62	§ 62
Aufsichts- und Durchsetzungsmaßnahmen für wichtige Einrichtungen	**Aufsichts- und Durchsetzungsmaßnahmen für wichtige Einrichtungen**
Rechtfertigen Tatsachen die Annahme, dass eine wichtige Einrichtung Verpflichtungen nach § 30 Absatz 1 Satz 1, § 32 Absatz 1 bis 3 und § 38 Absatz 3 nicht oder nicht richtig umsetzt, so kann das Bundesamt deren Einhaltung überprüfen und Maßnahmen nach § 61 treffen.	Rechtfertigen Tatsachen die Annahme, dass eine wichtige Einrichtung Verpflichtungen nach § 30 Absatz 1 Satz 1, § 32 Absatz 1 bis 3 und § 38 Absatz 3 nicht oder nicht richtig umsetzt, so kann das Bundesamt deren Einhaltung überprüfen und Maßnahmen nach § 61 treffen.
§ 63	§ 63
Verwaltungszwang	**Verwaltungszwang**
Sofern das Bundesamt Zwangsgelder verhängt, beträgt deren Höhe abweichend von § 11 Absatz 3 des Verwaltungsvollstreckungsgesetzes bis zu 100 000 Euro.	Sofern das Bundesamt Zwangsgelder verhängt, beträgt deren Höhe abweichend von § 11 Absatz 3 des Verwaltungsvollstreckungsgesetzes bis zu 100 000 Euro.

Entwurf	Beschlüsse des 4. Ausschusses
§ 64	§ 64
Zuwiderhandlungen durch Institutionen der sozialen Sicherung	**Zuwiderhandlungen durch Institutionen der sozialen Sicherung**
Bei Zuwiderhandlungen gegen eine in § 65 Absatz 1 bis 4 genannte Vorschrift, die von 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 § 65 Absatz 1 bis 4 genannte Vorschrift, die von 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.
Teil 8	Teil 8
Bußgeldvorschriften	Bußgeldvorschriften
§ 65	§ 65
Bußgeldvorschriften	**Bußgeldvorschriften**
(1) Ordnungswidrig handelt, wer entgegen § 39 Absatz 1 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 56 Absatz 4 Satz 1 einen Nachweis nicht richtig oder nicht vollständig erbringt.	(1) Ordnungswidrig handelt, wer entgegen § 39 Absatz 1 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 56 Absatz 4 Satz 1 einen Nachweis nicht richtig oder nicht vollständig erbringt.
(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig	(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig
1. einer vollziehbaren Anordnung nach	1. einer vollziehbaren Anordnung nach
a) § 11 Absatz 6, § 16 Absatz 1 Satz 1, auch in Verbindung mit § 16 Absatz 3, § 17 Satz 1, oder § 39 Absatz 1 Satz 5,	a) § 11 Absatz 6, § 16 Absatz 1 Satz 1, auch in Verbindung mit § 16 Absatz 3, § 17 Satz 1, oder § 39 Absatz 1 Satz 5,

Entwurf	Beschlüsse des 4. Ausschusses
b) § 14 Absatz 2 Satz 1,	b) § 14 Absatz 2 Satz 1,
c) den §§ 18, 40 Absatz 5 Satz 1 oder nach § 61 Absatz 3 Satz 1 oder Absatz 6 Satz 1 oder 3 oder Absatz 7 Satz 1 oder 3 oder Absatz 8, jeweils auch in Verbindung mit § 62, oder	c) den §§ 18, § 40 Absatz 5 Satz 1 oder nach § 61 Absatz 3 Satz 1 oder Absatz 6 Satz 1 oder 3 oder Absatz 7 Satz 1 oder 3 oder Absatz 8, jeweils auch in Verbindung mit § 62, oder
d) § 35 Absatz 1 Satz 1 oder § 36 Absatz 2 Satz 1,	d) § 35 Absatz 1 Satz 1 oder § 36 Absatz 2 Satz 1,
zuwiderhandelt,	zuwiderhandelt,
2. entgegen § 30 Absatz 1 Satz 1 eine dort genannte Maßnahme nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig ergreift,	2. entgegen § 30 Absatz 1 Satz 1 eine dort genannte Maßnahme nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig ergreift,
3. entgegen § 30 Absatz 1 Satz 3 die Einhaltung der Verpflichtung nicht, nicht richtig oder nicht vollständig dokumentiert,	3. entgegen § 30 Absatz 1 Satz 3 die Einhaltung der Verpflichtung nicht, nicht richtig oder nicht vollständig dokumentiert,
4. entgegen § 32 Absatz 1 Satz 1 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,	4. entgegen § 32 Absatz 1 Satz 1 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,
5. entgegen § 32 Absatz 2 Satz 2 eine Abschlussmeldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vorlegt,	5. entgegen § 32 Absatz 2 Satz 2 eine Abschlussmeldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vorlegt,
6. entgegen § 33 Absatz 1 oder 2 Satz 1, jeweils auch in Verbindung mit einer Rechtsverordnung nach § 56 Absatz 4 Satz 1, oder entgegen § 34 Absatz 1 eine Angabe nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt,	6. entgegen § 33 Absatz 1 oder 2 Satz 1, jeweils auch in Verbindung mit einer Rechtsverordnung nach § 56 Absatz 4 Satz 1, oder entgegen § 34 Absatz 1 eine Angabe nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt,
7. entgegen § 33 Absatz 2 Satz 2 nicht sicherstellt, dass er erreichbar ist,	7. entgegen § 33 Absatz 2 Satz 2 nicht sicherstellt, dass er erreichbar ist,
8. entgegen § 34 Absatz 2 das Bundesamt nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet,	8. entgegen § 34 Absatz 2 das Bundesamt nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet,
9. entgegen § 35 Absatz 2 Satz 1, auch in Verbindung mit Satz 2, eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,	9. entgegen § 35 Absatz 2 Satz 1, auch in Verbindung mit Satz 2, eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

Entwurf	Beschlüsse des 4. Ausschusses
10. entgegen § 39 Absatz 1 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 56 Absatz 4 Satz 1 einen Nachweis nicht oder nicht rechtzeitig erbringt,	10. entgegen § 39 Absatz 1 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 56 Absatz 4 Satz 1 einen Nachweis nicht oder nicht rechtzeitig erbringt,
	11. entgegen § 41 Absatz 5 nicht an der Ermittlung des Sachverhaltes mitwirkt.
11. entgegen § 49 Absatz 3 Satz 1 eine dort genannte Vorgabe oder ein dort genanntes Verfahren nicht vorhält,	12. entgegen § 49 Absatz 3 Satz 1 eine dort genannte Vorgabe oder ein dort genanntes Verfahren nicht vorhält,
12. entgegen § 49 Absatz 3 Satz 2 oder Absatz 4 eine dort genannte Vorgabe, ein dort genanntes Verfahren oder Daten nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig zugänglich macht,	13. entgegen § 49 Absatz 3 Satz 2 oder Absatz 4 eine dort genannte Vorgabe, ein dort genanntes Verfahren oder Daten nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig zugänglich macht,
13. entgegen § 50 Absatz 1 Satz 1 einen Zugang nicht oder nicht rechtzeitig gewährt,	14. entgegen § 50 Absatz 1 Satz 1 einen Zugang nicht oder nicht rechtzeitig gewährt,
14. entgegen § 52 Absatz 2 Satz 4, § 53 Absatz 1 Satz 4, § 54 Absatz 6 Satz 2 oder § 55 Absatz 4 Satz 1 ein dort genanntes Zertifikat, eine dort genannte Erklärung oder ein dort genanntes Kennzeichen verwendet,	15. entgegen § 52 Absatz 2 Satz 4, § 53 Absatz 1 Satz 4, § 54 Absatz 6 Satz 2 oder § 55 Absatz 4 Satz 1 ein dort genanntes Zertifikat, eine dort genannte Erklärung oder ein dort genanntes Kennzeichen verwendet,
15. entgegen § 53 Absatz 3 Satz 2 oder § 54 Absatz 2 Satz 2 tätig wird oder	16. entgegen § 53 Absatz 3 Satz 2 oder § 54 Absatz 2 Satz 2 tätig wird oder
16. entgegen § 61 Absatz 5 Satz 3 das Betreten eines dort genannten Raums nicht gestattet, eine dort genannte Aufzeichnung, ein dort genanntes Schriftstück oder eine dort genannte Unterlage nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vorlegt oder eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt.	17. entgegen § 61 Absatz 5 Satz 3 das Betreten eines dort genannten Raums nicht gestattet, eine dort genannte Aufzeichnung, ein dort genanntes Schriftstück oder eine dort genannte Unterlage nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vorlegt oder eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt.
(3) Ordnungswidrig handelt, wer eine in Absatz 1 bezeichnete Handlung fahrlässig begeht.	(3) Ordnungswidrig handelt, wer eine in Absatz 1 bezeichnete Handlung fahrlässig begeht.

Entwurf	Beschlüsse des 4. Ausschusses
(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 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	(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 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
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
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 Sicherheitslücke oder Unregelmäßigkeit gibt.
(5) Die Ordnungswidrigkeit kann geahndet werden:	(5) Die Ordnungswidrigkeit kann geahndet werden:
1. in den Fällen des Absatzes 2 Nummer 1 Buchstabe d, Nummer 2 bis 5 und 9,	1. in den Fällen des Absatzes 2 Nummer 1 Buchstabe d, Nummer 2 bis 5 und 9,
a) bei besonders wichtigen Einrichtungen nach § 28 Absatz 1 Satz 1 mit einer Geldbuße bis zu zehn Millionen Euro,	a) bei besonders wichtigen Einrichtungen nach § 28 Absatz 1 Satz 1 mit einer Geldbuße bis zu zehn Millionen Euro,
b) bei wichtigen Einrichtungen im Sinne des § 28 Absatz 2 Satz 1 mit einer Geldbuße bis zu sieben Millionen Euro,	b) bei wichtigen Einrichtungen im Sinne des § 28 Absatz 2 Satz 1 mit einer Geldbuße bis zu sieben Millionen Euro,
2. in den Fällen des Absatzes 2 Nummer 1 Buchstabe a mit einer Geldbuße bis zu zwei Millionen Euro,	2. in den Fällen des Absatzes 2 Nummer 1 Buchstabe a mit einer Geldbuße bis zu zwei Millionen Euro,
3. in den Fällen der Absätze 1 und 2 Nummer 10 mit einer Geldbuße bis zu einer Million Euro,	3. in den Fällen der Absatzes 1 und 2 Nummer 10 mit einer Geldbuße bis zu einer Million Euro,
4. in den Fällen des Absatzes 2 Nummer 1 Buchstabe c, Nummer 6, 8, 11 bis 15 und des Absatzes 4 mit einer Geldbuße bis zu fünfhunderttausend Euro und	4. in den Fällen des Absatzes 2 Nummer 1 Buchstabe c, Nummer 6, 8, 12 bis 16 und des Absatzes 4 mit einer Geldbuße bis zu fünfhunderttausend Euro und

Entwurf	Beschlüsse des 4. Ausschusses
5. in den Fällen des Absatzes 2 Nummer 1 Buchstabe b, Nummer 7 und 16 und des Absatzes 3 mit einer Geldbuße bis zu hunderttausend Euro.	5. in den Fällen des Absatzes 2 Nummer 1 Buchstabe b, Nummer 7 und 17 und des Absatzes 3 mit einer Geldbuße bis zu hunderttausend Euro,
	6. in den Fällen des Absatzes 2 Nr. 11 mit einer Geldbuße bis zu zehn Millionen Euro.
In den Fällen des Satzes 1 Nummer 2 und 3 ist § 30 Absatz 2 Satz 3 des Gesetzes über Ordnungswidrigkeiten anzuwenden.	In den Fällen des Satzes 1 Nummer 2 und 3 ist § 30 Absatz 2 Satz 3 des Gesetzes über Ordnungswidrigkeiten anzuwenden.
(6) Bei einer besonders wichtigen Einrichtung im Sinne des § 28 Absatz 1 Satz 1 mit einem Jahresumsatz von mehr als 500 Millionen Euro kann abweichend von Absatz 5 Satz 1 Nummer 1 Buchstabe a eine Ordnungswidrigkeit in den Fällen des Absatzes 2 Nummer 1 Buchstabe d, Nummer 2 bis 5 und 9 mit einer Geldbuße bis zu 2 Prozent des Jahresumsatzes geahndet werden.	(6) Bei einer besonders wichtigen Einrichtung im Sinne des § 28 Absatz 1 Satz 1 mit einem Jahresumsatz von mehr als 500 Millionen Euro kann abweichend von Absatz 5 Satz 1 Nummer 1 Buchstabe a eine Ordnungswidrigkeit in den Fällen des Absatzes 2 Nummer 1 Buchstabe d, Nummer 2 bis 5 und 9 mit einer Geldbuße bis zu 2 Prozent des Jahresumsatzes geahndet werden.
(7) Bei einer wichtigen Einrichtung im Sinne des § 28 Absatz 2 Satz 1 mit einem Jahresumsatz von mehr als 500 Millionen Euro kann abweichend von Absatz 5 Nummer 1 Buchstabe b eine Ordnungswidrigkeit in den Fällen des Absatzes 2 Nummer 1 Buchstabe d, Nummer 2 bis 5 und 9 mit einer Geldbuße bis zu 1,4 Prozent des Jahresumsatzes geahndet werden.	(7) Bei einer wichtigen Einrichtung im Sinne des § 28 Absatz 2 Satz 1 mit einem Jahresumsatz von mehr als 500 Millionen Euro kann abweichend von Absatz 5 Nummer 1 Buchstabe b eine Ordnungswidrigkeit in den Fällen des Absatzes 2 Nummer 1 Buchstabe d, Nummer 2 bis 5 und 9 mit einer Geldbuße bis zu 1,4 Prozent des Jahresumsatzes geahndet werden.
(8) Der Jahresumsatz im Sinne der Absätze 6 und 7 ist der gesamte weltweit getätigte Umsatz des Unternehmens, dem die besonders wichtige Einrichtung oder die wichtige Einrichtung angehört, der in dem Geschäftsjahr erzielt wurde, das dem Verstoß vorangeht.	(8) Der Jahresumsatz im Sinne der Absätze 6 und 7 ist der gesamte weltweit getätigte Umsatz des Unternehmens, dem die besonders wichtige Einrichtung oder die wichtige Einrichtung angehört, der in dem Geschäftsjahr erzielt wurde, das dem Verstoß vorangeht.
(9) Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist das Bundesamt.	(9) Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist das Bundesamt. Abweichend von Satz 1 ist für Ordnungswidrigkeiten nach Absatz 2 Nummer 11 Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten das Bundesministerium des Innern und für Heimat.

Entwurf	Beschlüsse des 4. Ausschusses
(10) Verhängen die in Artikel 55 oder 56 der Verordnung (EU) 2016/679 genannten Aufsichtsbehörden gemäß Artikel 58 Absatz 2 Buchstabe i der Verordnung (EU) 2016/679 eine Geldbuße, so darf eine weitere Geldbuße für einen Verstoß nach diesem Gesetz, der sich aus demselben Verhalten ergibt wie jener Verstoß, der Gegenstand der Geldbuße nach Artikel 58 Absatz 2 Buchstabe i der Verordnung (EU) 2016/679 war, nicht verhängt werden.	(10) Verhängen die in Artikel 55 oder 56 der Verordnung (EU) 2016/679 genannten Aufsichtsbehörden gemäß Artikel 58 Absatz 2 Buchstabe i der Verordnung (EU) 2016/679 eine Geldbuße, so darf eine weitere Geldbuße für einen Verstoß nach diesem Gesetz, der sich aus demselben Verhalten ergibt wie jener Verstoß, der Gegenstand der Geldbuße nach Artikel 58 Absatz 2 Buchstabe i der Verordnung (EU) 2016/679 war, nicht verhängt werden.

Entwurf	Beschlüsse des 4. Ausschusses
Anlage 1	**Anlage 1**
Sektoren besonders wichtiger und wichtiger Einrichtungen	**Sektoren besonders wichtiger und wichtiger Einrichtungen**

Entwurf

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
1	**Energie**		
1.1		Stromversorgung	
1.1.1			Stromlieferanten nach § 3 Nummer 31c EnWG
1.1.2			Betreiber von Elektrizitätsverteilernetzen nach § 3 Nummer 3 EnWG
1.1.3			Betreiber von Übertragungsnetzen nach § 3 Nummer 10 EnWG
1.1.4			Betreiber von Erzeugungsanlagen nach § 3 Nummer 18d EnWG
1.1.5			Nominierte Strommarktbetreiber nach Artikel 2 Nummer 8 der Verordnung (EU) 2019/943 des Europäischen Parlaments und des Rates vom 5 Juni 2019 über den Elektrizitätsbinnenmarkt (ABl. L 158 vom 14.6.2019, S. 54)
1.1.6			Aggregatoren nach § 3 Nummer 1a EnWG
1.1.7			Betreiber von Energiespeicheranlagen nach § 3 Nummer 15d EnWG
1.1.8			Anbieter von Ausgleichsleistungen nach § 3 Nummer 1b EnWG
1.1.9			Ladepunktbetreiber nach § 2 Nummer 8 LSV
1.2		Fernwärmeversorgung oder Fernkältekälteversorgung	
1.2.1			Betreiber von Fernwärme- oder Fernkälteversorgung im Sinne von § 3 Nummer 19 oder Nummer 20 GEG
1.3		Kraftstoff- und Heizölversorgung	
1.3.1			Betreiber von Erdöl-Fernleitungen
1.3.2			Betreiber von Anlagen zur Produktion, Raffination und Aufbereitung von Erdöl sowie Betreiber von Erdöllagern und Erdöl-Fernleitungen
1.3.3			Zentrale Bevorratungsstellen nach Artikel 2 Buchstabe f der Richtlinie 2009/119/EG des Rates vom 14. September 2009 zur Verpflichtung der Mitgliedstaaten, Mindestvorräte an Erdöl und/oder Erdölerzeugnissen zu halten (ABl. L 265 vom 9.10.2009, S. 9)
1.4		Gasversorgung	

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
1.4.1			Betreiber von Gasverteilernetzen nach § 3 Nummer 8 EnWG
1.4.2			Betreiber von Fernleitungsnetzen nach § 3 Nummer 5 EnWG
1.4.3			Betreiber von Gasspeicheranlagen nach § 3 Nummer 6 EnWG
1.4.4			Betreiber von LNG-Anlagen nach § 3 Nummer 9 EnWG
1.4.5			Gaslieferanten nach § 3 Nummer 19b EnWG
1.4.6			Betreiber von Anlagen zur Gewinnung von Erdgas
1.4.7			Betreiber von Anlagen zur Raffination und Aufbereitung von Erdgas
1.4.8			Betreiber im Bereich Wasserstofferzeugung, -speicherung und -fernleitung
2	**Transport und Verkehr**		
2.1		Luftverkehr	
2.1.1			Luftfahrtunternehmen nach Artikel 3 Nummer 4 der Verordnung (EG) Nr. 300/2008 des Europäischen Parlaments und des Rates vom 11. März 2008 über gemeinsame Vorschriften für die Sicherheit in der Zivilluftfahrt und zur Aufhebung der Verordnung (EG) Nr. 2320/2002 (ABl. L 97 vom 9.4.2008, S. 72), die für gewerbliche Zwecke genutzt werden
2.1.2			Flughafenleitungsorgane nach Artikel 2 Nummer 2 der Richtlinie 2009/12/EG des Europäischen Parlaments und des Rates vom 11. März 2009 über Flughafenentgelte (ABl. L 70 vom 14.3.2009, S. 11), Flughäfen nach Artikel 2 Nummer 1 jener Richtlinie, einschließlich der in Anhang II Abschnitt 2 der Verordnung (EU) Nr. 1315/2013 des Europäischen Parlaments und des Rates vom 11. Dezember 2013 über Leitlinien der Union für den Aufbau eines transeuropäischen Verkehrsnetzes und zur Aufhebung des Beschlusses Nr. 661/2010/EU (ABl. L 348, 20.12.2013, S. 1) aufgeführten Flughäfen des Kernnetzes, und Einrichtungen, die innerhalb von Flughäfen befindliche zugehörige Einrichtungen betreiben
2.1.3			Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen, die Flugverkehrskontrolldienste im Sinne von Artikel 2 Nummer 1 der Verordnung (EG) Nr. 549/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Festlegung des Rahmens für die Schaffung eines einheitlichen europäischen Luftraums (ABl. L 96 vom 31.3.2004, S. 1) bereitstellen
2.2		Schienenverkehr	
2.2.1			Betreiber von Eisenbahninfrastruktur nach § 2 Absatz 6 und 6a AEG einschließlich zentraler Einrichtungen, die den Zugbetrieb

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
			vorausschauend und bei unerwartet eintretenden Ereignissen disponiert
2.2.2			Eisenbahnverkehrsunternehmen nach § 2 Absatz 3 AEG, einschließlich Betreiber einer Serviceeinrichtung nach § 2 Nummer 9 AEG
2.3		Schifffahrt	
2.3.1			Passagier- und Frachtbeförderungsunternehmen der Binnen-, See- und Küstenschifffahrt, wie sie in Anhang I der Verordnung (EG) Nr. 725/2004 des Europäischen Parlaments und des Rates vom 31. März 2004 zur Erhöhung der Gefahrenabwehr auf Schiffen und in Hafenanlagen (ABl. L 129 vom 29.4.2004, S. 6) für die Schifffahrt definiert sind, ausschließlich der einzelnen von diesen Unternehmen betriebenen Schiffe
2.3.2			Leitungsorgane von Häfen nach Artikel 3 Nummer 1 der Richtlinie 2005/65/EG des Europäischen Parlaments und des Rates vom 26. Oktober 2005 zur Erhöhung der Gefahrenabwehr in Häfen (ABl. L 310 vom 25.11.2005, S. 28), einschließlich ihrer Hafenanlagen nach Artikel 2 Nummer 11 der Verordnung (EG) Nr. 725/2004, sowie Einrichtungen, die innerhalb von Häfen befindliche Anlagen und Ausrüstung betreiben
2.3.3			Betreiber einer Anlage oder eines Systems zum sicheren Betrieb einer Wasserstraße im Sinne von § 1 Absatz 6 Nummer 1 WaStrG
2.4		Straßenverkehr	
2.4.1			Betreiber einer Anlage oder eines System zur Verkehrsbeeinflussung im Straßenverkehr einschließlich der in § 1 Absatz 4 Nummer 1, 3 und 4 FStrG genannten Einrichtungen, zum Beispiel Verkehrs-, Betriebs- und Tunnelleitzentralen, Entwässerungsanlagen, intelligente Verkehrssysteme und Fachstellen für Informationstechnik und -sicherheit im Straßenbau, sowie der Telekommunikationsnetze der Bundesautobahnen
2.4.2			Betreiber eines intelligenten Verkehrssystems nach § 2 Nummer 1 IVSG.
3	**Finanzwesen**		
3.1		Bankwesen	
3.1.1			Kreditinstitute: Einrichtungen deren Tätigkeit darin besteht, Einlagen oder andere rückzahlbare Gelder des Publikums entgegenzunehmen und Kredite für eigene Rechnung zu gewähren
3.2		Finanzmarktinfrastrukturen	
3.2.1			Handelsplätze im Sinne von § 2 Absatz 22 WpHG
3.2.2			Zentrale Gegenparteien, die zwischen die Gegenparteien der auf einem Markt oder mehreren Märkten gehandelten Kontrakte

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
			tritt und somit als Käufer für jeden Verkäufer bzw. als Verkäufer für jeden Käufer fungiert
4	**Gesundheit**		
4.1.1			Erbringer von Gesundheitsdienstleistungen im Sinne der Richtlinie (EU) 2011/24 des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung (ABl. L 88 vom 4.4.2011, S. 45)
4.1.2			EU-Referenzlaboratorien nach Artikel 15 der Verordnung (EU) 2022/2371 des Europäischen Parlaments und des Rates vom 23. November 2022 zu schwerwiegenden grenzüberschreitenden Gesundheitsgefahren und zur Aufhebung des Beschlusses Nr. 1082/2013/EU (ABl. L 314 vom 6.12.2022, S. 26)
4.1.3			Unternehmen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel nach § 2 AMG ausüben
4.1.4			Unternehmen, die pharmazeutische Erzeugnisse nach Abschnitt C Abteilung 21 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) herstellen
4.1.5			Unternehmen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch nach Artikel 22 der Verordnung (EU) 2022/123 des Europäischen Parlaments und des Rates vom 25. Januar 2022 zu einer verstärkten Rolle der Europäischen Arzneimittel-Agentur bei der Krisenvorsorge und -bewältigung in Bezug auf Arzneimittel und Medizinprodukte (ABl. L 20 vom 31.1.2022, S. 1) („Liste kritischer Medizinprodukte für Notlagen im Bereich der öffentlichen Gesundheit“) eingestuft werden
5	**Wasser**		
5.1		Trinkwasserversorgung	
5.1.1			Betreiber von Wasserversorgunsanlagen im Sinne von § 2 Nummer 3 TrinkwV, jedoch unter Ausschluss der Lieferanten, für die die Lieferung von Wasser für den menschlichen Gebrauch ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit der Lieferung anderer Rohstoffe und Güter ist
5.2		Abwasserbeseitigung	
5.2.1			Unternehmen, die Abwasser nach § 2 Absatz 1 AbwAG sammeln, entsorgen oder behandeln, jedoch unter Ausschluss der Unternehmen, für die das Sammeln, die Entsorgung oder die Behandlung solchen Abwassers ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit ist.
6	**Digitale Infrastruktur**		
6.1.1			Betreiber von Internet Exchange Points

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
6.1.2			DNS-Dienstanbieter, ausgenommen Betreiber von Root-Nameservern
6.1.3			Top Level Domain Name Registry
6.1.4			Anbieter von Cloud-Computing-Diensten
6.1.5			Anbieter von Rechenzentrumsdiensten
6.1.6			Betreiber von Content Delivery Networks
6.1.7			Vertrauensdienstanbieter
6.1.8			Betreiber öffentlicher Telekommunikationsnetze
6.1.9			Anbieter öffentlich zugänglicher Telekommunikationsdienste
6.1.10			Managed Services Provider
6.1.11			Managed Security Services Provider
7	**Weltraum**		
7.1.1			Betreiber von Bodeninfrastrukturen, die sich im Eigentum von Mitgliedstaaten oder privaten Parteien befinden und von diesen verwaltet und betrieben werden und die Erbringung von weltraumgestützten Diensten unterstützen, ausgenommen Anbieter öffentlicher elektronischer Kommunikationsnetze

Beschlüsse des 4. Ausschusses

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
1	**Energie**		
1.1		Stromversorgung	
1.1.1			Stromlieferanten nach § 3 Nummer 31c EnWG
1.1.2			Betreiber von Elektrizitätsverteilernetzen nach § 3 Nummer 3 EnWG
1.1.3			Betreiber von Übertragungsnetzen nach § 3 Nummer 10 EnWG
1.1.4			Betreiber von Erzeugungsanlagen nach § 3 Nummer 18d EnWG
1.1.5			Nominierte Strommarktbetreiber nach Artikel 2 Nummer 8 der Verordnung (EU) 2019/943 des Europäischen Parlaments und des Rates vom 5 Juni 2019 über den Elektrizitätsbinnenmarkt (ABl. L 158 vom 14.6.2019, S. 54)
1.1.6			Aggregatoren nach § 3 Nummer 1a EnWG
1.1.7			Betreiber von Energiespeicheranlagen nach § 3 Nummer 15d EnWG
1.1.8			Anbieter von Ausgleichsleistungen nach § 3 Nummer 1b EnWG
1.1.9			Ladepunktbetreiber nach § 2 Nummer 8 LSV

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
1.2		Fernwärmeversorgung oder Fernkältekälteversorgung	
1.2.1			Betreiber von Fernwärme- oder Fernkälteversorgung im Sinne von § 3 Nummer 19 oder Nummer 20 GEG
1.3		Kraftstoff- und Heizölversorgung	
1.3.1			Betreiber von Erdöl-Fernleitungen
1.3.2			Betreiber von Anlagen zur Produktion, Raffination und Aufbereitung von Erdöl sowie Betreiber von Erdöllagern und Erdöl-Fernleitungen
1.3.3			Zentrale Bevorratungsstellen nach Artikel 2 Buchstabe f der Richtlinie 2009/119/EG des Rates vom 14. September 2009 zur Verpflichtung der Mitgliedstaaten, Mindestvorräte an Erdöl und/oder Erdölerzeugnissen zu halten (ABl. L 265 vom 9.10.2009, S. 9)
1.4		Gasversorgung	
1.4.1			Betreiber von Gasverteilernetzen nach § 3 Nummer 8 EnWG
1.4.2			Betreiber von Fernleitungsnetzen nach § 3 Nummer 5 EnWG
1.4.3			Betreiber von Gasspeicheranlagen nach § 3 Nummer 6 EnWG
1.4.4			Betreiber von LNG-Anlagen nach § 3 Nummer 9 EnWG
1.4.5			Gaslieferanten nach § 3 Nummer 19b EnWG
1.4.6			Betreiber von Anlagen zur Gewinnung von Erdgas
1.4.7			Betreiber von Anlagen zur Raffination und Aufbereitung von Erdgas
1.4.8			Betreiber im Bereich Wasserstofferzeugung, -speicherung und -fernleitung
2	**Transport und Verkehr**		
2.1		Luftverkehr	
2.1.1			Luftfahrtunternehmen nach Artikel 3 Nummer 4 der Verordnung (EG) Nr. 300/2008 des Europäischen Parlaments und des Rates vom 11. März 2008 über gemeinsame Vorschriften für die Sicherheit in der Zivilluftfahrt und zur Aufhebung der Verordnung (EG) Nr. 2320/2002 (ABl. L 97 vom 9.4.2008, S. 72), die für gewerbliche Zwecke genutzt werden
2.1.2			Flughafenleitungsorgane nach Artikel 2 Nummer 2 der Richtlinie 2009/12/EG des Europäischen Parlaments und des Rates vom 11. März 2009 über Flughafenentgelte (ABl. L 70 vom 14.3.2009, S. 11), Flughäfen nach Artikel 2 Nummer 1 jener Richtlinie, einschließlich der in Anhang II Abschnitt 2

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
			der Verordnung (EU) Nr. 1315/2013 des Europäischen Parlaments und des Rates vom 11. Dezember 2013 über Leitlinien der Union für den Aufbau eines transeuropäischen Verkehrsnetzes und zur Aufhebung des Beschlusses Nr. 661/2010/EU (ABl. L 348, 20.12.2013, S. 1) aufgeführten Flughäfen des Kernnetzes, und Einrichtungen, die innerhalb von Flughäfen befindliche zugehörige Einrichtungen betreiben
2.1.3			Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen, die Flugverkehrskontrolldienste im Sinne von Artikel 2 Nummer 1 der Verordnung (EG) Nr. 549/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Festlegung des Rahmens für die Schaffung eines einheitlichen europäischen Luftraums (ABl. L 96 vom 31.3.2004, S. 1) bereitstellen
2.2		Schienenverkehr	
2.2.1			Betreiber von Eisenbahninfrastruktur nach § 2 Absatz 6 und 6a AEG einschließlich zentraler Einrichtungen, die den Zugbetrieb vorausschauend und bei unerwartet eintretenden Ereignissen disponiert
2.2.2			Eisenbahnverkehrsunternehmen nach § 2 Absatz 3 AEG, einschließlich Betreiber einer Serviceeinrichtung nach § 2 Nummer 9 AEG
2.3		Schifffahrt	
2.3.1			Passagier- und Frachtbeförderungsunternehmen der Binnen-, See- und Küstenschifffahrt, wie sie in Anhang I der Verordnung (EG) Nr. 725/2004 des Europäischen Parlaments und des Rates vom 31. März 2004 zur Erhöhung der Gefahrenabwehr auf Schiffen und in Hafenanlagen (ABl. L 129 vom 29.4.2004, S. 6) für die Schifffahrt definiert sind, ausschließlich der einzelnen von diesen Unternehmen betriebenen Schiffe
2.3.2			Leitungsorgane von Häfen nach Artikel 3 Nummer 1 der Richtlinie 2005/65/EG des Europäischen Parlaments und des Rates vom 26. Oktober 2005 zur Erhöhung der Gefahrenabwehr in Häfen (ABl. L 310 vom 25.11.2005, S. 28), einschließlich ihrer Hafenanlagen nach Artikel 2 Nummer 11 der Verordnung (EG) Nr. 725/2004, sowie Einrichtungen, die innerhalb von Häfen befindliche Anlagen und Ausrüstung betreiben
2.3.3			Betreiber einer Anlage oder eines Systems zum sicheren Betrieb einer Wasserstraße im Sinne von § 1 Absatz 6 Nummer 1 WaStrG
2.4		Straßenverkehr	
2.4.1			Betreiber einer Anlage oder eines System zur Verkehrsbeeinflussung im Straßenverkehr einschließlich der in § 1 Absatz 4 Nummer 1, 3 und 4 FStrG genannten Einrichtungen, zum Beispiel Verkehrs-, Betriebs- und Tunnelleitzentralen, Entwässerungsanlagen,

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
			intelligente Verkehrssysteme und Fachstellen für Informationstechnik und -sicherheit im Straßenbau, sowie der Telekommunikationsnetze der Bundesautobahnen
2.4.2			Betreiber eines intelligentes Verkehrssystem nach § 2 Nummer 1 IVSG.
3	**Finanzwesen**		
3.1		Bankwesen	
3.1.1			Kreditinstitute: Einrichtungen deren Tätigkeit darin besteht, Einlagen oder andere rückzahlbare Gelder des Publikums entgegenzunehmen und Kredite für eigene Rechnung zu gewähren
3.2		Finanzmarktinfrastrukturen	
3.2.1			Handelsplätze im Sinne von § 2 Absatz 22 WpHG
3.2.2			Zentrale Gegenparteien, die zwischen die Gegenparteien der auf einem oder mehreren Märkten gehandelten Kontrakte tritt und somit als Käufer für jeden Verkäufer bzw. als Verkäufer für jeden Käufer fungiert
4	**Gesundheit**		
4.1.1			Erbringer von Gesundheitsdienstleistungen im Sinne der Richtlinie (EU) 2011/24 des Europäischen Parlaments und des Rates vom 9. März 2011 über die Ausübung der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung (ABl. L 88 vom 4.4.2011, S. 45)
4.1.2			EU-Referenzlaboratorien nach Artikel 15 der Verordnung (EU) 2022/2371 des Europäischen Parlaments und des Rates vom 23. November 2022 zu schwerwiegenden grenzüberschreitenden Gesundheitsgefahren und zur Aufhebung des Beschlusses Nr. 1082/2013/EU (ABl. L 314 vom 6.12.2022, S. 26)
4.1.3			Unternehmen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel nach § 2 AMG ausüben
4.1.4			Unternehmen, die pharmazeutische Erzeugnisse nach Abschnitt C Abteilung 21 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) herstellen
4.1.5			Unternehmen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch nach Artikel 22 der Verordnung (EU) 2022/123 des Europäischen Parlaments und des Rates vom 25. Januar 2022 zu einer verstärkten Rolle der Europäischen Arzneimittel-Agentur bei der Krisenvorsorge und -bewältigung in Bezug auf Arzneimittel und Medizinprodukte (ABl. L 20 vom 31.1.2022, S. 1)

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
			(„Liste kritischer Medizinprodukte für Notlagen im Bereich der öffentlichen Gesundheit“) eingestuft werden
5	**Wasser**		
5.1		Trinkwasserversorgung	
5.1.1			Betreiber von Wasserversorgunsanlagen im Sinne von § 2 Nr. 3 TrinkwV, jedoch unter Ausschluss der Lieferanten, für die die Lieferung von Wasser für den menschlichen Gebrauch ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit der Lieferung anderer Rohstoffe und Güter ist
5.2		Abwasserbeseitigung	
5.2.1			Unternehmen, die Abwasser nach § 54 Absatz 1 WHG sammeln, entsorgen oder behandeln, jedoch unter Ausschluss der Unternehmen, für die das Sammeln, die Entsorgung oder die Behandlung solchen Abwassers ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit ist.
6	**Digitale Infrastruktur**		
6.1.1			Betreiber von Internet Exchange Points
6.1.2			DNS-Dienstanbieter, ausgenommen Betreiber von Root-Nameservern
6.1.3			Top Level Domain Name Registry
6.1.4			Anbieter von Cloud-Computing-Diensten
6.1.5			Anbieter von Rechenzentrumsdiensten
6.1.6			Betreiber von Content Delivery Networks
6.1.7			Vertrauensdienstanbieter
6.1.8			Betreiber öffentlicher Telekommunikationsnetze
6.1.9			Anbieter öffentlich zugänglicher Telekommunikationsdienste
6.1.10			Managed Services Provider
6.1.11			Managed Security Services Provider
7	**Weltraum**		
7.1.1			Betreiber von Bodeninfrastrukturen, die sich im Eigentum von Mitgliedstaaten oder privaten Parteien befinden und von diesen verwaltet und betrieben werden und die Erbringung von weltraumgestützten Diensten unterstützen, ausgenommen Anbieter öffentlicher elektronischer Kommunikationsnetze

Entwurf	**Beschlüsse des 4. Ausschusses**

Entwurf	Beschlüsse des 4. Ausschusses
Anlage 2	**Anlage 2**
Sektoren wichtiger Einrichtungen	**Sektoren wichtiger Einrichtungen**

Entwurf

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
1	**Transport und Verkehr**		
1.1		Post- und Kurierdienste	
1.1.1			Anbieter von Postdienstleistungen nach § 3 Nummer 15 PostG, einschließlich Anbieter von Kurierdiensten
2	**Abfallbewirtschaftung**		
2.1.1			Unternehmen der Abfallbewirtschaftung nach § 3 Absatz 14 KrWG, ausgenommen Unternehmen, für die Abfallbewirtschaftung nicht ihre Hauptwirtschaftstätigkeit ist
3	**Produktion, Herstellung und Handel mit chemischen Stoffen**		
3.1.1			Hersteller und Importeure nach Artikel 3 Nummern 9 und 11 der Verordnung (EG) Nr. 1907/2006 des Europäischen Parlaments und des Rates vom 18. Dezember 2006 zur Registrierung, Bewertung, Zulassung und Beschränkung chemischer Stoffe (REACH), zur Schaffung einer Europäischen Chemikalienagentur, zur Änderung der Richtlinie 1999/45/EG und zur Aufhebung der Verordnung (EWG) Nr. 793/93 des Rates, der Verordnung (EG) Nr. 1488/94 der Kommission, der Richtlinie 76/769/EWG des Rates sowie der Richtlinien 91/155/EWG, 93/67/EWG, 93/105/EG und 2000/21/EG der Kommission (ABl. L 396 vom 30.12.2006, S. 1) von chemischen Stoffen und Gemischen im Sinne des Artikels 3 Nummer 1 und 2 der genannten Verordnung, sofern diese in Kategorie 20 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) fallen und der Registrierungspflicht nach Artikel 6 der genannten Richtline unterliegen.
4	**Produktion, Verarbeitung und Vertrieb von Lebensmitteln**		
4.1.1			Lebensmittelunternehmen nach Artikel 3 Nummer 2 der Verordnung (EG) Nr. 178/2002 des Europäischen Parlaments und des Rates vom 28. Januar 2002 zur Festlegung der allgemeinen Grundsätze und Anforderungen des Lebensmittelrechts, zur Errichtung der Europäischen Behörde für Lebensmittelsicherheit und zur Festlegung von Verfahren zur Lebensmittelsicherheit (ABl. L 31 vom 1.2.2002, S. 1), die im

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
			Großhandel sowie in der industriellen Produktion und Verarbeitung tätig sind
5	**Verarbeitendes Gewerbe/Herstellung von Waren**		
5.1		Herstellung von Medizinprodukten und In-vitro-Diagnostika	
5.1.1			Unternehmen, die Medizinprodukte nach Artikel 2 Nummer 1 der Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates (ABl. L 117 vom 5.5.2017, S. 1) herstellen, und Unternehmen, die In-vitro-Diagnostika nach Artikel 2 Nummer 2 der Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates vom 5. April 2017 über In-vitro-Diagnostika und zur Aufhebung der Richtlinie 98/79/EG und des Beschlusses 2010/227/EU der Kommission (ABl. L 117 vom 5.5.2017, S. 176) herstellen, mit Ausnahme von Unternehmen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch nach Artikel 22 der Verordnung (EU) 2022/123 des Europäischen Parlaments und des Rates vom 25. Januar 2022 zu einer verstärkten Rolle der Europäischen Arzneimittel-Agentur bei der Krisenvorsorge und -bewältigung in Bezug auf Arzneimittel und Medizinprodukte (ABl. L 20 vom 31.1.2022, S. 1) („Liste kritischer Medizinprodukte für Notlagen im Bereich der öffentlichen Gesundheit“) eingestuft werden
5.2		Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen	
5.2.1			Unternehmen, die eine der Wirtschaftstätigkeiten nach Abschnitt C Abteilung 26 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
5.3		Herstellung von elektrischen Ausrüstungen	
5.3.1			Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 27 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
5.4		Maschinenbau	
5.4.1			Unternehmen, die eine der Wirtschaftstätigkeiten nach Abschnitt C Abteilung 28 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
5.5		Herstellung von Kraftwagen und Kraftwagenteilen	
5.5.1			Unternehmen, die eine der Wirtschaftstätigkeiten nach Abschnitt C Abteilung 29 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
5.6		Sonstiger Fahrzeugbau	
5.6.1			Unternehmen, die eine der Wirtschaftstätigkeiten nach Abschnitt C Abteilung 30 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
6	**Anbieter digitaler Dienste**		
6.1.1			Anbieter von Online-Marktplätzen
6.1.2			Anbieter von Online-Suchmaschinen
6.1.3			Anbieter von Plattformen für Dienste sozialer Netzwerke
7	**Forschung**		
7.1.1			Forschungseinrichtungen

Beschlüsse des 4. Ausschusses

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
1	**Transport und Verkehr**		
1.1		Post- und Kurierdienste	
1.1.1			Anbieter von Postdienstleistungen nach § 3 Nummer 15 PostG, einschließlich Anbieter von Kurierdiensten
2	**Abfallbewirtschaftung**		
2.1.1			Unternehmen der Abfallbewirtschaftung nach § 3 Absatz 14 KrWG, ausgenommen Unternehmen, für die Abfallbewirtschaftung nicht ihre Hauptwirtschaftstätigkeit ist
3	**Produktion, Herstellung und Handel mit chemischen Stoffen**		
3.1.1			Hersteller und Importeure nach Artikel 3 Nummern 9 und 11 der Verordnung (EG) Nr. 1907/2006 des Europäischen Parlaments und des Rates vom 18. Dezember 2006 zur Registrierung, Bewertung, Zulassung und Beschränkung chemischer Stoffe (REACH), zur Schaffung einer Europäischen Chemikalienagentur, zur Änderung der Richtlinie 1999/45/EG und zur Aufhebung der Verordnung (EWG) Nr. 793/93 des Rates, der Verordnung (EG) Nr. 1488/94 der Kommission, der Richtlinie 76/769/EWG des Rates sowie der Richtlinien 91/155/EWG, 93/67/EWG, 93/105/EG und 2000/21/EG der Kommission (ABl. L 396 vom 30.12.2006, S. 1) von chemischen

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
			Stoffen und Gemischen im Sinne des Artikels 3 Nummer 1 und 2 der genannten Verordnung, sofern diese in Kategorie 20 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) fallen und der Registrierungspflicht nach Artikel 6 der genannten Richtline unterliegen
4	**Produktion, Verarbeitung und Vertrieb von Lebensmitteln**		
4.1.1			Lebensmittelunternehmen nach Artikel 3 Nummer 2 der Verordnung (EG) Nr. 178/2002 des Europäischen Parlaments und des Rates vom 28. Januar 2002 zur Festlegung der allgemeinen Grundsätze und Anforderungen des Lebensmittelrechts, zur Errichtung der Europäischen Behörde für Lebensmittelsicherheit und zur Festlegung von Verfahren zur Lebensmittelsicherheit (ABl. L 31 vom 1.2.2002, S. 1), die im Großhandel sowie in der industriellen Produktion und Verarbeitung tätig sind
5	**Verarbeitendes Gewerbe/Herstellung von Waren**		
5.1		Herstellung von Medizinprodukten und In-vitro-Diagnostika	
5.1.1			Unternehmen, die Medizinprodukte nach Artikel 2 Nummer 1 der Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates über Medizinprodukte, zur Änderung der Richtlinie 2001/83/EG, der Verordnung (EG) Nr. 178/2002 und der Verordnung (EG) Nr. 1223/2009 und zur Aufhebung der Richtlinien 90/385/EWG und 93/42/EWG des Rates (ABl. L 117 vom 5.5.2017, S. 1) herstellen, und Unternehmen, die In-vitro-Diagnostika nach Artikel 2 Nummer 2 der Verordnung (EU) 2017/746 des Europäischen Parlaments und des Rates vom 5. April 2017 über In-vitro-Diagnostika und zur Aufhebung der Richtlinie 98/79/EG und des Beschlusses 2010/227/EU der Kommission (ABl. L 117 vom 5.5.2017, S. 176) herstellen, mit Ausnahme von Unternehmen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch nach Artikel 22 der Verordnung (EU) 2022/123 des Europäischen Parlaments und des Rates vom 25. Januar 2022 zu einer verstärkten Rolle der Europäischen Arzneimittel-Agentur bei der Krisenvorsorge und -bewältigung in Bezug auf Arzneimittel und Medizinprodukte (ABl. L 20 vom 31.1.2022, S. 1) („Liste kritischer Medizinprodukte für Notlagen im Bereich der öffentlichen Gesundheit“) eingestuft werden
5.2		Herstellung von Datenverarbeitungsgeräten,	

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Sektor	Branche	Einrichtungsart
		elektronischen und optischen Erzeugnissen	
5.2.1			Unternehmen, die eine der Wirtschaftstätigkeiten nach Abschnitt C Abteilung 26 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
5.3		Herstellung von elektrischen Ausrüstungen	
5.3.1			Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 27 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
5.4		Maschinenbau	
5.4.1			Unternehmen, die eine der Wirtschaftstätigkeiten nach Abschnitt C Abteilung 28 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
5.5		Herstellung von Kraftwagen und Kraftwagenteilen	
5.5.1			Unternehmen, die eine der Wirtschaftstätigkeiten nach Abschnitt C Abteilung 29 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
5.6		Sonstiger Fahrzeugbau	
5.6.1			Unternehmen, die eine der Wirtschaftstätigkeiten nach Abschnitt C Abteilung 30 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
6	**Anbieter digitaler Dienste**		
6.1.1			Anbieter von Online-Marktplätzen
6.1.2			Anbieter von Online-Suchmaschinen
6.1.3			Anbieter von Plattformen für Dienste sozialer Netzwerke
7	**Forschung**		
7.1.1			Forschungseinrichtungen

Entwurf	Beschlüsse des 4. Ausschusses

Entwurf	Beschlüsse des 4. Ausschusses
Artikel 2	**Artikel 2**
Änderung des BND-Gesetzes	**Änderung des BND-Gesetzes**
In § 24 Absatz 5 Satz 2 des BND-Gesetzes vom 20. Dezember 1990 (BGBl. I S. 2954, 2979), das zuletzt durch Artikel 4 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist, werden die Wörter „§ 5 Absatz 7 Satz 2 bis 8 des BSI-Gesetzes“ durch die Wörter „§ 8 Absatz 8 Satz 2 bis 8 des BSI-Gesetzes“ ersetzt.	In § 24 Absatz 5 Satz 2 des BND-Gesetzes vom 20. Dezember 1990 (BGBl. I S. 2954, 2979), das zuletzt durch Artikel 4 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist, werden die Wörter „§ 5 Absatz 7 Satz 2 bis 8 des BSI-Gesetzes“ durch die Wörter „§ 8 Absatz 8 Satz 2 bis 8 des BSI-Gesetzes“ ersetzt.
Artikel 3	**Artikel 3**
Änderung der Sicherheitsüberprüfungsfeststellungsverordnung	**Änderung der Sicherheitsüberprüfungsfeststellungsverordnung**
In § 1 Nummer 8 der Sicherheitsüberprüfungsfeststellungsverordnung vom 6. Februar 2023 (BGBl. 2023 I Nr. 33), werden die Wörter „§ 3 Absatz 1 Satz 2 Nummer 1, Nummer 13 Satz 1 Buchstabe b und c, Nummer 15 und Nummer 18 des BSI-Gesetzes“ durch die Wörter „§ 3 Absatz 1 Satz 2 Nummer 1, 18 Buchstabe b und c, Nummer 22 und 25 des BSI-Gesetzes“ ersetzt.	In § 1 Nummer 8 der Sicherheitsüberprüfungsfeststellungsverordnung vom 6. Februar 2023 (BGBl. 2023 I Nr. 33), werden die Wörter „§ 3 Absatz 1 Satz 2 Nummer 1, Nummer 13 Satz 1 Buchstabe b und c, Nummer 15 und Nummer 18 des BSI-Gesetzes“ durch die Wörter „§ 3 Absatz 1 Satz 2 Nummer 1, 18 Buchstabe b und c, Nummer 22 und 25 des BSI-Gesetzes“ ersetzt.

Entwurf	Beschlüsse des 4. Ausschusses
Artikel 4	
Änderung der Besonderen Gebührenverordnung des Bundesministeriums des Innern, für Bau und Heimat für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich	
Die Anlage 1 Abschnitt 7 der besonderen Gebührenverordnung des Bundesministeriums des Innern, für Bau und Heimat für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich vom 2. September 2019 (BGBl. I S. 1359), zuletzt geändert durch Art. 1 V v. 10.09.2021 I 4229 (BGBl. I S. 4229), wird wie folgt geändert:	
1. In den Nummern 1.1.1.; 1.1.1.4.1; 1.1.1.4.2; 1.1.2; 1.1.3; 1.1.4; 1.1.5; 1.2; 1.3; 1.4; 1.5; 1.6; 1.7 werden die Wörter „§ 3 Absatz 1 Satz 2 Nummer 5 in Verbindung mit § 9 Absatz 2 Satz 1 und Absatz 4 BSIG“ durch die Wörter „§ 3 Absatz 1 Satz 2 Nummer 8 in Verbindung mit § 52 Absatz 2 Satz 1 und Absatz 4 BSIG“ ersetzt.	
2. In Nummer 1.8 werden die Wörter „§ 3 Absatz 1 Satz 2 Nummer 5 in Verbindung mit § 9 Absatz 7 BSIG“ durch die Wörter „§ 3 Absatz 1 Satz 2 Nummer 8 in Verbindung mit § 52 Absatz 7 BSIG“ ersetzt.	
3. In Nummer 1.9 wird die Angabe „§ 3 Absatz 1 Satz 2 Nummer 5 in Verbindung mit § 9 Absatz 6 BSIG“ durch die Angabe „§ 3 Absatz 1 Satz 2 Nummer 8 in Verbindung mit § 52 Absatz 6 BSIG“ ersetzt.	
4. In Nummer 1.10 wird die Angabe „§ 3 Absatz 1 Satz 2 Nummer 8 BSIG“ durch die Angabe „§ 3 Absatz 1 Satz 2 Nummer 12 BSIG“ ersetzt.	

Entwurf	Beschlüsse des 4. Ausschusses
5. In Nummer 2 wird die Angabe „§ 3 Absatz 1 Satz 2 Nummer 8 BSIG“ durch die Angabe „§ 3 Absatz 1 Satz 2 Nummer 12 BSIG“ ersetzt.	
6. In Nummer 3 wird die Angabe „§ 3 Absatz 1 Satz 2 Nummer 9 BSIG“ durch die Angabe „§ 3 Absatz 1 Satz 2 Nummer 13 BSIG“ ersetzt.	
7. In Nummer 4 werden die Wörter „§ 3 Absatz 1 Satz 2 Nummer 12, 13 und 13a BSIG“ durch die Wörter „§ 3 Absatz 1 Satz 2 Nummer 16, 18 und 19 BSIG“ ersetzt.	
8. In Nummer 5 wird die Angabe „§ 3 Absatz 1 Satz 2 Nummer 14 BSIG“ durch die Angabe „§ 3 Absatz 1 Satz 2 Nummer 20 BSIG“ ersetzt.	
9. In Nummer 6 werden die Wörter „§ 3 Absatz 1 Satz 2 Nummer 14a in Verbindung mit § 9c Absatz 5 BSIG“ durch die Wörter „§ 3 Absatz 1 Satz 2 Nummer 21 in Verbindung mit § 55 Absatz 5 BSIG“ ersetzt.	
10. In Nummer 7 werden die Wörter „§ 3 Absatz 1 Satz 2 Nummer 17 in Verbindung mit § 8a Absatz 2 BSIG“ durch die Wörter „§ 3 Absatz 1 Satz 2 Nummer 24 in Verbindung mit § 39 BSIG“ ersetzt.	
11. In Nummer 8 wird die Angabe „§ 3 Absatz 1 Satz 2 Nummer 17 in Verbindung mit § 8a Absatz 3 Satz 4 BSIG“ durch die Angabe „§ 3 Absatz 1 Satz 2 Nummer 24 BSIG in Verbindung mit § 39 Absatz 1“ ersetzt.	
12. In Nummer 9 werden die Wörter „§ 3 Absatz 1 Satz 2 Nummer 18 in Verbindung mit § 5b BSIG“ durch die Wörter „§ 3 Absatz 1 Satz 2 Nummer 25 in Verbindung mit § 11 BSIG“ ersetzt.	
13. In Nummer 10 wird die Angabe „§ 3 Absatz 1 Satz 2 Nummer 19 BSIG“ durch die Angabe „§ 3 Absatz 1 Satz 2 Nummer 26 BSIG“ ersetzt.	

Entwurf	Beschlüsse des 4. Ausschusses
Artikel 5	**Artikel 4**
Änderung des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes	**Änderung des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes**
In § 19 Absatz4 Satz 2 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes vom 23. Juni 2021 (BGBl. I S. 1982; 2022 I S. 1045), das zuletzt durch Artikel 8 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist, werden die Wörter „§ 7d Satz 1 BSI-Gesetz“ durch die Wörter „§ 17 Satz 1 des BSI-Gesetzes“ ersetzt.	In § 19 Absatz4 Satz 2 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz vom 23. Juni 2021 (BGBl. I S. 1982; 2022 I S. 1045), das zuletzt durch Artikel 44 des Gesetzes vom 12. Juli 2024 (BGBl. 2024 I Nr. 234) geändert worden ist, werden die Wörter „§ 7d Satz 1 BSI-Gesetz“ durch die Wörter „§ 17 Satz 1 des BSI-Gesetzes“ ersetzt.
Artikel 6	**Artikel 5**
Änderung der Gleichstellungsbeauftragtenwahlverordnung	**Änderung der Gleichstellungsbeauftragtenwahlverordnung**
In § 19 Absatz 9 der Gleichstellungsbeauftragtenwahlverordnung vom 17. Dezember 2015 (BGBl. I S. 2274), die durch Artikel 3 des Gesetzes vom 7. August 2021 geändert worden ist, werden die Wörter „§ 9 des BSI-Gesetzes“ durch die Wörter „§ 52 des BSI-Gesetzes“ ersetzt.	In § 19 Absatz 9 der Gleichstellungsbeauftragtenwahlverordnung vom 17. Dezember 2015 (BGBl. I S. 2274), die durch Artikel 3 des Gesetzes vom 7. August 2021 geändert worden ist, werden die Wörter „§ 9 des BSI-Gesetzes“ durch die Wörter „§ 52 des BSI-Gesetzes“ ersetzt.
Artikel 7	**Artikel 6**
Änderung des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme	**Änderung des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme**
Artikel 6 Absatz 1 des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme vom 18. Mai 2021 (BGBl. I S. 1122, 4304), wird wie folgt geändert:	Artikel 6 Absatz 1 des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme vom 18. Mai 2021 (BGBl. I S. 1122, 4304), wird wie folgt geändert:

Entwurf	Beschlüsse des 4. Ausschusses
1. Die Nummerbezeichnung „1.“ wird gestrichen und das Wort „und“ am Ende wird durch einen Punkt ersetzt.	1. Die Nummerbezeichnung „1.“ wird gestrichen und das Wort „und“ am Ende wird durch einen Punkt ersetzt.
2. Nummer 2 wird aufgehoben.	2. Nummer 2 wird aufgehoben.
Artikel 8	**Artikel 7**
Änderung der BSI-Zertifizierungs- und -Anerkennungsverordnung	**Änderung der BSI-Zertifizierungs- und -Anerkennungsverordnung**
Die BSI-Zertifizierungs- und -Anerkennungsverordnung vom 17. Dezember 2014 (BGBl. I S. 2231), die zuletzt durch Artikel 74 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist, wird wie folgt geändert:	Die BSI-Zertifizierungs- und -Anerkennungsverordnung vom 17. Dezember 2014 (BGBl. I S. 2231), die zuletzt durch Artikel 74 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist, wird wie folgt geändert:
1. Die Eingangsformel wird wie folgt gefasst:	
„Auf Grund des § 56 Absatz 1 des BSI-Gesetzes in der Fassung der Bekanntmachung vom … [*einfügen: Datum und Fundstelle dieses Gesetzes*) verordnet das Bundesministerium des Innern und für Heimat nach Anhörung der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Klimaschutz:“.	
2. In § 1 werden die Wörter „§ 9 des BSI-Gesetzes“ durch die Wörter „§ 52 des BSI-Gesetzes“ ersetzt.	1. In § 1 werden die Wörter „§ 9 des BSI-Gesetzes“ durch die Wörter „§ 52 des BSI-Gesetzes“ ersetzt.
3. In § 12 Absatz 1 werden die Wörter „§ 9 Absatz 4 des BSI-Gesetzes“ durch die Wörter „§ 52 Absatz 4 des BSI-Gesetzes“ ersetzt.	2. In § 12 Absatz 1 werden die Wörter „§ 9 Absatz 4 des BSI-Gesetzes“ durch die Wörter „§ 52 Absatz 4 des BSI-Gesetzes“ ersetzt.
4. In § 15 Absatz 1 und § 18 Absatz 1 werden jeweils die Wörter „§ 9 Absatz 5 des BSI-Gesetzes“ durch die Wörter „§ 52 Absatz 6 des BSI-Gesetzes“ und die Wörter „§ 9 Absatz 4 Nummer 2 des BSI-Gesetzes“ durch die Wörter „§ 52 Absatz 4 Satz 1 Nummer 2 des BSI-Gesetzes“ ersetzt.	3. In § 15 Absatz 1 und § 18 Absatz 1 werden jeweils die Wörter „§ 9 Absatz 5 des BSI-Gesetzes“ durch die Angabe „§ 52 Absatz 6 des BSI-Gesetzes“ und die Wörter „§ 9 Absatz 4 Nummer 2 des BSI-Gesetzes“ durch die Wörter „§ 52 Absatz 4 Nummer 2 des BSI-Gesetzes“ ersetzt.

Entwurf	Beschlüsse des 4. Ausschusses
5. § 21 wird wie folgt geändert:	4. § 21 wird wie folgt geändert:
a) In Absatz 1 werden die Wörter „§ 9 Absatz 6 des BSI-Gesetzes“ durch die Wörter „§ 52 Absatz 7 des BSI-Gesetzes“ ersetzt.	a) In Absatz 1 werden die Wörter „§ 9 Absatz 6 des BSI-Gesetzes“ durch die Wörter „§ 52 Absatz 7 des BSI-Gesetzes“ ersetzt.
b) In Absatz 1 Nummer 2 werden die Wörter „§ 9 Absatz 6 Nummer 2 des BSI-Gesetzes“ durch die Wörter „§ 52 Absatz 7 Satz 1 Nummer 2 des BSI-Gesetzes“ ersetzt.	b) In Absatz 1 Nummer 2 werden die Wörter „§ 9 Absatz 6 Nummer 2 des BSI-Gesetzes“ durch die Wörter „§ 52 Absatz 7 Satz 1 Nummer 2 des BSI-Gesetzes“ ersetzt.
c) In Absatz 4 Satz 1 werden die Wörter „§ 9 Absatz 6 Satz 2 des BSI-Gesetzes“ durch die Wörter „§ 52 Absatz 7 Satz 2 des BSI-Gesetzes“ ersetzt.	c) In Absatz 4 Satz 1 werden die Wörter „§ 9 Absatz 6 Satz 2 des BSI-Gesetzes“ durch die Wörter „§ 52 Absatz 7 Satz 2 des BSI-Gesetzes“ ersetzt.
	Artikel 8
	Änderung der BSI-Kritisverordnung
	Die BSI-Kritisverordnung vom 22. April 2016 (BGBl. I S. 958), die zuletzt durch Artikel 1 der Verordnung vom 29. November 2023 (BGBl. 2023 I Nr. 339) geändert worden ist, wird wie folgt geändert:
	1. Der Titel wird wie folgt gefasst: „Verordnung zur Bestimmung kritischer Anlagen nach dem BSI-Gesetz“.
	2. § 1 Absatz 1 wird wie folgt geändert:
	a) Die Nummern 2 und 3 werden aufgehoben.
	b) Die bisherigen Nummern 4 und 5 werden die Nummern 2 und 3.
	3. § 7 wird wie folgt geändert:
	a) Die Überschrift wird wie folgt gefasst:

Entwurf	Beschlüsse des 4. Ausschusses
	„§ 7
	Sektor Finanzwesen“.
	b) In Absatz 1 und Absatz 7 werden die Wörter „Finanz- und Versicherungswesen“ durch das Wort „Finanzwesen“ ersetzt.
	c) In Absatz 1 Nummer 5 werden die Wörter „Versicherungsdienstleistungen und“ gestrichen.
	d) Die Absätze 6 und 8 werden aufgehoben.
	e) Der bisherige Absatz 7 wird Absatz 6.
	4. Die bisherigen §§ 8, 9 und 10 werden die §§ 9, 10 und 11.
	5. Nach § 7 wird folgender § 8 eingefügt:
	„§ 8
	Sektor Sozialversicherungsträger sowie Grundsicherung für Arbeitssuchende
	(1) Leistungen der Sozialversicherung werden im Bereich Inanspruchnahme von Sozialversicherungsleistungen erbracht. Leistungen der Grundsicherung für Arbeitsuchende werden im Bereich der Inanspruchnahme von Leistungen, die der Sicherung des Lebensunterhalts dienen, mithilfe von IT-Systemen der Bundesagentur für Arbeit erbracht.
	(2) Im Sektor Sozialversicherungsträger sowie Grundsicherung für Arbeitssuchende sind kritische Anlagen solche Anlagen oder Teile davon, die
	1. den in Anhang 9 Teil 3 Spalte B genannten Kategorien zuzuordnen sind und

Entwurf	Beschlüsse des 4. Ausschusses
	2. den Schwellenwert nach Anhang 9 Teil 3 Spalte D erreichen oder überschreiten.“
	6. In § 11 werden die Wörter „Betreiber Kritischer Infrastrukturen“ durch die Wörter „Betreiber kritischer Anlagen“ und die Wörter „§ 10 Absatz 1 Satz 1 des BSI-Gesetzes“ durch die Wörter „§ 56 Absatz 4 des BSI-Gesetzes“ ersetzt.
	7. In den Überschriften von Anhang 1, Anhang 2, Anhang 3, Anhang 4,Anhang 5, Anhang 7 und Anhang 8 werden die Angaben „§ 1 Nummer 4 und 5“ jeweils durch „§ 1 Absatz 1 Nummer 2 und 3“ ersetzt.
	8. Anhang 1 wird wie folgt geändert
	a) Teil 1 Nr. 2.2 wird wie folgt gefasst: „2.2. Digitaler Energiedienst Eine Anlage oder ein System, das den zentralen, standortübergreifenden Zugriff auf die Steuerung oder die unmittelbare Beeinflussung von Energie-anlagen oder zentralen, standortübergreifenden Zugriff auf die Steuerung oder die unmittelbare Beeinflussung dezentralen Anlagen zum Verbrauch elektrischer Energie oder Gas ermöglicht“
	b) In Anhang 1 Teil 3 Nr. 1.1.2 werden die Wörter „Anlage oder System zur Steuerung/Bündelung elektrischer Leistung“ durch die Wörter „Digitaler Energiedienst“ ersetzt.
	9. Anhang 6 wird wie folgt geändert:
	a) Die Überschrift wird wie folgt gefasst:

Entwurf	Beschlüsse des 4. Ausschusses
	„(zu § 1 Absatz 1 Nummer 2 und 3, § 7 Absatz 7 Nummer 1 und 2) Anlagenkategorien und Schwellenwerte im Sektor Finanzwesen“.
	b) Die Nummern 1.23 bis 1.27 in Teil 1 werden gestrichen.
	c) Die Nummern 5, 5.1, 5.1.1, 5.1.2, 5.1.3, 5.1.4, 5.2, 5.2.1, 5.2.2 und 5.2.3 in Teil 3 werden gestrichen.
	10. Nach Anhang 8 wird folgender Anhang 9 eingefügt:
	„Anhang 9
	(zu § 1 Absatz 1 Nummer 2 und 3, § 8 Absatz 2 Nummer 1 und 2) Anlagenkategorien und Schwellenwerte im Sektor Sozialversicherungsträger sowie Grundsicherung für Arbeitssuchende
	Teil 1 Grundsätze und Fristen
	1. Im Sinne von Anhang 9 ist oder sind
	1.1 Verwaltungs- und Zahlungssystem der gesetzlichen Kranken- und Pflegeversicherung
	ein integriertes Anwendungssystem im Bereich der gesetzlichen Kranken- und Pflegeversicherung.

Entwurf	Beschlüsse des 4. Ausschusses
	2. Eine Anlage, die einer in Teil 2 Spalte B genannten Anlagenkategorie zuzuordnen ist, gilt ab dem 1. April des Kalenderjahres, das auf das Kalenderjahr folgt, in dem ihr Versorgungsgrad den in Teil 2 Spalte D genannten Schwellenwert erstmals erreicht oder überschreitet, als kritische Anlage. Nicht mehr als kritische Anlage gilt eine solche Anlage ab dem 1. April des Kalenderjahres, das auf das Kalenderjahr folgt, in dem ihr Versorgungsgrad den genannten Schwellenwert unterschreitet.
	3. Der Betreiber hat den Versorgungsgrad seiner Anlage für das zurückliegende Kalenderjahr jeweils bis zum 31. März des Folgejahres zu ermitteln.
	4. Stehen mehrere Anlagen derselben Art in einem engen betrieblichen Zusammenhang (gemeinsame Anlage) und erreichen oder überschreiten die in Teil 2 Spalte D genannten Schwellenwerte zusammen, gilt die gemeinsame Anlage als kritische Anlage. Ein enger betrieblicher Zusammenhang ist gegeben, wenn die Anlagen
	a) mit gemeinsamen Betriebseinrichtungen verbunden sind,
	b) einem identischen technischen Zweck dienen und
	c) unter gemeinsamer Leitung stehen.
	Teil 2 Anlagenkategorien und Schwellenwerte

Beschlüsse des 4. Ausschusses

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
1	**Leistungen der Sozialversicherung sowie der Grundsicherung für Arbeitsuchende**		
1.1	Leistungen der Sozialversicherung sowie der Grundsicherung für Arbeitsuchende		
1.1.1	Verwaltungs- und Zahlungssystem der gesetzlichen Kranken- und Pflegeversicherung	Anzahl der Versicherten	500 000
1.1.2	Leistungssystem	Leistungsfälle Sozialversicherungsträger der gesetzlichen Unfall- und Arbeitslosenversicherung/Jahr oder	500 000
		Anzahl der Versicherungskonten des Sozialversicherungsträgers der gesetzlichen Rentenversicherung oder	500 000
		Leistungsfälle zur Sicherung des Lebensunterhalts in der Grundsicherung für Arbeitsuchende nach dem Zweiten Buch Sozialgesetzbuch	500 000
1.1.3	Auszahlungssystem	Leistungsfälle Sozialversicherungsträger der gesetzlichen Unfall- und Arbeitslosenversicherung/Jahr oder	500 000
		Anzahl der Versicherungskonten des Sozialversicherungsträgers der gesetzlichen Rentenversicherung oder	500 000
		Leistungsfälle zur Sicherung des Lebensunterhalts in der Grundsicherung für Arbeitsuchende nach dem Zweiten Buch Sozialgesetzbuch	500 000“.

Entwurf	Beschlüsse des 4. Ausschusses
	11. In § 2 Absatz 6, § 3 Absatz 4, § 4 Absatz 3, § 5 Absatz 4, § 6 Absatz 4, § 7 Absatz 6, § 9 Absatz 3 und § 10 Absatz 3 werden die Wörter „Kritische Infrastrukturen“ jeweils durch die Wörter „kritische Anlagen“ ersetzt.
	12. Anhang 1 Teil 1 Nummern 3 und 7, Anhang 2 Teil 1 Nummern 2 und 5, Anhang 3 Teil 1 Nummern 3 und 5, Anhang 4 Teil 1 Nummern 3 und 6, Anhang 5 Teil 1 Nummern 2 und 4, Anhang 6 Teil 1 Nummern 2, 3 und 6, Anhang 7 Teil 1 Nummern 2 und 4, Anhang 8 Teil 1 Nummern 2 und 4, werden die Wörter „Kritische Infrastruktur“ jeweils durch die Wörter „kritische Anlage“ ersetzt.

Entwurf	Beschlüsse des 4. Ausschusses
	13. In § 1 Absatz 1 Nummer 3, § 2 Absatz 1, § 3 Absatz 1, § 4 Absatz 1, § 5 Absatz 1, § 6 Absatz 1, § 7 Absatz 1, § 9 Absatz 1, § 10 Absatz 1 und § 11 werden die Wörter„§ 10 Absatz 1 Satz 1 des BSI-Gesetzes“ jeweils durch die Wörter „§ 56 Absatz 4 Satz 1 in Verbindung mit § 2 Nummer 24 des BSI-Gesetzes“ ersetzt.
Artikel 9	**Artikel 9**
Änderung der BSI-IT-Sicherheitskennzeichenverordnung	**Änderung der BSI-IT-Sicherheitskennzeichenverordnung**
Die BSI-IT-Sicherheitskennzeichenverordnung vom 24. November 2021 (BGBl. I S. 4978), wird wie folgt geändert:	Die BSI-IT-Sicherheitskennzeichenverordnung vom 24. November 2021 (BGBl. I S. 4978), wird wie folgt geändert:
1. Die Eingangsformel wird wie folgt gefasst:	
„Auf Grund des § 56 Absatz 2 des BSI-Gesetzes in der Fassung der Bekanntmachung vom … [einfügen: Datum und Fundstelle dieses Gesetzes] verordnet das Bundesministerium des Innern und für Heimat im Einvernehmen mit dem Bundesministerium für Wirtschaft und Klimaschutz und dem Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz:“.	
2. In § 2 Nummer 4 werden die Wörter „§ 9c Absatz 3 Satz 1 des BSI-Gesetzes“ durch die Wörter „§ 55 Absatz 3 Satz 1 des BSI-Gesetzes“ ersetzt.	1. In § 2 Nummer 4 werden die Wörter „§ 9c Absatz 3 Satz 1 des BSI-Gesetzes“ durch die Wörter „§ 55 Absatz 3 Satz 1 des BSI-Gesetzes“ ersetzt.
3. In § 3 Absatz 1 Satz 1 werden die Wörter „§ 9c Absatz 2 des BSI-Gesetzes“ durch die Wörter „§ 55 Absatz 2 des BSI-Gesetzes“ ersetzt.	2. In § 3 Absatz 1 Satz 1 werden die Wörter „§ 9c Absatz 2 des BSI-Gesetzes“ durch die Wörter „§ 55 Absatz 2 des BSI-Gesetzes“ ersetzt.
4. § 5 wird wie folgt geändert:	3. § 5 wird wie folgt geändert:
a) In Absatz 4 werden die Wörter „§ 9c Absatz 5 BSIG“ durch die wörter „§ 55 Absatz 5 des BSI-Gesetzes“ ersetzt.	a) In Absatz 4 werden die Wörter „§ 9c Absatz 5 BSIG“ durch die Wörter „§ 55 Absatz 5 des BSI-Gesetzes“ ersetzt.

Entwurf	Beschlüsse des 4. Ausschusses
b) In Absatz 5 Satz 1 Nummer 5 werden die Wörter „§§ 7 oder 7a des BSI-Gesetzes“ durch die Wörter „§ 13 oder 14 des BSI-Gesetzes“ und die Wörter „§ 9c Absatz 8 des BSI-Gesetzes“ durch die Wörter „§ 55 Absatz 8 des BSI-Gesetzes“ ersetzt.	b) In Absatz 5 Satz 1 Nummer 5 werden die Wörter „§§ 7 oder 7a des BSI-Gesetzes“ durch die Wörter „§ 13 oder 14 des BSI-Gesetzes“ und die Wörter „§ 9c Absatz 8 des BSI-Gesetzes“ durch die Wörter „§ 55 Absatz 8 des BSI-Gesetzes“ ersetzt.
5. In § 6 Absatz 1 werden die Wörter „§ 9 des BSI-Gesetzes“ durch die Wörter „§ 52 des BSI-Gesetzes“ ersetzt.	4. In § 6 Absatz 1 werden die Wörter „§ 9 des BSI-Gesetzes“ durch die Wörter „§ 52 des BSI-Gesetzes“ ersetzt.
6. In § 7 Absatz 3 und § 9 Absatz 1 Satz 1 werden die Wörter „§ 9c des BSI-Gesetzes“ durch die Wörter „§ 55 des BSI-Gesetzes“ ersetzt.	5. In § 7 Absatz 3 und § 9 Absatz 1 Satz 1 werden die Wörter „§ 9c des BSI-Gesetzes“ durch die Wörter „§ 55 des BSI-Gesetzes“ ersetzt.
7. § 13 wird wie folgt geändert:	6. § 13 wird wie folgt geändert:
a) In Satz 1 werden die Wörter „§ 9c Absatz 2 des BSI-Gesetzes“ durch die Wörter „§ 55 Absatz 2 des BSI-Gesetzes“ ersetzt.	a) In Satz 1 werden die Wörter „§ 9c Absatz 2 des BSI-Gesetzes“ durch die Wörter „§ 55 Absatz 2 des BSI-Gesetzes“ ersetzt.
b) In Satz 2 werden die Wörter „§§ 7 oder 7a des BSI-Gesetzes“ durch die Wörter „§ 13 oder 14 des BSI-Gesetzes“ ersetzt.	b) In Satz 2 werden die Wörter „§§ 7 oder 7a des BSI-Gesetzes“ durch die Wörter „§ 13 oder 14 des BSI-Gesetzes“ ersetzt.
8. In § 14 werden die Wörter „§ 10 Absatz 3 Satz 1 des BSI-Gesetzes“ durch die Wörter „§ 56 Absatz 2 des BSI-Gesetzes“ ersetzt.	7. In § 14 werden die Wörter „§ 10 Absatz 3 Satz 1 des BSI-Gesetzes“ durch die Wörter „§ 56 Absatz 2 des BSI-Gesetzes“ ersetzt.
Artikel 10	**Artikel 10**
Änderung des De-Mail-Gesetzes	**Änderung des De-Mail-Gesetzes**
In § 18 Absatz 3 Nummer 3 des De-Mail-Gesetzes vom 28. April 2011 (BGBl. I S. 666), das zuletzt durch Artikel 10 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist, werden die Wörter „§ 9 Absatz 2 Satz 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik“ durch die Wörter „§ 52 Absatz 2 Satz 1 des BSI-Gesetzes“ ersetzt.	In § 18 Absatz 3 Nummer 3 des De-Mail-Gesetzes vom 28. April 2011 (BGBl. I S. 666), das zuletzt durch Artikel 10 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist, werden die Wörter „§ 9 Absatz 2 Satz 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik“ durch die Wörter „§ 52 Absatz 2 Satz 1 des BSI-Gesetzes“ ersetzt.

Entwurf	Beschlüsse des 4. Ausschusses
Artikel 11	**Artikel 11**
Änderung des E-Government-Gesetz	**Änderung des E-Government-Gesetz**
In § 10 des 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, wird Satz 2 aufgehoben.	In § 10 des E-Government-Gesetz vom 25. Juli 2013 (BGBl. I S. 2749), das zuletzt durch Artikel 2 des Gesetzes vom 19. Juli 2024 (BGBl. 2024 I Nr. 245) geändert worden ist wird Satz 2 aufgehoben.
Artikel 12	**Artikel 12**
Änderung der Passdatenerfassungs- und Übermittlungsverordnung	**Änderung der Passdatenerfassungs- und Übermittlungsverordnung**
In § 4 Absatz 2 der Passdatenerfassungs- und Übermittlungsverordnung vom 9. Oktober 2007 (BGBl. I S. 2312), die zuletzt durch Artikel 4 der Verordnung vom 30. Oktober 2023 (BGBl. 2023 I Nr. 290) geändert worden ist, werden die Wörter „§ 9 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821)“ durch die Wörter „§ 52 des BSI-Gesetzes vom … [einsetzen: Datum und Fundstelle dieses Gesetzes]“ ersetzt.	In § 4 Absatz 2 der Passdatenerfassungs- und Übermittlungsverordnung vom 9. Oktober 2007 (BGBl. I S. 2312), die zuletzt durch Artikel 4 der Verordnung vom 30. Oktober 2023 (BGBl. 2023 I Nr. 290) geändert worden ist, werden die Wörter „§ 9 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821)“ durch die Wörter „§ 52 des BSI-Gesetzes vom … [einsetzen: Datum und Fundstelle dieses Gesetzes]“ ersetzt.

Entwurf	Beschlüsse des 4. Ausschusses
Artikel 13	**Artikel 13**
Änderung der Personalausweisverordnung	**Änderung der Personalausweisverordnung**
In § 3 Absatz 2 der Personalausweisverordnung vom 1. November 2010 (BGBl. I S. 1460), die zuletzt durch Artikel 2 der Verordnung vom 12. April 2024 (BGBl. 2024 I Nr. 125) geändert worden ist, werden die Wörter „§ 9 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 1 des Gesetzes vom 23. Juni 2017 (BGBl. I S. 1885) geändert worden ist,“ durch die Wörter „§ 52 des BSI-Gesetzes vom … [einsetzen: Datum und Fundstelle dieses Gesetzes]“ ersetzt.	In § 3 Absatz 2 der Personalausweisverordnung vom 1. November 2010 (BGBl. I S. 1460), die zuletzt durch Artikel 2 der Verordnung vom 12. April 2024 (BGBl. 2024 I Nr. 125) geändert worden ist, werden die Wörter „§ 9 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 1 des Gesetzes vom 23. Juni 2017 (BGBl. I S. 1885) geändert worden ist,“ durch die Wörter „§ 52 des BSI-Gesetzes vom … [einsetzen: Datum und Fundstelle dieses Gesetzes]“ ersetzt.
Artikel 14	**Artikel 14**
Änderung des Hinweisgeberschutzgesetzes	**Änderung des Hinweisgeberschutzgesetzes**
In § 2 Absatz 1 Nummer 3 Buchstabe q des Hinweisgeberschutzgesetzes vom 31. Mai 2023 (BGBl. 2023 I Nr. 140), werden die Wörter „§ 2 Absatz 2 des BSI-Gesetzes“ durch die wörter „§ 2 Nummer 39 des BSI-Gesetzes“ und werden die Wörter „Anbietern digitaler Dienste im Sinne des § 2 Absatz 12 des BSI-Gesetzes“ durch die Wörter „besonders wichtigen Einrichtungen nach § 28 Absatz 1 des BSI-Gesetzes und wichtigen Einrichtungen nach § 28 Absatz 2 des BSI-Gesetzes, soweit diese den Einrichtungsarten nach Anhang 1 Nummer 6.1.4. oder Anhang 2 Nummern 6.1.1. oder 6.1.2 des BSI-Gesetzes zuzuordnen sind“ ersetzt.	In § 2 Absatz 1 Nummer 3 Buchstabe q des Hinweisgeberschutzgesetzes vom 31. Mai 2023 (BGBl. 2023 I Nr. 140), werden die Wörter „§ 2 Absatz 2 des BSI-Gesetzes“ durch die Wörter „§ 2 Nummer 39 des BSI-Gesetzes“ und werden die Wörter „Anbietern digitaler Dienste im Sinne des § 2 Absatz 12 des BSI-Gesetzes“ durch die Wörter „besonders wichtigen Einrichtungen nach § 28 Absatz 1 des BSI-Gesetzes und wichtigen Einrichtungen nach § 28 Absatz 2 des BSI-Gesetzes, soweit diese den Einrichtungsarten nach Anhang 1 Nummer 6.1.4. oder Anhang 2 Nummern 6.1.1. oder 6.1.2 des BSI-Gesetzes zuzuordnen sind“ ersetzt.

Entwurf	Beschlüsse des 4. Ausschusses
Artikel 15	**Artikel 15**
Änderung der Kassensicherungsverordnung	**Änderung der Kassensicherungsverordnung**
In § 11 Absatz 1 der Kassensicherungsverordnung vom 26. September 2017 (BGBl. I S. 3515), die durch Artikel 2 der Verordnung vom 30. Juli 2021 (BGBl. I S. 3295) geändert worden ist, werden die Wörter „§ 9 des BSI-Gesetzes“ durch die Wörter „§ 52 des BSI-Gesetzes“ ersetzt.	In § 11 Absatz 1 der Kassensicherungsverordnung vom 26. September 2017 (BGBl. I S. 3515), die durch Artikel 2 der Verordnung vom 30. Juli 2021 (BGBl. I S. 3295) geändert worden ist, werden die Wörter „§ 9 des BSI-Gesetzes“ durch die Wörter „§ 52 des BSI-Gesetzes“ ersetzt.
Artikel 16	**Artikel 16**
Änderung des Atomgesetzes	**Änderung des Atomgesetzes**
In § 44b des Atomgesetzes in der Fassung der Bekanntmachung vom 15. Juli 1985 (BGBl. I S. 1565), das zuletzt durch Artikel 1 des Gesetzes vom 4. Dezember 2022 (BGBl. I S. 2153) geändert worden ist, werden die Wörter „§ 8b Absatz 1, 2 Nummer 1 bis 3, Nummer 4 Buchstabe a bis c und Absatz 7 des BSI-Gesetzes“ durch die Wörter „§ 40 Absatz 1, 3 Nummer 1, 2, 3, 4 Buchstabe a, d und Absatz 6 des BSI-Gesetzes“ ersetzt.	In § 44b des Atomgesetzes in der Fassung der Bekanntmachung vom 15. Juli 1985 (BGBl. I S. 1565), das zuletzt durch Artikel 1 des Gesetzes vom 4. Dezember 2022 (BGBl. I S. 2153) geändert worden ist, werden die Wörter „§ 8b Absatz 1, 2 Nummer 1 bis 3, Nummer 4 Buchstabe a bis c und Absatz 7 des BSI-Gesetzes“ durch die Wörter „§ 40 Absatz 1, 3 Nummer 1, 2, 3, 4 Buchstabe a, d und Absatz 6 des BSI-Gesetzes“ ersetzt.
Artikel 17	**Artikel 17**
Änderung des Energiewirtschaftsgesetzes	**Änderung des Energiewirtschaftsgesetzes**
Das Energiewirtschaftsgesetz vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 1 des Gesetzes vom 14. Mai 2024 (BGBl. 2024 I Nr. 161) geändert worden ist, wird wie folgt geändert:	Das Energiewirtschaftsgesetz vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 26 des Gesetzes vom 15. Juli 2024 (BGBl. 2024 I Nr. 236) geändert worden ist , wird wie folgt geändert:
1. In der Inhaltsübersicht wird nach der Angabe zu § 5b folgende Angabe eingefügt:	1. In der Inhaltsübersicht wird nach der Angabe zu § 5b folgende Angabe eingefügt:

Entwurf	Beschlüsse des 4. Ausschusses
„§ 5c IT-Sicherheit im Anlagen- und Netzbetrieb, Festlegungskompetenz“.	„§ 5c IT-Sicherheit im Anlagen- und Netzbetrieb, Festlegungskompetenz“.
	2. § 3 wird wie folgt geändert:
	a) Nach Nummer 1d wird folgende Nummer 1e angefügt: „1e. Betreiber digitaler Energiedienste eine natürliche oder juristische Person, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf die Beschaffenheit und den Betrieb eines oder mehrerer digitaler Energiedienste ausübt; Betreiber von Energieversorgungsnetzen und Anlagen stellen keine Betreiber von digitalen Energiediensten dar,“.
	b) Nach Nummer 11 wird folgende Nummer 11a eingefügt: „11a. Digitale Energiedienste eine Anlage oder ein System, das den zentralen, standortübergreifenden Zugriff auf die Steuerung oder die unmittelbare Beeinflussung von Energieanlagen oder zentralen, standortüber-greifenden Zugriff auf die Steuerung oder die unmittelbare Beeinflussung dezentralen An-lagen zum Verbrauch elektrischer Energie oder Gas ermöglicht,“.
2. Nach § 5b wird folgender § 5c eingefügt:	3. Nach § 5b wird folgender § 5c eingefügt:

Entwurf	Beschlüsse des 4. Ausschusses
„§ 5c	„§ 5c
IT-Sicherheit im Anlagen- und Netzbetrieb, Festlegungskompetenz	IT-Sicherheit im Anlagen- und Netzbetrieb, Festlegungskompetenz
(1) Der Betreiber eines Energieversorgungsnetzes hat einen angemessenen Schutz gegen Bedrohungen für Telekommunikationssysteme sowie elektronische Datenverarbeitungssysteme, die für den sicheren Netzbetrieb notwendig sind, zu gewährleisten. Der angemessene Schutz nach Satz 1 ist auch durch Berücksichtigung erforderlicher Anforderungen bei der Beschaffung von Anlagengütern und Dienstleistungen sicherzustellen. Die Bundesnetzagentur bestimmt im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik durch Festlegung nach § 29 Absatz 1 in einem Katalog von Sicherheitsanforderungen (IT-Sicherheitskatalog) die Anforderungen an den angemessenen Schutz. Dabei beteiligt die Bundesnetzagentur die Betreiber von Energieversorgungsnetzen und deren Branchenverbände. Die Bundesnetzagentur überprüft den IT-Sicherheitskatalog alle zwei Jahre und aktualisiert ihn bei Bedarf. Ein angemessener Schutz nach Satz 1 liegt vor, wenn die Anforderung des IT-Sicherheitskatalogs eingehalten werden. Die Einhaltung der Anforderungen des IT-Sicherheitskatalogs ist vom Betreiber zu dokumentieren.	(1) Der Betreiber eines Energieversorgungsnetzes hat einen angemessenen Schutz gegen Bedrohungen für Telekommunikationssysteme sowie elektronische Datenverarbeitungssysteme, die für den sicheren Netzbetrieb notwendig sind, zu gewährleisten. Der angemessene Schutz nach Satz 1 ist auch durch Berücksichtigung erforderlicher Anforderungen bei der Beschaffung von Anlagengütern und Dienstleistungen sicherzustellen. Die Bundesnetzagentur bestimmt im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik durch Festlegung nach § 29 Absatz 1 in einem Katalog von Sicherheitsanforderungen (IT-Sicherheitskatalog) die Anforderungen an den angemessenen Schutz. Dabei beteiligt die Bundesnetzagentur die Betreiber von Energieversorgungsnetzen und deren Branchenverbände. Die Bundesnetzagentur überprüft den IT-Sicherheitskatalog alle zwei Jahre und aktualisiert ihn bei Bedarf. Ein angemessener Schutz nach Satz 1 liegt vor, wenn die Anforderung des IT-Sicherheitskatalogs eingehalten werden. Die Einhaltung der Anforderungen des IT-Sicherheitskatalogs ist vom Betreiber zu dokumentieren.

(2) Der Betreiber einer Energieanlage, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes vom … [einsetzen: Datum und Fundstelle nach Artikel 1 dieses Gesetzes] in der jeweils geltenden Fassung oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist und dessen Energieanlage an ein Energieversorgungsnetz angeschlossen ist, hat einen angemessenen Schutz gegen Bedrohungen für Telekommunikationssysteme sowie elektronische Datenverarbeitungssysteme zu gewährleisten, die für einen sicheren Anlagenbetrieb notwendig sind. § 28 Absatz 1 Satz 2 sowie § 28 Absatz 2 Satz 2 des BSI-Gesetzes bleiben unberührt. Der angemessene Schutz nach Satz 1 ist auch durch Berücksichtigung erforderlicher Anforderungen bei der Beschaffung von Anlagengütern und Dienstleistungen sicherzustellen. Die Bundesnetzagentur bestimmt im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik durch Festlegung nach § 29 Absatz 1 in einem IT-Sicherheitskatalog die Anforderungen an den angemessenen Schutz. Dabei beteiligt die Bundesnetzagentur die Betreiber nach Satz 1 und deren Branchenverbände. Die Bundesnetzagentur überprüft den IT-Sicherheitskatalog alle zwei Jahre und aktualisiert ihn bei Bedarf. Für Telekommunikationssysteme sowie elektronische Datenverarbeitungssysteme von Anlagen nach § 7 Absatz 1 des Atomgesetzes in der Fassung der Bekanntmachung vom 15. Juli 1985 (BGBl. I S. 1565), das zuletzt durch Artikel 16 des Gesetzes vom … [einsetzen: Datum und Fundstelle nach Artikel 33 Absatz 1 Satz 1 dieses Gesetzes] geändert worden ist, haben Vorgaben auf Grund des Atomgesetzes Vorrang vor den Anforderungen des IT-Sicherheitskatalogs nach Satz 4. Die für die nukleare Sicherheit zuständigen Genehmigungs- und Aufsichtsbehörden des Bundes und der Länder sind bei der Erarbeitung des IT-Sicherheitskatalogs nach Satz 4 zu beteiligen. Ein angemessener Schutz nach Satz 1 liegt vor, wenn die Anforderungen des IT-Sicherheitskatalogs eingehalten werden. Die Einhaltung der Anforderungen des	(2) Der Betreiber einer Energieanlage, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes vom … [einsetzen: Datum und Fundstelle nach Artikel 1 dieses Gesetzes] in der jeweils geltenden Fassung oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist und dessen Energieanlage an ein Energieversorgungsnetz angeschlossen ist, hat einen angemessenen Schutz gegen Bedrohungen für Telekommunikationssysteme sowie elektronische Datenverarbeitungssysteme zu gewährleisten, die für einen sicheren Anlagenbetrieb notwendig sind. § 28 Absatz 1 Satz 2 sowie § 28 Absatz 2 Satz 2 des BSI-Gesetzes bleiben unberührt. Der angemessene Schutz nach Satz 1 ist auch durch Berücksichtigung erforderlicher Anforderungen bei der Beschaffung von Anlagengütern und Dienstleistungen sicherzustellen. Die Bundesnetzagentur bestimmt im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik durch Festlegung nach § 29 Absatz 1 in einem IT-Sicherheitskatalog die Anforderungen an den angemessenen Schutz. Dabei beteiligt die Bundesnetzagentur die Betreiber nach Satz 1 und deren Branchenverbände. Die Bundesnetzagentur überprüft den IT-Sicherheitskatalog alle zwei Jahre und aktualisiert ihn bei Bedarf. Für Telekommunikationssysteme sowie elektronische Datenverarbeitungssysteme von Anlagen nach § 7 Absatz 1 des Atomgesetzes in der Fassung der Bekanntmachung vom 15. Juli 1985 (BGBl. I S. 1565), das zuletzt durch Artikel 16 des Gesetzes vom … [einsetzen: Datum und Fundstelle nach Artikel 33 Absatz 1 Satz 1 dieses Gesetzes] geändert worden ist, haben Vorgaben auf Grund des Atomgesetzes Vorrang vor den Anforderungen des IT-Sicherheitskatalogs nach Satz 4. Die für die nukleare Sicherheit zuständigen Genehmigungs- und Aufsichtsbehörden des Bundes und der Länder sind bei der Erarbeitung des IT-Sicherheitskatalogs nach Satz 4 zu beteiligen. Ein angemessener Schutz nach Satz 1 liegt vor, wenn die Anforderungen des IT-Sicherheitskatalogs eingehalten werden. Die Einhaltung der Anforderungen des

Entwurf	Beschlüsse des 4. Ausschusses
IT-Sicherheitskatalogs ist vom Betreiber zu dokumentieren.	IT-Sicherheitskatalogs ist vom Betreiber zu dokumentieren.
	(3) Der Betreiber eines digitalen Energiedienstes, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes vom ... [einsetzen: Datum und Fundstelle nach Artikel 1] in der jeweils geltenden Fassung oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist und dessen Energieanlage an ein Energieversorgungsnetz angeschlossen ist, hat einen angemessenen Schutz gegen Bedrohungen für Telekommunikationssysteme sowie elektronische Datenverarbeitungssysteme zu gewährleisten, die für einen sicheren Anlagenbetrieb notwendig sind. § 28 Absatz 1 Satz 2 sowie § 28 Absatz 2 Satz 2 des BSI-Gesetzes bleiben unberührt. Der angemessene Schutz nach Satz 1 ist auch durch Berücksichtigung erforderlicher Anforderungen bei der Beschaffung von Anlagengütern und Dienstleistungen sicherzustellen. Die Bundesnetzagentur bestimmt im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik durch Festlegung nach § 29 Absatz 1 in einem IT-Sicherheitskatalog die Anforderungen an den angemessenen Schutz. Dabei beteiligt die Bundesnetzagentur die Betreiber nach Satz 1 und deren Branchenverbände. Die Bundesnetzagentur überprüft den IT-Sicherheitskatalog alle zwei Jahre und aktualisiert ihn bei Bedarf. Ein angemessener Schutz nach Satz 1 liegt vor, wenn die Anforderungen des IT-Sicherheitskatalogs eingehalten werden. Die Einhaltung der Anforderungen des IT-Sicherheitskatalogs ist vom Betreiber zu dokumentieren.

Entwurf	Beschlüsse des 4. Ausschusses
(3) Der IT-Sicherheitskatalog nach Absatz 1 Satz 3 und der IT-Sicherheitskatalog nach Absatz 2 Satz 4 sollen jeweils den Stand der Technik einhalten und unter Berücksichtigung der einschlägigen europäischen Normen oder der einschlägigen 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 des Betreibers sowie die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen, zu berücksichtigen. Der IT-Sicherheitskatalog nach Absatz 1 Satz 3 und der IT-Sicherheitskatalog nach Absatz 2 Satz 4 umfassen jeweils zumindest Vorgaben für:	(4) Der IT-Sicherheitskatalog nach Absatz 1 Satz 3, der IT-Sicherheitskatalog nach Absatz 2 Satz 4 und der IT-Sicherheitskatalog nach Absatz 3 Satz 4 sollen jeweils den Stand der Technik einhalten und unter Berücksichtigung der einschlägigen europäischen Normen oder der einschlägigen 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 des Betreibers sowie die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen, zu berücksichtigen. Der IT-Sicherheitskatalog nach Absatz 1 Satz 3, der IT-Sicherheitskatalog nach Absatz 2 Satz 4 und der IT-Sicherheitskatalog nach Absatz 3 Satz 4 umfassen jeweils zumindest Vorgaben für:
1. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationstechnik,	1. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationstechnik,
2. die Bewältigung von Sicherheitsvorfällen,	2. die Bewältigung von Sicherheitsvorfällen,
3. die Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und für das Krisenmanagement,	3. die Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und für das Krisenmanagement,
4. die Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern,	4. die Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern,
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen,	5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen,

Entwurf	Beschlüsse des 4. Ausschusses
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit der Informationstechnik,	6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit der Informationstechnik,
7. grundlegende Verfahren im Bereich der Cyberhygiene und für Schulungen im Bereich der Sicherheit der Informationstechnik,	7. grundlegende Verfahren im Bereich der Cyberhygiene und für Schulungen im Bereich der Sicherheit der Informationstechnik,
8. Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,	8. Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,
9. die Sicherheit des Personals, Konzepte für die Zugriffskontrolle und das Management von Anlagen,	9. die Sicherheit des Personals, Konzepte für die Zugriffskontrolle und das Management von Anlagen,
10. die Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung,	10. die Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung,
11. den Einsatz von Systemen zur Angriffserkennung nach § 2 Nummer 41 des BSI-Gesetzes,	11. den Einsatz von Systemen zur Angriffserkennung nach § 2 Nummer 41 des BSI-Gesetzes,

Entwurf	Beschlüsse des 4. Ausschusses
12. den Einsatz eines Elements oder einer Gruppe von Elementen eines Netz- oder Informationssystems (IKT-Produkt), eines Dienstes, der vollständig oder überwiegend aus der Übertragung, Speicherung, Abfrage oder Verarbeitung von Informationen mittels Netz- und Informationssystemen besteht (IKT-Dienst) und jeglicher Tätigkeiten, mit denen ein IKT-Produkt oder IKT-Dienst konzipiert, entwickelt, bereitgestellt oder gepflegt werden soll (IKT-Prozess) mit Cybersicherheitszertifizierung gemäß europäischer Schemata nach Artikel 49 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 (ABl. 151 vom 7.6.2019, S. 15).	12. den Einsatz eines Elements oder einer Gruppe von Elementen eines Netz- oder Informationssystems (IKT-Produkt), eines Dienstes, der vollständig oder überwiegend aus der Übertragung, Speicherung, Abfrage oder Verarbeitung von Informationen mittels Netz- und Informationssystemen besteht (IKT-Dienst) und jeglicher Tätigkeiten, mit denen ein IKT-Produkt oder IKT-Dienst konzipiert, entwickelt, bereitgestellt oder gepflegt werden soll (IKT-Prozess) mit Cybersicherheitszertifizierung gemäß europäischer Schemata nach Artikel 49 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 (ABl. 151 vom 7.6.2019, S. 15).
Die Bundesnetzagentur kann in den IT-Sicherheitskatalogen nähere Bestimmungen zu Format, Inhalt und Gestaltung der nach Absatz 1 Satz 7 oder nach Absatz 2 Satz 10 erforderlichen Dokumentation über die Einhaltung der Anforderungen des jeweiligen IT-Sicherheitskatalogs sowie zur Behebung von Sicherheitsmängeln treffen. Die Bundesnetzagentur kann in den IT-Sicherheitskatalogen auch Regelungen zur regelmäßigen Überprüfung der Erfüllung der Sicherheitsanforderungen treffen.	Die Bundesnetzagentur kann in den IT-Sicherheitskatalogen nähere Bestimmungen zu Format, Inhalt und Gestaltung der nach Absatz 1 Satz 7, nach Absatz 2 Satz 10 oder nach Absatz 3 Satz 7 erforderlichen Dokumentation über die Einhaltung der Anforderungen des jeweiligen IT-Sicherheitskatalogs sowie zur Behebung von Sicherheitsmängeln treffen. Die Bundesnetzagentur kann in den IT-Sicherheitskatalogen auch Regelungen zur regelmäßigen Überprüfung der Erfüllung der Sicherheitsanforderungen treffen.

Entwurf	Beschlüsse des 4. Ausschusses
(4) Der Betreiber eines Energieversorgungsnetzes oder der Betreiber einer Energieanlage, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist und dessen Energieanlage an ein Energieversorgungsnetz angeschlossen ist, hat der Bundesnetzagentur die Dokumentation über die Einhaltung der Anforderungen des jeweiligen IT-Sicherheitskatalogs nach Absatz 1 Satz 7 oder nach Absatz 2 Satz 10 zu übermitteln. § 28 Absatz 1 Satz 2 sowie § 28 Absatz 2 Satz 2 des BSI-Gesetzes bleiben unberührt. Bei Bedarf kann die Bundesnetzagentur die Vorlage des Mängelbeseitigungsplans von dem Betreiber nach Satz 1 anfordern. Die Bundesnetzagentur kann bei Sicherheitsmängeln, die sich aus dem Mängelbeseitigungsplan ergeben, von dem Betreiber nach Satz 1 die Beseitigung dieser Mängel innerhalb einer durch die Bundesnetzagentur gesetzten Frist verlangen. Der Betreiber nach Satz 1 hat der Bundesnetzagentur und den in deren Auftrag handelnden Personen zum Zweck der Überprüfung der Einhaltung der Sicherheitsanforderungen nach Absatz 1 oder Absatz 2 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 die Bundesnetzagentur Gebühren und Auslagen nur, sofern die Bundesnetzagentur auf Grund von Anhaltspunkten tätig geworden ist, die berechtigte Zweifel an der Einhaltung der in den Absätzen 1 und 2 genannten Anforderungen begründen.	(5) Der Betreiber eines Energieversorgungsnetzes, der Betreiber einer Energieanlage, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist und dessen Energieanlage an ein Energieversorgungsnetz angeschlossen ist, oder der Betreiber eines digitalen Energiedienstes, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist, hat der Bundesnetzagentur die Dokumentation über die Einhaltung der Anforderungen des jeweiligen IT-Sicherheitskatalogs nach Absatz 1 Satz 7, nach Absatz 2 Satz 10 oder nach Absatz 3 Satz 7 zu übermitteln. § 28 Absatz 1 Satz 2 sowie § 28 Absatz 2 Satz 2 des BSI-Gesetzes bleiben unberührt. Bei Bedarf kann die Bundesnetzagentur die Vorlage des Mängelbeseitigungsplans von dem Betreiber nach Satz 1 anfordern. Die Bundesnetzagentur kann bei Sicherheitsmängeln, die sich aus dem Mängelbeseitigungsplan ergeben, von dem Betreiber nach Satz 1 die Beseitigung dieser Mängel innerhalb einer durch die Bundesnetzagentur gesetzten Frist verlangen. Der Betreiber nach Satz 1 hat der Bundesnetzagentur und den in deren Auftrag handelnden Personen zum Zweck der Überprüfung der Einhaltung der Sicherheitsanforderungen nach Absatz 1, Absatz 2 oder Absatz 3 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 die Bundesnetzagentur Gebühren und Auslagen nur, sofern die Bundesnetzagentur auf Grund von Anhaltspunkten tätig geworden ist, die berechtigte Zweifel an der Einhaltung der in den Absätzen 1 und 2 genannten Anforderungen begründen.

Entwurf	Beschlüsse des 4. Ausschusses
(5) Erlangt die Bundesnetzagentur Kenntnis über Hinweise oder Informationen, wonach ein Betreiber einer Energieanlage, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist und dessen Energieanlage an ein Energieversorgungsnetz angeschlossen ist, die Sicherheitsanforderungen nach Absatz 2 nicht oder nicht richtig umsetzt, so kann sie von diesem Betreiber Informationen anfordern, um die Einhaltung der Sicherheitsanforderungen nach Absatz 2 zu überprüfen. § 28 Absatz 1 Satz 2 sowie § 28 Absatz 2 Satz 2 des BSI-Gesetzes bleiben unberührt. Absatz 4 Satz 3 bis 6 ist entsprechend anzuwenden.	(6) Erlangt die Bundesnetzagentur Kenntnis über Hinweise oder Informationen, wonach ein Betreiber eines Energieversorgungsnetzes, ein Betreiber einer Energieanlage, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist und dessen Energieanlage an ein Energieversorgungsnetz angeschlossen ist, die Sicherheitsanforderungen nach Absatz 2 nicht oder nicht richtig umsetzt, so kann sie von diesem Betreiber Informationen anfordern, um die Einhaltung der Sicherheitsanforderungen nach Absatz 2 zu überprüfen. § 28 Absatz 1 Satz 2 sowie § 28 Absatz 2 Satz 2 des BSI-Gesetzes bleiben unberührt. Absatz 4 Satz 3 bis 6 ist entsprechend anzuwenden.
(6) Der Betreiber eines Energieversorgungsnetzes oder der Betreiber einer Energieanlage, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist und dessen Energieanlage an ein Energieversorgungsnetz angeschlossen ist, ist verpflichtet, folgende Informationen an eine vom Bundesamt für Sicherheit in der Informationstechnik und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete gemeinsame Meldestelle zu melden:	(7) Der Betreiber eines Energieversorgungsnetzes oder der Betreiber einer Energieanlage, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist und dessen Energieanlage an ein Energieversorgungsnetz angeschlossen ist, oder der Betreiber eines digitalen Energiedienstes, der eine besonders wichtige Ein-richtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist, ist verpflichtet, folgende Informationen an eine vom Bundesamt für Sicherheit in der Informationstechnik und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete gemeinsame Meldestelle zu melden:

Entwurf	Beschlüsse des 4. Ausschusses
1. unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall nach § 2 Nummer 11 des BSI-Gesetzes, eine frühe Erstmeldung, in der angegeben wird, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf eine rechtswidrige oder eine böswillige Handlung zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte,	1. unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall nach § 2 Nummer 11 des BSI-Gesetzes, eine frühe Erstmeldung, in der angegeben wird, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf eine rechtswidrige oder eine böswillige Handlung zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte,
2. unverzüglich, spätestens jedoch innerhalb von 72 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall nach § 2 Nummer 11 des BSI-Gesetzes, eine Meldung über den erheblichen 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,	2. unverzüglich, spätestens jedoch innerhalb von 72 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall nach § 2 Nummer 11 des BSI-Gesetzes, eine Meldung über den erheblichen 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,
3. auf Ersuchen des Bundesamtes für Sicherheit in der Informationstechnik eine Zwischenmeldung über relevante Statusaktualisierungen,	3. auf Ersuchen des Bundesamtes für Sicherheit in der Informationstechnik eine Zwischenmeldung über relevante Statusaktualisierungen,
4. spätestens einen Monat nach Übermittlung der Meldung des erheblichen Sicherheitsvorfalls nach § 2 Nummer 11 des BSI-Gesetzes eine Abschlussmeldung, die Folgendes enthält:	4. spätestens einen Monat nach Übermittlung der Meldung des erheblichen Sicherheitsvorfalls nach § 2 Nummer 11 des BSI-Gesetzes eine Abschlussmeldung, die Folgendes enthält:
a) eine ausführliche Beschreibung des erheblichen Sicherheitsvorfalls nach § 2 Nummer 11 des BSI-Gesetzes, einschließlich seines Schweregrads und seiner Auswirkungen,	a) eine ausführliche Beschreibung des erheblichen Sicherheitsvorfalls nach § 2 Nummer 11 des BSI-Gesetzes, einschließlich seines Schweregrads und seiner Auswirkungen,

Entwurf	Beschlüsse des 4. Ausschusses
b) Angaben zur Art der Bedrohung beziehungsweise zugrunde liegenden Ursache, die wahrscheinlich den erheblichen Sicherheitsvorfall nach § 2 Nummer 11 des BSI-Gesetzes ausgelöst hat,	b) Angaben zur Art der Bedrohung beziehungsweise zugrunde liegenden Ursache, die wahrscheinlich den erheblichen Sicherheitsvorfall nach § 2 Nummer 11 des BSI-Gesetzes ausgelöst hat,
c) Angaben zu den getroffenen und den laufenden Abhilfemaßnahmen,	c) Angaben zu den getroffenen und den laufenden Abhilfemaßnahmen,
d) gegebenenfalls die grenzüberschreitenden Auswirkungen des erheblichen Sicherheitsvorfalls nach § 2 Nummer 11 des BSI-Gesetzes.	d) gegebenenfalls die grenzüberschreitenden Auswirkungen des erheblichen Sicherheitsvorfalls nach § 2 Nummer 11 des BSI-Gesetzes.
§ 28 Absatz 1 Satz 2 sowie § 28 Absatz 2 Satz 2 des BSI-Gesetzes bleiben unberührt. § 32 Absatz 2 bis 5 und § 36 des BSI-Gesetzes sind entsprechend anzuwenden. Bei Meldungen nach diesem Absatz trifft das Bundesamt für Sicherheit in der Informationstechnik Maßnahmen nach § 36 des BSI-Gesetzes im Benehmen mit der Bundesnetzagentur.	§ 28 Absatz 1 Satz 2 sowie § 28 Absatz 2 Satz 2 des BSI-Gesetzes bleiben unberührt. § 32 Absatz 2 bis 5 und § 36 des BSI-Gesetzes sind entsprechend anzuwenden. Bei Meldungen nach diesem Absatz trifft das Bundesamt für Sicherheit in der Informationstechnik Maßnahmen nach § 36 des BSI-Gesetzes im Benehmen mit der Bundesnetzagentur.

(7) Das Bundesamt für Sicherheit in der Informationstechnik hat die Meldungen nach Absatz 6 und solche Meldungen über Sicherheitsvorfälle nach § 32 des BSI-Gesetzes, bei welchen das Bundesamt für Sicherheit in der Informationstechnik Kenntnis von einer Relevanz für die Energieversorgungssicherheit und Erfüllung der Zwecke und Ziele nach § 1 erlangt, unverzüglich an die Bundesnetzagentur weiterzuleiten. Die Bundesnetzagentur führt unverzüglich eine Bewertung der Auswirkungen des nach Satz 1 übermittelten Sicherheitsvorfalls auf die Energieversorgungssicherheit durch und übermittelt ihre Ergebnisse 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 und ist befugt, zur Bewertung der Auswirkungen des Sicherheitsvorfalls auf die Energieversorgungssicherheit erforderliche personenbezogene Daten zu erheben, zu speichern und zu verwenden. Das betroffene Unternehmen hat 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-, von Fernleitungs- sowie von Verteilnetzen einbeziehen und ist befugt, ihnen die hierzu erforderlichen personenbezogenen Daten zu übermitteln. Die Betreiber von Übertragungs-, von Fernleitungs- sowie von Verteilnetzen sind befugt, die ihnen nach Satz 5 zum dort genannten Zweck übermittelten personenbezogenen Daten zu erheben, zu speichern und zu verwenden. Nach Erstellung der Bewertung sind die hierzu verwendeten personenbezogenen Daten von der Bundesnetzagentur und den Betreibern von Übertragungs-, von Fernleitungs- sowie von Verteilnetzen unverzüglich zu löschen. Das Bundesamt für Sicherheit in der Informati-	(8) Das Bundesamt für Sicherheit in der Informationstechnik hat die Meldungen nach Absatz 7 und solche Meldungen über Sicherheitsvorfälle nach § 32 des BSI-Gesetzes, bei welchen das Bundesamt für Sicherheit in der Informationstechnik Kenntnis von einer Relevanz für die Energieversorgungssicherheit und Erfüllung der Zwecke und Ziele nach § 1 erlangt, unverzüglich an die Bundesnetzagentur weiterzuleiten. Die Bundesnetzagentur führt unverzüglich eine Bewertung der Auswirkungen des nach Satz 1 übermittelten Sicherheitsvorfalls auf die Energieversorgungssicherheit durch und übermittelt ihre Ergebnisse 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 und ist befugt, zur Bewertung der Auswirkungen des Sicherheitsvorfalls auf die Energieversorgungssicherheit erforderliche personenbezogene Daten zu erheben, zu speichern und zu verwenden. Das betroffene Unternehmen hat 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-, von Fernleitungs- sowie von Verteilnetzen einbeziehen und ist befugt, ihnen die hierzu erforderlichen personenbezogenen Daten zu übermitteln. Die Betreiber von Übertragungs-, von Fernleitungs- sowie von Verteilnetzen sind befugt, die ihnen nach Satz 5 zum dort genannten Zweck übermittelten personenbezogenen Daten zu erheben, zu speichern und zu verwenden. Nach Erstellung der Bewertung sind die hierzu verwendeten personenbezogenen Daten von der Bundesnetzagentur und den Betreibern von Übertragungs-, von Fernleitungs- sowie von Verteilnetzen unverzüglich zu löschen. Das Bundesamt für Sicherheit in der Informati-

Entwurf	Beschlüsse des 4. Ausschusses
onstechnik berücksichtigt die Bewertung der Bundesnetzagentur bei der Erfüllung der Aufgaben nach § 40 Absatz 3 Nummer 2 des BSI-Gesetzes. Das Bundesamt für Sicherheit in der Informationstechnik und die Bundesnetzagentur haben jeweils 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 den Absätzen 1 bis 6 sowie dieses Absatzes wird nicht gewährt. § 29 des Verwaltungsverfahrensgesetzes bleibt unberührt.	onstechnik berücksichtigt die Bewertung der Bundesnetzagentur bei der Erfüllung der Aufgaben nach § 40 Absatz 3 Nummer 2 des BSI-Gesetzes. Das Bundesamt für Sicherheit in der Informationstechnik und die Bundesnetzagentur haben jeweils 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 den Absätzen 1 bis 6 sowie dieses Absatzes wird nicht gewährt. § 29 des Verwaltungsverfahrensgesetzes bleibt unberührt.

(8) Der Betreiber eines Energieversorgungsnetzes oder einer Energieanlage, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist und dessen Energieanlage an ein Energieversorgungsnetz angeschlossen ist, ist verpflichtet, spätestens drei Monate, nachdem er erstmals oder erneut als eine der vorgenannten Einrichtungen gilt, dem Bundesamt für Sicherheit in der Informationstechnik über eine gemeinsam vom Bundesamt für Sicherheit in der Informationstechnik und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete Registrierungsmöglichkeit die Angaben nach § 33 Absatz 1 Nummer 1 bis 4 des BSI-Gesetzes zu übermitteln. Der Betreiber eines Energieversorgungsnetzes, der nicht eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder nicht eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist, ist verpflichtet, spätestens bis zum Ablauf des … [einsetzen: Datum desjenigen Tages des dritten auf den Monat des Inkrafttretens nach Artikel 33 Absatz 1 Satz 1 dieses Gesetzes folgenden Kalendermonats, dessen Zahl mit der des Tages der des Inkrafttretens nach Artikel 33 Absatz 1 Satz 1 dieses Gesetzes übereinstimmt, oder, wenn es einen solchen Kalendertag nicht gibt, Datum des ersten Tages des darauffolgenden Kalendermonats] dem Bundesamt für Sicherheit in der Informationstechnik über eine gemeinsam vom Bundesamt für Sicherheit in der Informationstechnik und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete Registrierungsmöglichkeit die Angaben nach § 33 Absatz 1 Nummer 1 bis 4 des BSI-Gesetzes zu übermitteln. § 28 Absatz 1 Satz 2 sowie § 28 Absatz 2 Satz 2 des BSI-Gesetzes bleiben unberührt. § 33 Absatz 2, 4 und 5 des BSI-Gesetzes ist entsprechend anzuwenden. Das Bundesamt für Sicherheit in der Informationstechnik übermittelt die Registrierungen nach den Sätzen 1 und 2 einschließlich der damit verbundenen Kon-	(9) Der Betreiber eines Energieversorgungsnetzes, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist, der Betreiber oder einer Energieanlage, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist und dessen Energieanlage an ein Energieversorgungsnetz angeschlossen ist, oder der Betreiber eines digitalen Energiedienstes, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist, ist verpflichtet, spätestens drei Monate, nachdem er erstmals oder erneut als eine der vorgenannten Einrichtungen gilt, dem Bundesamt für Sicherheit in der Informationstechnik über eine gemeinsam vom Bundesamt für Sicherheit in der Informationstechnik und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete Registrierungsmöglichkeit die Angaben nach § 33 Absatz 1 Nummer 1 bis 4 des BSI-Gesetzes zu übermitteln. Der Betreiber eines Energieversorgungsnetzes, der nicht eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder nicht eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist, ist verpflichtet, spätestens bis zum Ablauf des … [einsetzen: Datum desjenigen Tages des dritten auf den Monat des Inkrafttretens nach Artikel 33 Absatz 1 Satz 1 dieses Gesetzes folgenden Kalendermonats, dessen Zahl mit der des Tages der des Inkrafttretens nach Artikel 33 Absatz 1 Satz 1 dieses Gesetzes übereinstimmt, oder, wenn es einen solchen Kalendertag nicht gibt, Datum des ersten Tages des darauffolgenden Kalendermonats] dem Bundesamt für Sicherheit in der Informationstechnik über eine gemeinsam vom Bundesamt für Sicherheit in der Informationstechnik und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete Registrierungsmöglichkeit die Angaben nach § 33 Absatz 1 Nummer 1 bis 4 des

Entwurf	Beschlüsse des 4. Ausschusses
taktdaten und jede Änderung der Registrierungen unverzüglich an die Bundesnetzagentur. Die Registrierungen nach den Sätzen 1 und 2 kann das Bundesamt für Sicherheit in der Informationstechnik auch selbst vornehmen und eine Kontaktstelle benennen, wenn der Betreiber seine Pflicht zur Registrierung nicht erfüllt. Nimmt das Bundesamt für Sicherheit in der Informationstechnik eine solche Registrierung selbst vor, informiert es sowohl den betreffenden Betreiber als auch die Bundesnetzagentur darüber und übermittelt die damit verbundenen Kontaktdaten. Jeder Betreiber hat sicherzustellen, dass er über die benannte oder durch das Bundesamt für Sicherheit in der Informationstechnik festgelegte Kontaktstelle jederzeit erreichbar ist. Die Übermittlung von Informationen durch das Bundesamt für Sicherheit in der Informationstechnik nach § 40 Absatz 3 Nummer 4 Buchstabe a des BSI-Gesetzes erfolgt an diese Kontaktstelle.	BSI-Gesetzes zu übermitteln. § 28 Absatz 1 Satz 2 sowie § 28 Absatz 2 Satz 2 des BSI-Gesetzes bleiben unberührt. § 33 Absatz 2, 4 und 5 des BSI-Gesetzes ist entsprechend anzuwenden. Das Bundesamt für Sicherheit in der Informationstechnik übermittelt die Registrierungen nach den Sätzen 1 und 2 einschließlich der damit verbundenen Kontaktdaten und jede Änderung der Registrierungen unverzüglich an die Bundesnetzagentur. Die Registrierungen nach den Sätzen 1 und 2 kann das Bundesamt für Sicherheit in der Informationstechnik auch selbst vornehmen und eine Kontaktstelle benennen, wenn der Betreiber seine Pflicht zur Registrierung nicht erfüllt. Nimmt das Bundesamt für Sicherheit in der Informationstechnik eine solche Registrierung selbst vor, informiert es sowohl den betreffenden Betreiber als auch die Bundesnetzagentur darüber und übermittelt die damit verbundenen Kontaktdaten. Jeder Betreiber hat sicherzustellen, dass er über die benannte oder durch das Bundesamt für Sicherheit in der Informationstechnik festgelegte Kontaktstelle jederzeit erreichbar ist. Die Übermittlung von Informationen durch das Bundesamt für Sicherheit in der Informationstechnik nach § 40 Absatz 3 Nummer 4 Buchstabe a des BSI-Gesetzes erfolgt an diese Kontaktstelle.

Entwurf	Beschlüsse des 4. Ausschusses
(9) Geschäftsleitungen eines Betreibers eines Energieversorgungsnetzes oder eines Betreibers einer Energieanlage, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist und dessen Energieanlage an ein Energieversorgungsnetz angeschlossen ist, sind verpflichtet, die Sicherheitsanforderungen nach Absatz 1 oder Absatz 2 umzusetzen und ihre Umsetzung zu überwachen. § 28 Absatz 1 Satz 2 sowie § 28 Absatz 2 Satz 2 des BSI-Gesetzes bleiben unberührt.	(10) Geschäftsleitungen eines Betreibers eines Energieversorgungsnetzes oder eines Betreibers einer Energieanlage, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist und dessen Energieanlage an ein Energieversorgungsnetz angeschlossen ist, oder eines Betreibers eines digitalen Energiedienstes, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist, sind verpflichtet, die Sicherheitsanforderungen nach Absatz 1, Absatz 2 oder Absatz 3 umzusetzen und ihre Umsetzung zu überwachen. § 28 Absatz 1 Satz 2 sowie § 28 Absatz 2 Satz 2 des BSI-Gesetzes bleiben unberührt.
(10) Geschäftsleitungen, die ihre Pflichten nach Absatz 9 verletzen, haften ihrer Einrichtung für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Einrichtung anwendbaren Regeln des Gesellschaftsrechts. Nach diesem Gesetz haften sie nur, wenn die für die Einrichtung maßgeblichen gesellschaftsrechtlichen Bestimmungen keine Haftungsregelung nach Satz 1 enthalten.	(11) Geschäftsleitungen, die ihre Pflichten nach Absatz 9 verletzen, haften ihrer Einrichtung für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Einrichtung anwendbaren Regeln des Gesellschaftsrechts. Nach diesem Gesetz haften sie nur, wenn die für die Einrichtung maßgeblichen gesellschaftsrechtlichen Bestimmungen keine Haftungsregelung nach Satz 1 enthalten.

Entwurf	Beschlüsse des 4. Ausschusses
(11) Die Geschäftsleitungen eines Betreibers eines Energieversorgungsnetzes oder eines Betreibers einer Energieanlage, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist und dessen Energieanlage an ein Energieversorgungsnetz angeschlossen ist, müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können. § 28 Absatz 1 Satz 2 sowie § 28 Absatz 2 Satz 2 des BSI-Gesetzes bleiben unberührt.	(12) Die Geschäftsleitungen eines Betreibers eines Energieversorgungsnetzes oder eines Betreibers einer Energieanlage, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist und dessen Energieanlage an ein Energieversorgungsnetz angeschlossen ist, oder eines Betreibers eines digitalen Energiedienstes, der eine besonders wichtige Einrichtung nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes oder eine wichtige Einrichtung nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes ist, müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können. § 28 Absatz 1 Satz 2 sowie § 28 Absatz 2 Satz 2 des BSI-Gesetzes bleiben unberührt.
(12) Die Bundesnetzagentur legt bis zum Ablauf des … [einsetzen: Datum desjenigen Tages des ersten auf den Monat des Inkrafttretens nach Artikel 33 Absatz 1 Satz 1 dieses Gesetzes folgenden Kalendermonats, dessen Zahl mit der des Tages des Inkrafttretens nach Artikel 33 Absatz 1 Satz 1 dieses Gesetzes übereinstimmt, oder, wenn es einen solchen Kalendertag nicht gibt, Datum des ersten Tages des darauffolgenden Kalendermonats] 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,	(13) Die Bundesnetzagentur legt bis zum Ablauf des … [einsetzen: Datum desjenigen Tages des ersten auf den Monat des Inkrafttretens nach Artikel 33 Absatz 1 Satz 1 dieses Gesetzes folgenden Kalendermonats, dessen Zahl mit der des Tages des Inkrafttretens nach Artikel 33 Absatz 1 Satz 1 dieses Gesetzes übereinstimmt, oder, wenn es einen solchen Kalendertag nicht gibt, Datum des ersten Tages des darauffolgenden Kalendermonats] 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,

Entwurf	Beschlüsse des 4. Ausschusses
1. welche Komponenten kritische Komponenten nach § 2 Nummer 23 Buchstabe c Doppelbuchstabe aa des BSI-Gesetzes sind oder	1. welche Komponenten kritische Komponenten nach § 2 Nummer 23 in Verbindung mit § 56 Absatz 7 Satz 2 des BSI-Gesetzes sind oder
2. welche Funktionen kritisch bestimmte Funktionen nach § 2 Nummer 23 Buchstabe c Doppelbuchstabe bb des BSI-Gesetzes sind.	2. welche Funktionen kritisch bestimmte Funktionen im Sinne von § 56 Absatz 7 Satz 2 Ziffer 3 des BSI-Gesetzes sind.
Der Betreiber eines Energieversorgungsnetzes, das eine kritische Anlage nach § 2 Nummer 22 des BSI-Gesetzes ist, oder der Betreiber einer Energieanlage, die eine kritische Anlage nach § 2 Nummer 22 des BSI-Gesetzes ist, hat die Vorgaben des Katalogs spätestens sechs Monate nach dessen in der Allgemeinverfügung bestimmten Inkrafttreten zu erfüllen, es sei denn, in dem Katalog ist eine davon abweichende Umsetzungsfrist festgelegt worden. Der Katalog wird mit den IT-Sicherheitskatalogen nach den Absätzen 1 und 2 verbunden.“	Der Betreiber eines Energieversorgungsnetzes, das eine kritische Anlage nach § 2 Nummer 22 des BSI-Gesetzes ist, der Betreiber einer Energieanlage, die eine kritische Anlage nach § 2 Nummer 22 des BSI-Gesetzes ist, oder der Betreiber eines digitalen Energiedienstes, der eine kritische Anlage nach § 2 Nummer 22 des BSI-Gesetzes ist, hat die Vorgaben des Katalogs spätestens sechs Monate nach dessen in der Allgemeinverfügung bestimmten Inkrafttreten zu erfüllen, es sei denn, in dem Katalog ist eine davon abweichende Umsetzungsfrist festgelegt worden. Der Katalog wird mit den IT-Sicherheitskatalogen nach den Absätzen 1 und 2 verbunden. Die Befugnis der Bundesnetzagentur nach Satz 1 besteht bis zum Erlass einer Rechtsverordnung nach § 56 Absatz 7 für den Sektor Energie im Sinne des § 2 Nr. 24 fort. Eine von der Bundesnetzagentur auf der Grundlage von Satz 1 oder auf der Grundlage von § 11 Absatz 1 Satz 1 EnWG a.F. erlassene Allgemeinverfügung ist mit dem Inkrafttreten einer Rechtsverordnung nach § 56 Absatz 7 BSIG für Energieversorgungsnetze und Energieanlagen aufzuheben“
3. § 11 Absatz 1a bis 1g wird aufgehoben.	3. § 11 Absatz 1a bis 1g wird aufgehoben.
4. § 59 Absatz 1 Nummer 1a wird wie folgt gefasst:	4. § 59 Absatz 1 Nummer 1a wird wie folgt gefasst:
„1a. die Festlegungen nach § 5c Absatz 1, 2 sowie 12,“.	„1a. die Festlegungen nach § 5c Absatz 1, 2 sowie 12,“.

Entwurf	Beschlüsse des 4. Ausschusses
5. In § 91 Absatz 1 Satz 1 Nummer 4 wird nach den Wörtern „Amtshandlungen auf Grund der §§“ die Angabe „5c Absatz 4,“ eingefügt.	5. In § 91 Absatz 1 Satz 1 Nummer 4 wird nach den Wörtern „Amtshandlungen auf Grund der §§“ die Angabe „5c Absatz 4,“ eingefügt.
6. § 95 wird wie folgt geändert:	6. § 95 wird wie folgt geändert:
a) Absatz 1 wird wie folgt geändert:	a) Absatz 1 wird wie folgt geändert:
aa) Die Nummern 2a und 2b werden aufgehoben.	aa) Die Nummern 2a und 2b werden aufgehoben.
bb) Nach Nummer 3a werden die folgenden Nummern 3b bis 3d eingefügt:	bb) Nach Nummer 3a werden die folgenden Nummern 3b bis 3d eingefügt:
„3b. entgegen § 5c Absatz 1 Satz 1 oder Absatz 2 Satz 1 einen dort genannten Schutz nicht gewährleistet,	„3b. entgegen § 5c Absatz 1 Satz 1 oder Absatz 2 Satz 1 einen dort genannten Schutz nicht gewährleistet,
3c. entgegen § 5c Absatz 1 Satz 7 oder Absatz 2 Satz 10 die Einhaltung der Anforderungen des IT-Sicherheitskatalogs nicht, nicht richtig oder nicht vollständig dokumentiert,	3c. entgegen § 5c Absatz 1 Satz 7 oder Absatz 2 Satz 10 die Einhaltung der Anforderungen des IT-Sicherheitskatalogs nicht, nicht richtig oder nicht vollständig dokumentiert,
3d. entgegen § 5c Absatz 6 Satz 1 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,“.	3d. entgegen § 5c Absatz 6 Satz 1 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,“.
cc) Die bisherigen Nummern 3b bis 3d werden die Nummern 3e bis 3g.	cc) Die bisherigen Nummern 3b bis 3d werden die Nummern 3e bis 3g.
dd) Die bisherigen Nummern 3f bis 3i werden die Nummern 3h bis 3k.	dd) Die bisherigen Nummern 3f bis 3i werden die Nummern 3h bis 3k.
b) Nach Absatz 2 werden die folgenden Absätze 2a bis 2d eingefügt:	b) Nach Absatz 2 werden die folgenden Absätze 2a bis 2d eingefügt:
„(2a) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummer 3b bis 3d geahndet werden:	„(2a) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummer 3b bis 3d geahndet werden:

Entwurf	Beschlüsse des 4. Ausschusses
1. bei besonders wichtigen Einrichtungen nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes mit einer Geldbuße bis zu zehn Millionen Euro,	1. bei besonders wichtigen Einrichtungen nach § 28 Absatz 1 Satz 1 des BSI-Gesetzes mit einer Geldbuße bis zu zehn Millionen Euro,
2. bei wichtigen Einrichtungen nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes mit einer Geldbuße bis zu sieben Millionen Euro und	2. bei wichtigen Einrichtungen nach § 28 Absatz 2 Satz 1 des BSI-Gesetzes mit einer Geldbuße bis zu sieben Millionen Euro und
3. in den übrigen Fällen mit einer Geldbuße bis zu einer Million Euro.	3. in den übrigen Fällen mit einer Geldbuße bis zu einer Million Euro.
(2b) Bei einer besonders wichtigen Einrichtung im Sinne des § 28 Absatz 1 Satz 1 des BSI-Gesetzes mit einem Jahresumsatz von mehr als 500 Millionen Euro kann abweichend von Absatz 2a Nummer 1 eine Ordnungswidrigkeit nach Absatz 1 Nummer 3b, 3c und 3d mit einer Geldbuße bis zu 2 Prozent des Jahresumsatzes geahndet werden.	(2b) Bei einer besonders wichtigen Einrichtung im Sinne des § 28 Absatz 1 Satz 1 des BSI-Gesetzes mit einem Jahresumsatz von mehr als 500 Millionen Euro kann abweichend von Absatz 2a Nummer 1 eine Ordnungswidrigkeit nach Absatz 1 Nummer 3b, 3c und 3d mit einer Geldbuße bis zu 2 Prozent des Jahresumsatzes geahndet werden.
(2c) Bei einer wichtigen Einrichtung im Sinne des § 28 Absatz 2 Satz 1 des BSI-Gesetzes mit einem Jahresumsatz von mehr als 500 Millionen Euro kann abweichend von Absatz 2a Nummer 2 eine Ordnungswidrigkeit nach Absatz 1 Nummer 3b, 3c und 3d mit einer Geldbuße bis zu 1,4 Prozent des Jahresumsatzes geahndet werden.	(2c) Bei einer wichtigen Einrichtung im Sinne des § 28 Absatz 2 Satz 1 des BSI-Gesetzes mit einem Jahresumsatz von mehr als 500 Millionen Euro kann abweichend von Absatz 2a Nummer 2 eine Ordnungswidrigkeit nach Absatz 1 Nummer 3b, 3c und 3d mit einer Geldbuße bis zu 1,4 Prozent des Jahresumsatzes geahndet werden.
(2d) § 65 Absatz 8 des BSI-Gesetzes ist entsprechend anzuwenden.“	(2d) § 65 Absatz 8 des BSI-Gesetzes ist entsprechend anzuwenden.“
c) In Absatz 5 wird die Angabe „Nummer 2b“ durch die Angabe „Nummer 3d“ ersetzt.	c) In Absatz 5 wird die Angabe „Nummer 2b“ durch die Angabe „Nummer 3d“ ersetzt.

Entwurf	Beschlüsse des 4. Ausschusses
Artikel 18	**Artikel 18**
Änderung des Messstellenbetriebsgesetzes	**Änderung des Messstellenbetriebsgesetzes**
In § 24 Absatz 2 des Messstellenbetriebsgesetzes vom 29. August 2016 (BGBl. I S. 2034), das zuletzt durch Artikel 7 des Gesetzes vom 8. Mai 2024 (BGBl. 2024 I Nr. 151) geändert worden ist, werden die Wörter „§ 9 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821)“ durch die Wörter „§ 52 des BSI-Gesetzes vom … [einsetzen: Datum und Fundstelle nach Artikel 1 dieses Gesetzes] in der jeweils geltenden Fassung“ ersetzt.	In § 24 Absatz 2 des Messstellenbetriebsgesetzes vom 29. August 2016 (BGBl. I S. 2034), das zuletzt durch Artikel 7 des Gesetzes vom 8. Mai 2024 (BGBl. 2024 I Nr. 151) geändert worden ist, werden die Wörter „§ 9 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821)“ durch die Wörter „§ 52 des BSI-Gesetzes vom … [einsetzen: Datum und Fundstelle nach Artikel 1 dieses Gesetzes] in der jeweils geltenden Fassung“ ersetzt.
Artikel 19	**Artikel 19**
Änderung des Energiesicherungsgesetzes	**Änderung des Energiesicherungsgesetzes**
Das Energiesicherungsgesetz vom 20. Dezember 1974 (BGBl. I S. 3681), das zuletzt durch Artikel 1 des Gesetzes vom 23. Juni 2023 (BGBl. 2023 I Nr. 167) geändert worden ist, wird wie folgt geändert:	Das Energiesicherungsgesetz vom 20. Dezember 1974 (BGBl. I S. 3681), das zuletzt durch Artikel 1 des Gesetzes vom 23. Juni 2023 (BGBl. 2023 I Nr. 167) geändert worden ist, wird wie folgt geändert:
1. Dem § 10 Absatz 1 wird folgender Satz angefügt:	1. Dem § 10 Absatz 1 wird folgender Satz angefügt:
„Soweit Daten im Sinne des Satzes 3 für Maßnahmen nach § 1 der Gassicherungsverordnung vom 26. April 1982 (BGBl. I S. 517), die zuletzt durch Artikel 1 der Verordnung vom 31. März 2023 (BGBl. 2023 Nr. 94) geändert worden ist, und für Solidaritätsmaßnahmen nach § 2a von der Bundesnetzagentur erlangt werden, übermittelt diese die Daten auf deren Ersuchen und soweit dies für die Erfüllung von deren Aufgaben erforderlich ist, an die Bundesanstalt für Finanzdienstleistungsaufsicht.“	„Soweit Daten im Sinne des Satzes 3 für Maßnahmen nach § 1 der Gassicherungsverordnung vom 26. April 1982 (BGBl. I S. 517), die zuletzt durch Artikel 1 der Verordnung vom 31. März 2023 (BGBl. 2023 Nr. 94) geändert worden ist, und für Solidaritätsmaßnahmen nach § 2a von der Bundesnetzagentur erlangt werden, übermittelt diese die Daten auf deren Ersuchen und soweit dies für die Erfüllung von deren Aufgaben erforderlich ist, an die Bundesanstalt für Finanzdienstleistungsaufsicht.“

Entwurf	Beschlüsse des 4. Ausschusses
2. In § 17 Absatz 1, § 18 Absatz 2 Satz 1 Nummer 1 und § 29 Absatz 1 Satz 1 werden jeweils die Wörter „Kritische Infrastrukturen“ durch die Wörter „kritische Anlagen“ und die Wörter „§ 2 Absatz 10 des BSI-Gesetzes“ durch die Wörter „§ 2 Nummer 22 des BSI-Gesetzes“ ersetzt.	2. In § 17 Absatz 1, § 18 Absatz 2 Satz 1 Nummer 1 und § 29 Absatz 1 Satz 1 werden jeweils die Wörter „Kritische Infrastrukturen“ durch die Wörter „kritische Anlagen“ und die Wörter „§ 2 Absatz 10 des BSI-Gesetzes“ durch die Wörter „§ 2 Nummer 22 des BSI-Gesetzes“ ersetzt.
Artikel 20	**Artikel 20**
Änderung des Wärmeplanungsgesetzes	**Änderung des Wärmeplanungsgesetzes**
In § 11 Absatz 4 Satz 1 des Wärmeplanungsgesetzes vom 20. Dezember 2023 (BGBl. 2023 I Nr. 394), werden die Wörter „Kritischen Infrastrukturen“ durch die Wörter „kritischen Anlagen“ und die Wörter „§ 2 Absatz 10 des BSI-Gesetzes 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“ durch die Wörter „§ 2 Nummer 22 des BSI-Gesetzes vom … [einsetzen: Datum und Fundstelle nach Artikel 1 dieses Gesetzes] in der jeweils geltenden Fassung“ ersetzt.	In § 11 Absatz 4 Satz 1 des Wärmeplanungsgesetzes vom 20. Dezember 2023 (BGBl. 2023 I Nr. 394), werden die Wörter „Kritischen Infrastrukturen“ durch die Wörter „kritischen Anlagen“ und die Wörter „§ 2 Absatz 10 des BSI-Gesetzes 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“ durch die Wörter „§ 2 Nummer 22 des BSI-Gesetzes vom … [einsetzen: Datum und Fundstelle nach Artikel 1 dieses Gesetzes] in der jeweils geltenden Fassung“ ersetzt.
Artikel 21	**Artikel 21**
Änderung des Fünften Buches Sozialgesetzbuch	**Änderung des Fünften Buches Sozialgesetzbuch**
Das Fünfte Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung – (Artikel 1 des Gesetzes vom 20. Dezember 1988, BGBl. I S. 2477, 2482), das zuletzt durch Artikel 3 des Gesetzes vom 30. Mai 2024 (BGBl. 2024 I Nr. 173) geändert worden ist, wird wie folgt geändert:	Das Fünfte Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung – (Artikel 1 des Gesetzes vom 20. Dezember 1988, BGBl. I S. 2477, 2482), das zuletzt durch Artikel 3 des Gesetzes vom 30. Juli 2024 (BGBl. 2024 I Nr. 254) geändert worden ist, wird wie folgt geändert:
1. § 391 wird wie folgt geändert:	1. § 391 wird wie folgt geändert:
a) In Absatz 4 werden die Wörter „§ 8a Absatz 2 des BSI-Gesetzes“ durch die Wörter „§ 30 Absatz 8 des BSI-Gesetzes“ ersetzt.	a) In Absatz 4 werden die Wörter „§ 8a Absatz 2 des BSI-Gesetzes“ durch die Wörter „§ 30 Absatz 8 des BSI-Gesetzes“ ersetzt.

Entwurf	Beschlüsse des 4. Ausschusses
b) In Absatz 5 werden die Wörter „Kritischer Infrastrukturen“ durch die Wörter „kritischer Anlagen“ und die Wörter „§ 8a des BSI-Gesetzes“ durch die Wörter „den §§ 30, 31 und 39 des BSI-Gesetzes“ ersetzt.	b) In Absatz 5 werden die Wörter „Kritischer Infrastrukturen“ durch die Wörter „kritischer Anlagen“ und die Wörter „§ 8a des BSI-Gesetzes“ durch die Wörter „den §§ 30, 31 und 39 des BSI-Gesetzes“ ersetzt.
2. § 392 wird wie folgt geändert:	2. § 392 wird wie folgt geändert:
a) In Absatz 3 werden die Wörter „§ 8a Absatz 2 des BSI-Gesetzes“ durch die Wörter „§ 30 Absatz 8 des BSI-Gesetzes“ ersetzt.	a) In Absatz 3 werden die Wörter „§ 8a Absatz 2 des BSI-Gesetzes“ durch die Wörter „§ 30 Absatz 8 des BSI-Gesetzes“ ersetzt.
b) In Absatz 5 werden die Wörter „Kritischer Infrastrukturen“ durch die Wörter „kritischer Anlagen“ und die Wörter „§ 8a des BSI-Gesetzes“ durch die Wörter „den §§ 30, 31 und 39 des BSI-Gesetzes“ ersetzt.	b) In Absatz 5 werden die Wörter „Kritischer Infrastrukturen“ durch die Wörter „kritischer Anlagen“ und die Wörter „§ 8a des BSI-Gesetzes“ durch die Wörter „den §§ 30, 31 und 39 des BSI-Gesetzes“ ersetzt.
Artikel 22	**Artikel 22**
Änderung der Digitale Gesundheitsanwendungen-Verordnung	**Änderung der Digitale Gesundheitsanwendungen-Verordnung**
In Anlage 1 der Digitale Gesundheitsanwendungen-Verordnung vom 8. April 2020 (BGBl. I S. 768), die zuletzt durch Artikel 4 des Gesetzes vom 22. März 2024 (BGBl. 2024 I Nr. 101) geändert worden ist, werden in dem Abschnitt „Datensicherheit“, Unterabschnitt „Basisanforderungen, die für alle digitalen Gesundheitsanwendungen gelten“ in Nummer 5 in der Spalte „Anforderung“ die Wörter „§ 8 Absatz 1 Satz 1 des BSI-Gesetzes“ durch die Wörter „§ 44 Absatz 1 Satz 1 des BSI-Gesetzes“ ersetzt.	In Anlage 1 der Digitale Gesundheitsanwendungen-Verordnung vom 8. April 2020 (BGBl. I S. 768), die zuletzt durch Artikel 4 des Gesetzes vom 22. März 2024 (BGBl. 2024 I Nr. 101) geändert worden ist, werden in dem Abschnitt „Datensicherheit“, Unterabschnitt „Basisanforderungen, die für alle digitalen Gesundheitsanwendungen gelten“ in Nummer 5 in der Spalte „Anforderung“ die Wörter „§ 8 Absatz 1 Satz 1 des BSI-Gesetzes“ durch die Wörter „§ 44 Absatz 1 Satz 1 des BSI-Gesetzes“ ersetzt.

Entwurf	Beschlüsse des 4. Ausschusses
Artikel 23	**Artikel 23**
Änderung des Sechsten Buches Sozialgesetzbuch	**Änderung des Sechsten Buches Sozialgesetzbuch**
Das Sechste Buch Sozialgesetzbuch – Gesetzliche Rentenversicherung – in der Fassung der Bekanntmachung vom 19. Februar 2002 (BGBl. I S. 754, 1404, 3384), das zuletzt durch Artikel 1 des Gesetzes vom 30. Mai 2024 (BGBl. 2024 I Nr. 173) geändert worden ist, wird wie folgt geändert:	Das Sechste Buch Sozialgesetzbuch – Gesetzliche Rentenversicherung – in der Fassung der Bekanntmachung vom 19. Februar 2002 (BGBl. I S. 754, 1404, 3384), das zuletzt durch Artikel 1 des Gesetzes vom 30. Mai 2024 (BGBl. 2024 I Nr. 173) geändert worden ist, wird wie folgt geändert:
1. Die Inhaltsübersicht wird wie folgt geändert:	1. Die Inhaltsübersicht wird wie folgt geändert:
a) Nach der Angabe zu § 145 wird folgende Angabe eingefügt:	a) Nach der Angabe zu § 145 wird folgende Angabe eingefügt:
„Achter Unterabschnitt	„Achter Unterabschnitt
Sicherheit in der Informationstechnik“.	Sicherheit in der Informationstechnik“.
b) Die Angabe zu § 146 wird wie folgt gefasst:	b) Die Angabe zu § 146 wird wie folgt gefasst:
„§ 146 Verbindliche Entscheidungen zur Sicherheit der Informationstechnik“.	„§ 146 Verbindliche Entscheidungen zur Sicherheit der Informationstechnik“.
2. § 138 Absatz 1 Satz 2 wird wie folgt geändert:	2. § 138 Absatz 1 Satz 2 wird wie folgt geändert:
a) In Nummer 15 wird das Wort „und“ am Ende durch ein Komma ersetzt.	a) In Nummer 15 wird das Wort „und“ am Ende durch ein Komma ersetzt.
b) In Nummer 16 wird der Punkt am Ende durch das Wort „und“ ersetzt.	b) In Nummer 16 wird der Punkt am Ende durch das Wort „und“ ersetzt.
c) Folgende Nummer 17 wird angefügt:	c) Folgende Nummer 17 wird angefügt:
„17. Koordinierung einer an den Zielen von Wirtschaftlichkeit und Sicherheit ausgerichteten Informationstechnik der Rentenversicherung.“	„17. Koordinierung einer an den Zielen von Wirtschaftlichkeit und Sicherheit ausgerichteten Informationstechnik der Rentenversicherung.“
3. Nach § 145 wird folgende Überschrift eingefügt:	3. Nach § 145 wird folgende Überschrift eingefügt:

Entwurf	Beschlüsse des 4. Ausschusses
„Achter Unterabschnitt	„Achter Unterabschnitt
Sicherheit in der Informationstechnik“.	Sicherheit in der Informationstechnik“.
4. § 146 wird wie folgt gefasst:	4. § 146 wird wie folgt gefasst:
„§ 146	„§ 146
Verbindliche Entscheidungen zur Sicherheit der Informationstechnik	Verbindliche Entscheidungen zur Sicherheit der Informationstechnik
Die Deutsche Rentenversicherung Bund hat in Wahrnehmung der ihr nach § 138 Absatz 1 Satz 2 Nummer 17 zugewiesenen Aufgaben bis 30. Juni 2025 folgende verbindliche Entscheidungen herbeizuführen:	Die Deutsche Rentenversicherung Bund hat in Wahrnehmung der ihr nach § 138 Absatz 1 Satz 2 Nummer 17 zugewiesenen Aufgaben bis 30. Juni 2025 folgende verbindliche Entscheidungen herbeizuführen:
1. zur Festlegung von einheitlichen Grundsätzen für die Informationstechnik und Informationssicherheit der Rentenversicherung,	1. zur Festlegung von einheitlichen Grundsätzen für die Informationstechnik und Informationssicherheit der Rentenversicherung,
2. zum Betrieb der informationstechnischen Infrastruktur und des Netzwerkes der Rentenversicherung,	2. zum Betrieb der informationstechnischen Infrastruktur und des Netzwerkes der Rentenversicherung,
3. zur Entwicklung rentenversicherungsbezogener Anwendungen und	3. zur Entwicklung rentenversicherungsbezogener Anwendungen und
4. zur Festlegung eines Beschaffungskonzepts.	4. zur Festlegung eines Beschaffungskonzepts.
Satz 1 gilt im Verhältnis zur Deutschen Rentenversicherung Knappschaft-Bahn-See mit der Maßgabe, dass notwendige Abweichungen wegen der dieser übertragenen weiteren gesetzlichen Aufgaben und ihrer spezifischen Leistungen zulässig sind.“	Satz 1 gilt im Verhältnis zur Deutschen Rentenversicherung Knappschaft-Bahn-See mit der Maßgabe, dass notwendige Abweichungen wegen der dieser übertragenen weiteren gesetzlichen Aufgaben und ihrer spezifischen Leistungen zulässig sind.“

Entwurf	Beschlüsse des 4. Ausschusses
Artikel 24	**Artikel 24**
Änderung der Verordnung zum Barrierefreiheitsstärkungsgesetz	**Änderung der Verordnung zum Barrierefreiheitsstärkungsgesetz**
In § 2 Nummer 3 der Verordnung zum Barrierefreiheitsstärkungsgesetz vom 15. Juni 2022 (BGBl. I S. 928) werden die Wörter „§ 2 Absatz 2 Satz 4 des BSI-Gesetzes 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“ durch die Wörter „§ 2 Nummer 39 des BSI-Gesetzes vom … [einsetzen: Datum und Fundstelle dieses Gesetzes]“.	In § 2 Nummer 3 der Verordnung zum Barrierefreiheitsstärkungsgesetz vom 15. Juni 2022 (BGBl. I S. 928) werden die Wörter „§ 2 Absatz 2 Satz 4 des BSI-Gesetzes 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“ durch die Wörter „§ 2 Nummer 39 des BSI-Gesetzes vom … [einsetzen: Datum und Fundstelle dieses Gesetzes]“.
Artikel 25	**Artikel 25**
Änderung des Elften Buches Sozialgesetzbuch	**Änderung des Elften Buches Sozialgesetzbuch**
§ 103a des Elften Buch Sozialgesetzbuch – Soziale Pflegeversicherung – (Artikel 1 des Gesetzes vom 26. Mai 1994, BGBl. I S. 1014, 1015), das zuletzt durch Artikel 4 des Gesetzes vom 30. Mai 2024 (BGBl. 2024 I Nr. 173) geändert worden ist, wird wie folgt geändert:	§ 103a des Elften Buch Sozialgesetzbuch – Soziale Pflegeversicherung – (Artikel 1 des Gesetzes vom 26. Mai 1994, BGBl. I S. 1014, 1015), das zuletzt durch Artikel 4 des Gesetzes vom 30. Mai 2024 (BGBl. 2024 I Nr. 173) geändert worden ist, wird wie folgt geändert:
1. In Absatz 3 werden die Wörter „§ 8a Absatz 2 des BSI-Gesetzes“ durch die Wörter „§ 30 Absatz 8 des BSI-Gesetzes“ ersetzt.	1. In Absatz 3 werden die Wörter „§ 8a Absatz 2 des BSI-Gesetzes“ durch die Wörter „§ 30 Absatz 8 des BSI-Gesetzes“ ersetzt.
2. In Absatz 5 werden die Wörter „Kritischer Infrastrukturen“ durch die Wörter „kritischer Anlagen“ und die Wörter „§ 8a des BSI-Gesetzes“ durch die Wörter „den §§ 30, 31 und 39 des BSI-Gesetzes“ ersetzt.	2. In Absatz 5 werden die Wörter „Kritischer Infrastrukturen“ durch die Wörter „kritischer Anlagen“ und die Wörter „§ 8a des BSI-Gesetzes“ durch die Wörter „den §§ 30, 31 und 39 des BSI-Gesetzes“ ersetzt.

Entwurf	Beschlüsse des 4. Ausschusses
Artikel 26	**Artikel 26**
Änderung des Telekommunikationsgesetzes	**Änderung des Telekommunikationsgesetzes**
Das Telekommunikationsgesetz vom 23. Juni 2021 (BGBl. I S. 1858), das zuletzt durch Artikel 35 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist, wird wie folgt geändert:	Das Telekommunikationsgesetz vom 23. Juni 2021 (BGBl. I S. 1858), das zuletzt durch Artikel 35 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist, wird wie folgt geändert:
1. In der Inhaltsübersicht wird die Angabe zu § 168 wie folgt gefasst:	1. In der Inhaltsübersicht wird die Angabe zu § 168 wie folgt gefasst:
„§ 168 Meldung eines Sicherheitsvorfalls“.	„§ 168 Meldung eines Sicherheitsvorfalls“.
2. § 3 wird wie folgt geändert:	2. § 3 wird wie folgt geändert:
a) Nummer 53 wird wie folgt gefasst:	a) Nummer 53 wird wie folgt gefasst:
„53. „Sicherheitsvorfall“ ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden oder zugänglich sind, beeinträchtigt;“.	„53. „Sicherheitsvorfall“ ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden oder zugänglich sind, beeinträchtigt;“.
b) In Nummer 79 wird der Punkt am Ende durch ein Semikolon ersetzt.	b) In Nummer 79 wird der Punkt am Ende durch ein Semikolon ersetzt.
c) Folgende Nummer 80 wird angefügt:	c) Folgende Nummer 80 wird angefügt:
„80. „Netz- und Informationssystem“	„80. „Netz- und Informationssystem“
a) ein Telekommunikationsnetz im Sinne von Nummer 65,	a) ein Telekommunikationsnetz im Sinne von Nummer 65,

Entwurf	Beschlüsse des 4. Ausschusses
b) ein Gerät oder eine Gruppe miteinander verbundener oder zusammenhängender Geräte, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung digitaler Daten durchführen, oder	b) ein Gerät oder eine Gruppe miteinander verbundener oder zusammenhängender Geräte, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung digitaler Daten durchführen, oder
c) digitale Daten, die von den in den Buchstaben a und b genannten Elementen zum Zwecke ihres Betriebs, ihrer Nutzung, ihres Schutzes und ihrer Pflege gespeichert, verarbeitet, abgerufen oder übertragen werden.“	c) digitale Daten, die von den in den Buchstaben a und b genannten Elementen zum Zwecke ihres Betriebs, ihrer Nutzung, ihres Schutzes und ihrer Pflege gespeichert, verarbeitet, abgerufen oder übertragen werden.“
	3. In § 79 Absatz 3 Nummer 3 und § 151 Absatz 1 Satz 2 werden jeweils die Wörter „Kritische Infrastrukturen“ durch die Wörter „kritische Anlagen“ ersetzt.
	4. In § 79 Absatz 3 Nummer 3, § 136 Absatz 4 Nummer 3, § 137 Absatz 3 Nummer 3, § 141 Absatz 2 Nummer 4, § 142 Absatz 4 Nummer 4 und § 143 Absatz 4 Nummer 1 werden jeweils die Wörter „der Kritischen Infrastruktur“ durch die Wörter „kritischer Anlagen“ ersetzt.
	5. In § 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 und § 174 Absatz 3 Nummer 8, Absatz 5 Nummer 8 werden jeweils die Wörter „Kritischen Infrastruktur“ durch die Wörter „kritischen Anlage“ ersetzt.
	6. In § 141 Absatz 2 Nummer 4 erster und zweiter Halbsatz, § 151 Absatz 1 Satz 2 und 3, Absatz 2 Satz 3, Absatz 3 Satz 2 und 3, § 153 Absatz 4 Nummer 3 und § 154 Absatz 4 Satz 2 Nummer 4 werden jeweils die Wörter „Kritischer Infrastrukturen“ durch die Wörter „kritischer Anlagen“ ersetzt.

Entwurf	Beschlüsse des 4. Ausschusses
	7. In § 141 Absatz 2 Nummer 4 werden die Wörter „Kritischen Infrastrukturen“ durch die Wörter „kritischen Anlagen“ ersetzt.
3. § 165 wird wie folgt geändert:	8. § 165 wird wie folgt geändert:
a) Absatz 2 Satz 3 wird durch die folgende Sätze ersetzt:	a) Absatz 2 Satz 3 wird durch die folgende Sätze ersetzt:
„Bei diesen Maßnahmen ist unter Berücksichtigung des Stands der Technik, der einschlägigen europäischen und internationalen Normen sowie der Umsetzungskosten ein Sicherheitsniveau der Netz- und Informationssysteme zu 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 des Betreibers oder des Anbieters sowie die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen.“	„Bei diesen Maßnahmen ist unter Berücksichtigung des Stands der Technik, der einschlägigen europäischen und internationalen Normen sowie der Umsetzungskosten ein Sicherheitsniveau der Netz- und Informationssysteme zu 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 des Betreibers oder des Anbieters sowie die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen.“
b) Nach Absatz 2 werden die folgenden Absätze 2a bis 2d eingefügt:	b) Nach Absatz 2 werden die folgenden Absätze 2a bis 2d eingefügt:
„(2a) Maßnahmen nach Absatz 2 von Betreibern öffentlicher Telekommunikationsnetze und Anbietern öffentlich zugänglicher Telekommunikationsdienste, die besonders wichtige Einrichtungen im Sinne von § 28 Absatz 1 Satz 1 Nummer 3 des BSI-Gesetzes oder wichtige Einrichtungen im Sinne von § 28 Absatz 2 Satz 1 Nummer 2 des BSI-Gesetzes sind, müssen auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen, und zumindest Folgendes umfassen:	„(2a) Maßnahmen nach Absatz 2 von Betreibern öffentlicher Telekommunikationsnetze und Anbietern öffentlich zugänglicher Telekommunikationsdienste, die besonders wichtige Einrichtungen im Sinne von § 28 Absatz 1 Satz 1 Nummer 3 des BSI-Gesetzes oder wichtige Einrichtungen im Sinne von § 28 Absatz 2 Satz 1 Nummer 2 des BSI-Gesetzes sind, müssen auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen, und zumindest Folgendes umfassen:

Entwurf	Beschlüsse des 4. Ausschusses
1. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme,	1. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme,
2. Bewältigung von Sicherheitsvorfällen,	2. Bewältigung von Sicherheitsvorfällen,
3. Aufrechterhaltung des Betriebs, wie Backup-Management und Widerherstellung nach einem Notfall, und Krisenmanagement,	3. Aufrechterhaltung des Betriebs, wie Backup-Management und Widerherstellung nach einem Notfall, und Krisenmanagement,
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Dienstleistern,	4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Dienstleistern,
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen,	5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen,
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Maßnahmen nach Absatz 2 im Bereich der Sicherheit von Netzen und Diensten,	6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Maßnahmen nach Absatz 2 im Bereich der Sicherheit von Netzen und Diensten,
7. Grundlegende Verfahren und Schulungen im Bereich der Sicherheit von Netzen und Diensten,	7. Grundlegende Verfahren und Schulungen im Bereich der Sicherheit von Netzen und Diensten,
8. Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,	8. Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung,
9. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen,	9. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen,

Entwurf	Beschlüsse des 4. Ausschusses
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.	10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.
(2b) Die Geschäftsleitungen von Betreibern öffentlicher Telekommunikationsnetze und Anbietern öffentlich zugänglicher Telekommunikationsdienste, die besonders wichtige Einrichtungen im Sinne von § 28 Absatz 1 Satz 1 Nummer 3 des BSI-Gesetzes oder wichtige Einrichtungen im Sinne von § 28 Absatz 2 Satz 1 Nummer 2 des BSI-Gesetzes sind, sind verpflichtet, die von diesen Einrichtungen nach Absatz 2 zu ergreifenden Maßnahmen umzusetzen und ihre Umsetzung zu überwachen.	(2b) Die Geschäftsleitungen von Betreibern öffentlicher Telekommunikationsnetze und Anbietern öffentlich zugänglicher Telekommunikationsdienste, die besonders wichtige Einrichtungen im Sinne von § 28 Absatz 1 Satz 1 Nummer 3 des BSI-Gesetzes oder wichtige Einrichtungen im Sinne von § 28 Absatz 2 Satz 1 Nummer 2 des BSI-Gesetzes sind, sind verpflichtet, die von diesen Einrichtungen nach Absatz 2 zu ergreifenden Maßnahmen umzusetzen und ihre Umsetzung zu überwachen.
(2c) Geschäftsleitungen, die ihre Pflichten nach Absatz 2b verletzen, haften ihrer Einrichtung für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Einrichtung anwendbaren Regeln des Gesellschaftsrechts. Nach diesem Gesetz haften sie nur, wenn die für die Einrichtung maßgeblichen gesellschaftsrechtlichen Bestimmungen keine Haftungsregelung nach Satz 1 enthalten.	(2c) Geschäftsleitungen, die ihre Pflichten nach Absatz 2b verletzen, haften ihrer Einrichtung für einen schuldhaft verursachten Schaden nach den auf die Rechtsform der Einrichtung anwendbaren Regeln des Gesellschaftsrechts. Nach diesem Gesetz haften sie nur, wenn die für die Einrichtung maßgeblichen gesellschaftsrechtlichen Bestimmungen keine Haftungsregelung nach Satz 1 enthalten.

Entwurf	Beschlüsse des 4. Ausschusses
(2d) Die Geschäftsleitungen von Betreibern öffentlicher Telekommunikationsnetze und Anbietern öffentlich zugänglicher Telekommunikationsdienste, die besonders wichtige Einrichtungen im Sinne von § 28 Absatz 1 Satz 1 Nummer 3 des BSI-Gesetzes oder wichtige Einrichtungen im Sinne von § 28 Absatz 2 Satz 1 Nummer 2 des BSI-Gesetzes sind, müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.“	(2d) Die Geschäftsleitungen von Betreibern öffentlicher Telekommunikationsnetze und Anbietern öffentlich zugänglicher Telekommunikationsdienste, die besonders wichtige Einrichtungen im Sinne von § 28 Absatz 1 Satz 1 Nummer 3 des BSI-Gesetzes oder wichtige Einrichtungen im Sinne von § 28 Absatz 2 Satz 1 Nummer 2 des BSI-Gesetzes sind, müssen regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.“
c) In Absatz 3 Satz 1 werden die Wörter „§ 2 Absatz 9b des BSI-Gesetzes“ durch die Wörter „§ 2 Nummer 41 des BSI-Gesetzes“ ersetzt.	c) In Absatz 3 Satz 1 werden die Wörter „§ 2 Absatz 9b des BSI-Gesetzes“ durch die Wörter „§ 2 Nummer 41 des BSI-Gesetzes“ ersetzt.
d) In Absatz 4 werden die Wörter „§ 2 Absatz 13 des BSI-Gesetzes“ durch die Wörter „§ 2 Nummer 23 des BSI-Gesetzes“ ersetzt.	d) In Absatz 4 werden die Wörter „§ 2 Absatz 13 des BSI-Gesetzes“ durch die Wörter „§ 2 Nummer 23 des BSI-Gesetzes“ ersetzt.

Entwurf	Beschlüsse des 4. Ausschusses
e) In Absatz 11 Satz 1 werden die Wörter „Artikel 9 der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1; L 33 vom 7. Februar 2018, S. 5)“ durch die Wörter „Artikel 10 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 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80)“ ersetzt.	e) In Absatz 11 Satz 1 werden die Wörter „Artikel 9 der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1; L 33 vom 7. Februar 2018, S. 5)“ durch die Wörter „Artikel 10 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 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80)“ ersetzt.

Entwurf	Beschlüsse des 4. Ausschusses
4. In § 167 Absatz 1 Satz 1 Nummer 2 werden die Wörter „§ 2 Absatz 13 Satz 1 Nummer 3 Buchstabe b des BSI-Gesetzes“ durch die Wörter „§ 2 Nummer 23 Buchstabe c Doppelbuchstabe bb des BSI-Gesetzes“ und die Wörter „§ 2 Absatz 13 des BSI-Gesetzes“ durch die Wörter „§ 2 Nummer 23 des BSI-Gesetzes“ ersetzt.	9. § 167 wird wie folgt geändert: a) Absatz 1 Satz 1 Nummer 2 wird wie folgt gefasst: „2. welche Funktionen kritische Funktionen sind, die von kritischen Komponenten im Sinne von § 2 Nummer 23 in Verbindung mit § 56 Absatz 7 Satz 2 des BSI-Gesetzes realisiert werden, und“. b) Nach Absatz 1 wird folgender Absatz 2 eingefügt: „(2) Die Befugnis der Bundesnetzagentur nach Absatz 1 Nr. 2 besteht bis zum Erlass einer Rechtsverordnung nach § 56 Absatz 7 des BSI-Gesetzes für den Sektor Informationstechnik und Telekommunikation im Sinne des § 2 Nr. 24 fort. Eine von der Bundesnetzagentur auf der Grundlage von Absatz 1 Nr. 2 erlassene Allgemeinverfügung ist mit dem Inkrafttreten einer Rechtsverordnung nach § 56 Absatz 7 des BSI-Gesetzes für den Sektor Informationstechnik und Tele-kommunikation aufzuheben.“. c) Der bisherige Absatz 2 wird Absatz 3.
5. § 168 wird wie folgt geändert:	10. § 168 wird wie folgt geändert:
a) Die Überschrift wird wie folgt gefasst:	a) Die Überschrift wird wie folgt gefasst:
„§ 168	„§ 168
Meldung eines Sicherheitsvorfalls“.	Meldung eines Sicherheitsvorfalls“.
b) Die Absätze 1 bis 3 werden wie folgt gefasst:	b) Die Absätze 1 bis 3 werden wie folgt gefasst:

Entwurf	Beschlüsse des 4. Ausschusses
„(1) Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, übermittelt der Bundesnetzagentur und dem Bundesamt für Sicherheit in der Informationstechnik:	„(1) Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, übermittelt der Bundesnetzagentur und dem Bundesamt für Sicherheit in der Informationstechnik:
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 Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte;	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 Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte;
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;	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;
3. auf Ersuchen der Bundesnetzagentur oder dem Bundesamt für Sicherheit in der Informationstechnik eine Zwischenmeldung über relevante Statusaktualisierungen;	3. auf Ersuchen der Bundesnetzagentur oder dem Bundesamt für Sicherheit in der Informationstechnik eine Zwischenmeldung über relevante Statusaktualisierungen;
4. spätestens einen Monat nach Übermittlung der Meldung des erheblichen Sicherheitsvorfalls gemäß Nummer 2, vorbehaltlich Absatz 2, eine Abschlussmeldung, die Folgendes enthält:	4. spätestens einen Monat nach Übermittlung der Meldung des erheblichen Sicherheitsvorfalls gemäß Nummer 2, vorbehaltlich Absatz 2, eine Abschlussmeldung, die Folgendes enthält:

Entwurf	Beschlüsse des 4. Ausschusses
a) eine ausführliche Beschreibung des erheblichen Sicherheitsvorfalls, einschließlich seines Schwergrads und seiner Auswirkungen;	a) eine ausführliche Beschreibung des erheblichen Sicherheitsvorfalls, einschließlich seines Schwergrads und seiner Auswirkungen;
b) Angaben zur Art der Bedrohung beziehungsweise zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat;	b) Angaben zur Art der Bedrohung beziehungsweise zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat;
c) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen;	c) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen;
d) Gegebenenfalls die grenzüberschreitenden Auswirkungen des erheblichen Sicherheitsvorfalls.	d) Gegebenenfalls die grenzüberschreitenden Auswirkungen des erheblichen Sicherheitsvorfalls.
§ 42 Absatz 4 und § 43 Absatz 4 des Bundesdatenschutzgesetzes gelten entsprechend.	§ 42 Absatz 4 und § 43 Absatz 4 des Bundesdatenschutzgesetzes gelten entsprechend.
(2) Dauert der erhebliche Sicherheitsvorfall im Zeitpunkt des Absatzes 1 Nummer 4 noch an, legt der Betroffene statt einer Abschlussmeldung zu diesem Zeitpunkt eine Fortschrittsmeldung und eine Abschlussmeldung innerhalb eines Monats nach Abschluss der Bearbeitung des erheblichen Sicherheitsvorfalls vor.	(2) Dauert der erhebliche Sicherheitsvorfall im Zeitpunkt des Absatzes 1 Nummer 4 noch an, legt der Betroffene statt einer Abschlussmeldung zu diesem Zeitpunkt eine Fortschrittsmeldung und eine Abschlussmeldung innerhalb eines Monats nach Abschluss der Bearbeitung des erheblichen Sicherheitsvorfalls vor.
(3) Ein Sicherheitsvorfall gilt als erheblich, wenn	(3) Ein Sicherheitsvorfall gilt als erheblich, wenn
1. er schwerwiegende Betriebsstörungen oder finanzielle Verluste für den betreffenden Betreiber öffentlicher Telekommunikationsnetze oder Anbieter öffentlich zugänglicher Telekommunikationsdienste verursacht hat oder verursachen kann oder	1. er schwerwiegende Betriebsstörungen oder finanzielle Verluste für den betreffenden Betreiber öffentlicher Telekommunikationsnetze oder Anbieter öffentlich zugänglicher Telekommunikationsdienste verursacht hat oder verursachen kann oder

Entwurf	Beschlüsse des 4. Ausschusses
2. er andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.“	2. er andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.“
c) In Absatz 4 wird das Wort „Mitteilungsverfahrens“ durch das Wort „Meldeverfahrens“ ersetzt.	c) In Absatz 4 wird das Wort „Mitteilungsverfahrens“ durch das Wort „Meldeverfahrens“ ersetzt.
d) Nach Absatz 4 wird folgender Absatz 5 eingefügt:	d) Nach Absatz 4 wird folgender Absatz 5 eingefügt:
„(5) Die Bundesnetzagentur übermittelt den nach Absatz 1 Satz 1 Verpflichteten unverzüglich und nach Möglichkeit innerhalb von 24 Stunden nach der frühen Erstmeldung nach Absatz 1 Satz 1 Nummer 1 eine Bestätigung über den Eingang der Meldung. Das Bundesamt für Sicherheit in der Informationstechnik kann auf Ersuchen der nach Absatz 1 Satz 1 Verpflichteten zusätzliche technische Unterstützung, Orientierungshilfen oder operative Beratung zu Abhilfemaßnahmen leisten. Das Bundesamt für Sicherheit in der Informationstechnik informiert die Bundesnetzagentur über Maßnahmen nach Satz 2.“	„(5) Die Bundesnetzagentur übermittelt den nach Absatz 1 Satz 1 Verpflichteten unverzüglich und nach Möglichkeit innerhalb von 24 Stunden nach der frühen Erstmeldung nach Absatz 1 Satz 1 Nummer 1 eine Bestätigung über den Eingang der Meldung. Das Bundesamt für Sicherheit in der Informationstechnik kann auf Ersuchen der nach Absatz 1 Satz 1 Verpflichteten zusätzliche technische Unterstützung, Orientierungshilfen oder operative Beratung zu Abhilfemaßnahmen leisten. Das Bundesamt für Sicherheit in der Informationstechnik informiert die Bundesnetzagentur über Maßnahmen nach Satz 2.“
e) Der bisherige Absatz 5 wird Absatz 6 und wird wie folgt gefasst:	e) Der bisherige Absatz 5 wird Absatz 6 und wird wie folgt gefasst:

Entwurf	Beschlüsse des 4. Ausschusses
„(6) Erforderlichenfalls unterrichtet die Bundesnetzagentur die nationalen Regulierungsbehörden der anderen Mitgliedstaaten der Europäischen Union und die Agentur der Europäischen Union für Cybersicherheit über den Sicherheitsvorfall. Ist eine Sensibilisierung der Öffentlichkeit erforderlich, um einen erheblichen Sicherheitsvorfall zu verhindern oder zu bewältigen, oder liegt die Offenlegung des erheblichen Sicherheitsvorfalls anderweitig im öffentlichen Interesse, so kann die Bundesnetzagentur nach Anhörung der nach Absatz 1 Satz 1 Verpflichteten die Öffentlichkeit unterrichten oder die nach Absatz 1 Satz 1 Verpflichteten zu dieser Unterrichtung verpflichten.“	„(6) Erforderlichenfalls unterrichtet die Bundesnetzagentur die nationalen Regulierungsbehörden der anderen Mitgliedstaaten der Europäischen Union und die Agentur der Europäischen Union für Cybersicherheit über den Sicherheitsvorfall. Ist eine Sensibilisierung der Öffentlichkeit erforderlich, um einen erheblichen Sicherheitsvorfall zu verhindern oder zu bewältigen, oder liegt die Offenlegung des erheblichen Sicherheitsvorfalls anderweitig im öffentlichen Interesse, so kann die Bundesnetzagentur nach Anhörung der nach Absatz 1 Satz 1 Verpflichteten die Öffentlichkeit unterrichten oder die nach Absatz 1 Satz 1 Verpflichteten zu dieser Unterrichtung verpflichten.“
f) Der bisherige Absatz 6 wird Absatz 7 und die Wörter „§ 8e des BSI-Gesetzes“ wird durch die Wörter „§ 42 des BSI-Gesetzes“ ersetzt.	f) Der bisherige Absatz 6 wird Absatz 7 und die Wörter „§ 8e des BSI-Gesetzes“ wird durch die Wörter „§ 42 des BSI-Gesetzes“ ersetzt.
g) Der bisherige Absatz 7 wird Absatz 8.	g) Der bisherige Absatz 7 wird Absatz 8.
6. In § 174 Absatz 3 Nummer 8 und Absatz 5 Nummer 8 werden die Wörter „Bereichen des § 2 Absatz 10 Satz 1 Nummer 1 des BSI-Gesetzes“ durch die Wörter „Sektoren des § 2 Nummer 24 des BSI-Gesetzes“ ersetzt.	11. In § 174 Absatz 3 Nummer 8 und Absatz 5 Nummer 8 werden die Wörter „Bereichen des § 2 Absatz 10 Satz 1 Nummer 1 des BSI-Gesetzes“ durch die Wörter „Sektoren des § 2 Nummer 24 des BSI-Gesetzes“ ersetzt.
7. In § 214 Absatz 3 werden die Wörter „Kritische Infrastrukturen“ durch die Wörter „kritische Anlagen“ und die Wörter „§ 2 Absatz 10 des BSI-Gesetzes“ durch die Angabe „§ 2 Nummer 22 des BSI-Gesetzes“ ersetzt.	12. In § 214 Absatz 3 werden die Wörter „Kritische Infrastrukturen“ durch die Wörter „kritische Anlagen“ und die Wörter „§ 2 Absatz 10 des BSI-Gesetzes“ durch die Angabe „§ 2 Nummer 22 des BSI-Gesetzes“ ersetzt.
8. In § 228 Absatz 2 Nummer 39 werden die Wörter „eine Mitteilung“ durch die Wörter „eine Meldung oder Mitteilung“ ersetzt.	13. In § 228 Absatz 2 Nummer 39 werden die Wörter „eine Mitteilung“ durch die Wörter „eine Meldung oder Mitteilung“ ersetzt.

Entwurf	Beschlüsse des 4. Ausschusses
Artikel 27	**Artikel 27**
Änderung der Krankenhausstrukturfonds-Verordnung	**Änderung der Krankenhausstrukturfonds-Verordnung**
Die Krankenhausstrukturfonds-Verordnung vom 17. Dezember 2015 (BGBl. I S. 2350), die zuletzt durch Artikel 6 des Gesetzes vom 20. Dezember 2022 (BGBl. I S. 2793) geändert worden ist, wird wie folgt geändert:	Die Krankenhausstrukturfonds-Verordnung vom 17. Dezember 2015 (BGBl. I S. 2350), die zuletzt durch Artikel 6 des Gesetzes vom 20. Dezember 2022 (BGBl. I S. 2793) geändert worden ist, wird wie folgt geändert:
1. In § 11 Absatz 1 Nummer 4 Buchstabe a werden nach den Wörtern „Anhangs 5 Teil 3 der BSI-Kritisverordnung“ die Wörter „vom 22. April 2016 (BGBl. I S. 958), die zuletzt durch Artikel 1 der Verordnung vom 29. November 2023 (BGBl. 2023 I Nr. 339) geändert worden ist,“ eingefügt und werden die Wörter „an die Vorgaben von § 8a des BSI-Gesetzes“ durch die Wörter „an die Anforderungen der §§ 30, 31 und 39 des BSI-Gesetzes“ ersetzt.	1. In § 11 Absatz 1 Nummer 4 Buchstabe a werden nach den Wörtern „Anhangs 5 Teil 3 der BSI-Kritisverordnung“ die Wörter „vom 22. April 2016 (BGBl. I S. 958), die zuletzt durch Artikel 1 der Verordnung vom 29. November 2023 (BGBl. 2023 I Nr. 339) geändert worden ist,“ eingefügt und werden die Wörter „an die Vorgaben von § 8a des BSI-Gesetzes“ durch die Wörter „an die Anforderungen der §§ 30, 31 und 39 des BSI-Gesetzes“ ersetzt.
2. In § 14 Absatz 2 Nummer 8 werden die Wörter „an die Vorgaben von § 8a des BSI-Gesetzes“ durch die Wörter „an die Anforderungen der §§ 30, 31 und 39 des BSI-Gesetzes“ ersetzt.	2. In § 14 Absatz 2 Nummer 8 werden die Wörter „an die Vorgaben von § 8a des BSI-Gesetzes“ durch die Wörter „an die Anforderungen der §§ 30, 31 und 39 des BSI-Gesetzes“ ersetzt.
Artikel 28	**Artikel 28**
Änderung der Außenwirtschaftsverordnung	**Änderung der Außenwirtschaftsverordnung**
§ 55a Absatz 1 der Außenwirtschaftsverordnung vom 2. August 2013 (BGBl. I S. 2865), die zuletzt durch Artikel 3 des Gesetzes vom 27. Februar 2024 (BGBl. 2024 I Nr. 71) geändert worden ist, wird wie folgt geändert:	§ 55a Absatz 1 der Außenwirtschaftsverordnung vom 2. August 2013 (BGBl. I S. 2865), die zuletzt durch Artikel 1 der Verordnung vom 17. Juli 2024 (BGBl. 2024 I Nr. 243) geändert worden ist , wird wie folgt geändert:
1. In Nummer 1 werden die Wörter „Kritischen Infrastruktur“ durch die Wörter „kritischen Anlage“ ersetzt.	1. In Nummer 1 werden die Wörter „Kritischen Infrastruktur“ durch die Wörter „kritischen Anlage“ ersetzt.

Entwurf	Beschlüsse des 4. Ausschusses
2. In Nummer 2 werden die Wörter „§ 2 Absatz 13 des BSI-Gesetzes“ durch die Wörter „§ 2 Nummer 23 des BSI-Gesetzes“ und die Wörter „Kritischen Infrastrukturen“ durch die Wörter „kritischen Anlagen“ ersetzt.	2. In Nummer 2 werden die Wörter „§ 2 Absatz 13 des BSI-Gesetzes“ durch die Wörter „§ 2 Nummer 23 des BSI-Gesetzes“ und die Wörter „Kritischen Infrastrukturen“ durch die Wörter „kritischen Anlagen“ ersetzt.
Artikel 29	**Artikel 29**
Änderung des Vertrauensdienstegesetzes	**Änderung des Vertrauensdienstegesetzes**
§ 2 Absatz 3 des Vertrauensdienstegesetzes 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, wird aufgehoben.	§ 2 Absatz 3 des Vertrauensdienstegesetzes 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, wird aufgehoben.
Artikel 30	
Weitere Änderung des BSI-Gesetzes	
Das BSI-Gesetz, das durch Artikel 1 dieses Gesetzes neu gefasst worden ist, wird wie folgt geändert:	
1. § 2 wird wie folgt geändert:	
a) Nummer 22 wird wie folgt gefasst: „22.„kritische Anlage“ eine Anlage im Sinne von § 2 Nummer 3 des Dachgesetzes zur Stärkung der physischen Resilienz kritischer Anlagen (KRITIS-Dachgesetz);“.	
b) In Nummer 23 werden die Wörter „§ 2 Nummer 24“ durch die Wörter „§ 4 Absatz 1 des KRITIS-Dachgesetzes“ ersetzt.	
c) Nummer 24 wird aufgehoben.	
2. In §12 Absatz 1 Satz 2 wird die Angabe „§ 2 Nummer 24“ durch die Wörter „§ 4 Absatz 1 des KRITIS-Dachgesetzes“ ersetzt.	

Entwurf	Beschlüsse des 4. Ausschusses
3. § 28 Absatz 7 wird aufgehoben.	
4. In § 33 Absatz 2 Satz 1 und § 41 Absatz 2 Satz 1, Absatz 3 Satz 4, Absatz 4 Satz 1, Absatz 6 Satz 1 und Absatz 7 werden jeweils die Wörter „§ 56 Absatz 4“ durch die Wörter „§ 5 Absatz 1 in Verbindung mit § 4 Absatz 3 des KRITIS-Dachgesetzes“ ersetzt.	
5. § 56 Absatz 4 wird aufgehoben.	
6. In § 65 Absatz 1, 2 Nummer 6 und 10 werden jeweils die Wörter „§ 56 Absatz 4 Satz 1“ jeweils durch die Wörter „§ 5 Absatz 1 in Verbindung mit § 4 Absatz 3 des KRITIS-Dachgesetzes“ ersetzt.	
Artikel 31	
Weitere Änderung des Telekommunikationsgesetzes	
In § 174 Absatz 3 Nummer 8 und Absatz 5 Nummer 8 des Telekommunikationsgesetzes vom 23. Juni 2021 (BGBl. I S. 1858), das zuletzt durch Artikel 26 dieses Gesetzes geändert worden ist, werden jeweils die Wörter „§ 2 Nummer 24 des BSI-Gesetzes“ durch die Wörter „§ 4 Absatz 1 des KRITIS-Dachgesetzes“ ersetzt.	
Artikel 32	
Weitere Änderung der Außenwirtschaftsverordnung	
In § 55a Absatz 1 Nummer 1 und 2 der Außenwirtschaftsverordnung vom 2. August 2013 (BGBl. I S. 2865; 2021 I S. 4304), die zuletzt durch Artikel 28 dieses Gesetzes geändert worden ist, werden die Wörter „im Sinne des BSI-Gesetzes“ durch die Wörter „gemäß § 2 Nummer 3 des KRITIS-Dachgesetzes“ ersetzt.	

Entwurf	Beschlüsse des 4. Ausschusses
Artikel 33	**Artikel 30**
Inkrafttreten, Außerkrafttreten	**Inkrafttreten, Außerkrafttreten**
(1) Dieses Gesetz tritt vorbehaltlich des Absatzes 2 am Tag nach der Verkündung in Kraft. Gleichzeitig tritt das BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821) außer Kraft.	(1) Dieses Gesetz tritt vorbehaltlich des § 43 Absatz 7 des Artikel 1 am Tag nach der Verkündung in Kraft. Gleichzeitig tritt das BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821) außer Kraft.
(2) Die Artikel 30, 31 und 32 treten an dem Tag in Kraft, an dem die Rechtsverordnung nach § 5 Absatz 1 in Verbindung mit § 4 Absatz 3 des Dachgesetzes zur Stärkung der physischen Resilienz kritischer Anlagen (KRITIS-Dachgesetz) in Kraft tritt, aber nicht vor dem Inkrafttretenstermin nach Absatz 1. Das Bundesministerium des Innern und für Heimat gibt den Tag des Inkrafttretens im Bundesgesetzblatt bekannt.	(2) Der § 43 Absatz 7 des Artikel 1 tritt am 1. Januar 2027 in Kraft.

Begründung

Zur Begründung allgemein wird auf Drucksache 20/13184 verwiesen. Die Änderungen begründen sich wie folgt:

[Hinweis: Die im Entwurf enthaltenen Verweise auf das Dachgesetz zur Stärkung der physischen Resilienz kritischer Anlagen (KRITIS-Dachgesetz) entsprechen weiterhin denjenigen des Referentenentwurfs mit Bearbeitungsstand 10.09.2024 16:41, Änderungen waren nicht erforderlich. Etwaig nachfolgende Änderungen sind im finalen Beschluss des Innenausschusses noch nachzutragen.]

Zu Artikel 1 (BSI-Gesetz)

Zu § 1

Die Änderungen in § 1 schreiben die mit dem IT-Sicherheitsgesetz 2.0 eingeleitete Stärkung der Unabhängigkeit des Bundesamtes fort. Das Bundesamt ist nach Satz 1 eine selbstständige Bundesoberbehörde, die eigene Aufgaben wahrnimmt. Das Bundesamt bleibt eine Behörde der unmittelbaren Bundesverwaltung und dem Bundesministerium des Innern und für Heimat nachgeordnet.

Als Instrument der Strategie- und Programmplanung und Mittel der Fachaufsicht erstellen nach Satz 4 das Bundesamt und das Bundesministerium des Innern und für Heimat gemeinsam in regelmäßigen Abständen, in der Regel jährlich, eine Zielvereinbarung. Die Zielvereinbarung stellt sicher, dass grundsätzlich keine Detailsteuerung durch das Bundesministerium des Innern und für Heimat im Einzelfall erfolgt. Vorgaben durch das Bundesministerium des Innern und für Heimat sind im Einzelfall möglich und bei erheblicher Bedeutung, insbesondere bei politisch sensiblen Vorgaben und Abweichungen von der Zielvereinbarung, schriftlich zu begründen; BMI und BSI unterrichten den zuständigen Ausschuss über die Ausübung der Rechts- und Fachaufsicht, insbesondere zu Einzelweisungen von erheblicher Bedeutung und ihrer jeweiligen Begründung.

Zu § 2 Nummer 23

Die Neuformulierung vereinheitlicht und vereinfacht das Verfahren zur Bestimmung kritischer Komponenten und erleichtert damit die Anwendung der Regelung in der Praxis.

Zu § 5

Absatz 3 Satz 1 normiert die Pflicht des BSI, ihm bekannt gewordene Schwachstellen unverzüglich an den jeweiligen Verantwortlichen zu melden, sodass dieser auf die Behebung der Schwachstelle hinwirken kann. Über den Verweis auf § 3 Absatz 1 Satz 1 („Das Bundesamt fördert die Sicherheit in der Informationstechnik“) wird klargestellt, dass die Weitergabe ausschließlich der schnellstmöglichen Schließung der Schwachstelle dienen darf. Sofern im Einzelfall damit zu rechnen ist, dass die Information des Herstellers der Sicherheit in der Informationstechnik nicht dienlich wäre, kann das BSI daher stattdessen von den anderen Instrumenten des § 5 – etwa einer öffentlichen Warnung– Gebrauch machen.

Gemäß § 3 Absatz 1 Nummer 21 hat das Bundesamt die Aufgabe des Verbraucherschutzes und der Verbraucherinformation im Bereich der Sicherheit in der Informationstechnik. Durch die Ergänzungen in Absatz 3 Satz 2 Nummer 1 wird klargestellt, dass Dritte im Sinne dieser Regelung insbesondere auch die Verbraucher sind. Das Bundesamt soll insoweit 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, die es gemäß Absatz 2 Satz 1 entgegennimmt, auch nutzen, um die Verbraucher auf verständliche Weise zu infor-

mieren, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist. Dies kann beispielsweise durch die Einrichtung eines Informationsportals erfolgen, auf dem Verbraucherinnen und Verbraucher Details der von ihnen genutzten Hard- und Software eingeben können und daraufhin eine leicht verständliche Übersicht darüber erhalten, ob sie von Sicherheitslücken betroffen sind, ob diese ggf. mit anderen Sicherheitslücken kombinierbar sind und wie sie ihre Systeme durch Updates schützen können. Die konkrete Ausgestaltung obliegt dem Bundesamt und soll sich in den bereits bestehenden CVD-Prozess integrieren. Hierbei sind die Zuständigkeiten der ENISA gemäß Artikel 12 Absatz 2 der NIS2-Richtlinie zu berücksichtigen. Mit Absatz 3 Satz 2 Nr. 6 wird klargestellt, dass das Bundesamt den Betrieb der europäischen Schwachstellendatenbank durch die Bereitstellung entsprechender Informationen unterstützt. Die Übermittlung zur Veröffentlichung geschieht dabei in der Regel nachdem die Schwachstelle durch den Hersteller beseitigt wurde oder anderweitig bekannt geworden ist.

Absatz 7 schreibt die bisherige Verwaltungspraxis des Bundesamts, den Prozess der Schwachstellenmeldung in einer sogenannten „CVD-Policy“ öffentlich zu dokumentieren, gesetzlich fest.

Zu § 6 Absatz 1:

Die Änderung ist eine Folgeänderung zur Änderung in § 5 Absatz 3 Nummer 1 und 6. Die Regelung stellt klar, dass das Bundesamt bei der Erfüllung der Aufgabe nach § 3 Absatz 1 Nummer 21 auch Verbrauchern eine Teilnahme an dem Online-Portal ermöglichen kann.

Zu § 7 (Kontrolle der Kommunikationstechnik des Bundes, Betretensrechte)

Zu Absatz 1

Mit der Änderung in Absatz 1 wird klargestellt, dass sich die Kontrollbefugnis des Bundesamtes sich unter anderem auch auf die Durchführung von Penetrationstests erstreckt.

Zu Absatz 5

In Absatz 5 wird in Anlehnung an § 10 hier der einheitliche Begriff der „Anordnung“ statt der „Anweisung“ gewählt.

Zu Absatz 8

In Absatz 8 wird eine Korrektur in Anlehnung an den Wortlaut von Artikel 35 der NIS-2-Richtlinie vorgenommen.

Zu Absatz 9

Die Pflicht zur Unterrichtung des Haushaltsausschusses des Deutschen Bundestags über die Anwendung des § 7 wird an den Koordinator oder die Koordinatorin für Informationssicherheit in der Bundesverwaltung übertragen und in § 48 Absatz 6 geregelt.

Zu § 8 (Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes)

Zu Absatz 4 Satz 2 Nummer 1

Hier erfolgt die Korrektur eines redaktionellen Versehens.

Zu § 10

Die Ausweitung der Anordnungsbefugnis des Bundesamtes auf Sicherheitsvorfälle allgemein, statt der Begrenzung auf „gegenwärtige“ Sicherheitsvorfälle, entspricht der Formulierung des Artikels 32 Absatz 4 Buchstabe b NIS-2-Richtlinie.

Zu § 15

Zunehmende Vernetzung und Digitalisierung erhöhen die Angriffsfläche im Cyberraum und damit einhergehende Gefahren für die Bundesverwaltung erheblich. Die verschiedensten an das Internet angeschlossenen Geräte („Internet of Things“) können – gerade auch ohne Wissen der Verantwortlichen – zur Gefahr werden und für Angriffe gezielt eingesetzt werden, etwa zusammen mit weiteren Geräten als Botnetze. Das gilt insbesondere für Geräte, die nicht regelmäßig aktualisiert und an den Stand der Technik angepasst, aber weiterhin betrieben werden. Im Lichte der Gewährleistung der Sicherheit der Bundesverwaltung und vor dem Hintergrund der Zeitenwende im digitalen Raum wird der zur Umsetzung der NIS-2-Richtlinie vorgesehene § 15 erweitert. BSI wird es ermöglicht, Gefahren von der Bundesverwaltung effizienter abwehren zu können und die Ergebnisse der Abfragen nach Abs. 1 in abstrahierter Form im Lagebild zu berücksichtigen.

Zu § 28 (Besonders wichtige Einrichtungen und wichtige Einrichtungen)

In Absatz 2 Nummer 2 Buchstabe b erfolgt die Korrektur eines redaktionellen Versehens, da die Voraussetzungen nur alternativ vorliegen müssen. Denn für die hier genannten Einrichtungsarten sieht Artikel 2 Absatz 2 Buchstabe a Ziffer i der NIS-2-Richtlinie vor, dass die Size-Cap-Rule nicht gilt und damit sämtliche Unternehmensgrößen erfasst werden. Alle Einrichtungen bis zur Größe eines Kleinunternehmens sind jedoch als wichtige Einrichtungen zu kategorisieren und Kleinunternehmen sind solche, die weniger als 50 Mitarbeiter beschäftigen und einen Jahresumsatz oder eine Jahresbilanzsumme von jeweils 10 Mio. Euro oder weniger aufweisen, vgl. Artikel 3 Absatz 1 Buchstabe c, Absatz 2 der NIS-2-Richtlinie. In Absatz 4 werden digitale Energiedienste aufgenommen (s. Art. 17).

Zu § 29 (Einrichtungen der Bundesverwaltung)

Zu Absatz 1

Die Bezeichnung wird an die des § 2 BBankG angepasst.

Zu § 30 (Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen)

Zu Absatz 8 Satz 6

Da branchenspezifische Sicherheitsstandards von allen Unternehmen einer Branche genutzt werden können und die Erstellung im allgemeinen gesellschaftlichen Interesse liegt, wird auf die Erhebung von Gebühren oder Auslagen verzichtet, um keine entgegenstehenden Anreize zu schaffen. Damit verbunden ist eine Entlastung der betroffenen Wirtschaftsunternehmen. Für den Wegfall der Gebühren und Auslagen bedarf es angesichts § 1 BGebG einer gesetzlichen Regelung.

Zu Absatz 9 Satz 2

Die Änderung ist eine Folgeänderung zur Änderung in § 30 Absatz 8 Satz 6.

Zu § 31 (Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen)

Zu Absatz 2 Satz 1

Durch die Einfügung wird klargestellt, dass sich die Pflicht zum Einsatz von Systemen zur Angriffserkennung – wie bislang auch – auf die kritische Anlage beschränkt, und nicht auf die gesamte Einrichtung bezogen ist.

Zu § 33 (Registrierungspflicht)

Absatz 2 wird um die Verpflichtung der Betreiber kritischer Anlagen ergänzt, im Zuge der Registrierung auch Angaben zu den bei ihnen zum Einsatz kommenden Typen von kritischen Komponenten an das Bundesamt zu übermitteln. Dies dient als Ausgleich für den Wegfall der Anzeigepflicht nach dem bisherigen § 9b BSI-Gesetz (§ 41). Da die entsprechende Übermittlung dieser Informationen im Rahmen der nach § 33 ohnehin bestehenden Registrierungspflicht erfolgt, ist der zusätzliche Aufwand für die Betreiber kritischer Anlagen gering.

Um die beim Bundesamt vorliegenden Informationen über die bei den Betreibern kritischer Anlagen zum Einsatz kommenden Typen von kritischen Komponenten einerseits aktuell zu halten, andererseits aber auch den hierdurch entstehenden Mehraufwand möglichst gering zu halten, sieht Absatz 5 vor, dass Änderungen in diesem Bereich von den Betreibern einmal jährlich an das Bundesamt zu übermitteln sind.

Zu § 39 (Nachweispflichten für Betreiber kritischer Anlagen)

Zu Absatz 1 Satz 1

Diese Ergänzung dient der Klarstellung, dass die Nachweise von KRITIS-Betreibern – wie bislang auch – lediglich die kritischen Anlagen zu Gegenstand haben, und nicht die Gesamte Einrichtung.

Zu § 41 (Prüfung des Einsatzes von kritischen Komponenten)

Die Neuregelung beruht auf Erkenntnissen, die im Rahmen der Verwaltungspraxis mit Prüfungen nach dem bisherigen § 9b BSI-Gesetz gewonnen wurden.

Die bisherige Anzeigepflicht nach dem bisherigen § 9b Absatz 2 BSI-Gesetz entfällt ersatzlos. Damit entfällt auch die Regelung, wonach vor Ablauf einer Frist von zwei Monaten nach einer Anzeige der Einsatz der betreffenden kritischen Komponenten nicht gestattet war. Auch die bisher in § 9b Absatz 3 BSI-Gesetz vorgesehene Garantieerklärung des Herstellers über seine Vertrauenswürdigkeit gegenüber dem Betreiber entfällt ersatzlos. Dies bedeutet einerseits eine erhebliche Reduzierung der Aufwände für die betroffenen Betreiber kritischer Anlagen.

Andererseits kann das Bundesministerium des Innern und für Heimat künftig unabhängig von einer Anzeige durch Betreiber kritischer Anlagen prüfen, ob der Einsatz von kritischen Komponenten, also IKT-Produkten, die die Voraussetzungen von § 2 Nummer 23 in Verbindung mit § 56 Absatz 7 BSI-Gesetz erfüllen, die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt. Das Bundesministerium des Innern und für Heimat kann damit flexibel auf ihm vorliegende Erkenntnisse reagieren. Mit Blick auf die Frage, ob das Bundesministerium des Innern und für Heimat ein Prüfverfahren nach § 41 Absatz 1 einleitet, werden Hinweise und Vorschläge der in § 41 Absatz 1 aufgeführten Bundesministerien berücksichtigt.

Wie im bisherigen § 9b BSI-Gesetz ist die Prüfmöglichkeit auf kritische Komponenten, nunmehr im Sinne von § 2 Nummer 23 in Verbindung mit § 56 Absatz 7, beschränkt.

Gemäß § 41 Absatz 1 kann das Bundesministerium des Innern und für Heimat gegenüber dem Betreiber kritischer Anlagen den Einsatz von kritischen Komponenten eines Herstellers im Benehmen mit den für den jeweiligen Sektor genannten Ministerien sowie dem Aus-

wärtigen Amt untersagen oder Anordnungen erlassen, wenn der Einsatz die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt. Untersagung ist das Verbot des weiteren Einsatzes der betreffenden kritischen Komponente. Das Verbot kann auch so gestaltet werden, dass es erst nach Ablauf einer bestimmen Umsetzungsfrist gilt. Unter Anordnungen sind alle weiteren möglichen Maßnahmen zur Gewährleistung der öffentlichen Ordnung oder Sicherheit zu verstehen, z.B. kann eine Diversifizierung verschiedener Hersteller durch Vorgabe prozentualer Anteile vorgegeben werden, der Einsatz nur in bestimmten Bereichen zulässig bleiben oder ähnliches.

Absatz 2 erweitert die Untersagungs- und Anordnungsbefugnis des Bundesministeriums des Innern und für Heimat. Wurde gemäß Absatz 1 gegenüber dem Betreiber kritischer Anlagen eine Untersagung oder Anordnung ausgesprochen, kann das Bundesministerium des Innern und für Heimat gegenüber diesem Betreiber kritischer Anlagen auch den zukünftigen Einsatz weiterer kritischer Komponenten desselben Herstellers und desselben Komponententyps untersagen (Nr. 1) bzw. gegenüber allen Betreibern kritischer Anlagen den Einsatz derselben kritischen Komponente sowie von kritischen Komponenten desselben Komponententyps untersagen oder Anordnungen erlassen (Nr. 2). Auch bei Absatz 2 kann ein Verbot so gestaltet werden, dass es erst nach Ablauf einer bestimmen Umsetzungsfrist gilt.

Da von einer Entscheidung nach Absatz 2 Nr. 2 eine Vielzahl von Betreibern kritischer Anlagen betroffen sein kann, ist es praxisgerecht, dass die entsprechende Entscheidung als Allgemeinverfügung ergeht und im Bundesanzeiger bekannt gegeben werden kann.

Einige Aspekte, die im Rahmen der Prüfung einer voraussichtlichen Beeinträchtigung der öffentlichen Ordnung oder Sicherheit berücksichtigt werden können, werden in Absatz 4 konkretisiert und bieten den betroffenen Betreibern dadurch eine bessere Orientierung. Das ist für die Betreiber zum Beispiel im Rahmen von Vergabeentscheidungen von Bedeutung und erhöht auch allgemein die Rechts- und Planungssicherheit der Betreiber. Neben einer Kontrolle oder Zusammenarbeit i.S.v. Nr. 1 und einer Beteiligung an Aktivitäten nach Nr. 2 kann bei der Prüfung nach Nummer 3 insbesondere berücksichtigt werden, ob hinreichende Anhaltspunkte dafür bestehen, dass der Hersteller unmittelbar oder mittelbar an Aktivitäten beteiligt war oder ist, die geeignet waren oder sind, nachteilige Auswirkungen auf kritische Anlagen oder Betreiber kritischer Anlagen zu haben. Solche Aktivitäten können beispielsweise dann vorliegen, wenn der Hersteller Schwachstellen oder Manipulationen nicht unverzüglich, nachdem er davon Kenntnis erlangt hat, beseitigt und dem Betreiber der kritischen Anlage gemeldet hat oder Hersteller versucht hat, missbräuchlich auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der kritischen Anlage einzuwirken.

Der Begriff „insbesondere“ verdeutlicht, dass die in Absatz 4 genannten Aspekte nicht abschließend aufgeführt werden.

Entscheidungen des Bundesministeriums des Innern und für Heimat nach Absatz 1 und 2 erfolgen im Benehmen mit dem für den jeweiligen Sektor in Absatz 1 genannten Bundesministerium. Für Entscheidungen nach Absatz 2 gilt Absatz 1 insoweit entsprechend. Das Benehmen dient u.a. dazu, die Fachkompetenz und die Perspektive des betreffenden Bundesministeriums mit in das Verwaltungsverfahren und den Entscheidungsprozess einzubeziehen. Die Zusammenarbeit der Bundesministerien ist wegen der Tragweite möglicher Untersagungen und Anordnungen des Bundesministeriums des Innern und für Heimat besonders wichtig. Um eine mögliche Entscheidung im Benehmen mit den im Einzelfall betroffenen Ressorts zu unterstützen und vorzubereiten, ist ein fortlaufender und regelmäßiger Austausch geboten. Diese Zusammenarbeit kann insoweit z.B. im Rahmen eines fortlaufenden und regelmäßigen „interministeriellen Jour Fixes“ erfolgen.

Die Betreiber kritischer Anlagen sind gemäß Absatz 5 zur Mitwirkung bei der Ermittlung des Sachverhalts verpflichtet. Dafür sind dem Bundesministerium des Innern und für Heimat

alle für das Verfahren erheblichen Tatsachen vollständig und wahrheitsgemäß offenzulegen und die den Betreibern kritischer Anlagen bekannten Beweismittel anzugeben.

Der bisherige § 9b BSI-Gesetz sah keine Mitwirkungspflichten der Betreiber an den Verfahren vor. Dies hat zu Schwierigkeiten in der Prüfpraxis geführt, da es für die Prüfungen insbesondere auf solche Informationen ankommt, die in der Regel nur oder vor allem bei den Betreibern vorliegen. Absatz 5 sieht daher nunmehr eine umfangreiche Pflicht der Betreiber zur Übermittlung von Auskünften und Dokumenten vor. Die Zuwiderhandlung stellt eine Ordnungswidrigkeit dar, für die § 65 ein Bußgeld vorsieht.

Zu § 43 (Informationssicherheitsmanagement)

Mit Absatz 7 wird die Meldepflicht der Einrichtungen der Bundesverwaltung über Informationen nach § 4 Absatz 2 Nummer 1 und insbesondere von Schwachstellen an das Bundesamt, mit einer Geltung ab dem 01. Januar 2027, neu geregelt.

Zu § 48 (Amt des Koordinators für Informationssicherheit)

Die neue Vorschrift regelt die Einrichtung eines Koordinators oder einer Koordinatorin für Informationssicherheit in der Bundesverwaltung (Chief Information Security Officer des Bundes kurz „CISO Bund“) sowie ihrer oder seiner Stellvertreterin oder Stellvertreter.

Absatz 1 regelt die Wahrnehmung der Rolle des CISO Bund durch die Leitung des Bundesamtes sowie die erforderlichen Qualifikationen.

Absätze 2 und 3 dienen der Festlegung der Aufgaben und Durchsetzungsbefugnisse des CISO Bund. Die operativ unabhängige Wahrnehmung dieser Aufgaben und Befugnisse wird dadurch gewährleistet, dass kein Einvernehmen mit den beaufsichtigten Einrichtungen der Bundesverwaltung herzustellen und bedeutet auch, dass der CISO Bund bei der Wahrnehmung dieser Aufgaben keinen Weisungen unterliegt. Wie in § 1 geregelt führen das Bundesamt, und damit auch dessen Leitung in der Rolle des CISO Bund seine Aufgaben fachlich-unabhängig auf Grundlage wissenschaftlich-technischer Erkenntnisse durch.

Absatz 4 legt die Pflicht des CISO Bund zur Unterstützung der Ressorts unter Berücksichtigung eines angemessenen Verhältnisses zwischen dem Einsatz von Informationstechnik und Informationssicherheit fest. Die Unterstützung durch die Ressorts erfolgt in einem angemessenen Umfang, ohne die Aufgabenerfüllung nach § 43 bis 47 zu gefährden. Die Unterstützung der Ressorts bei der Umsetzung der Vorgaben besteht aus der Bereit-stellung von Hilfsmitteln, bewährten Methoden und Vorgehensweisen („Best Practice“) sowie Erfahrungsaustausch und -dokumentation zur Nachnutzung. Zudem ist die Einrichtung eines „Kompetenzzentrums operative Sicherheitsberatung des Bundes“ (KoSi Bund) geplant.

Absatz 5 sieht Beteiligungsrechte für den CISO Bund zur effektiven Wahrnehmung der Aufgaben vor.

Mit Absatz 6 wird die Pflicht zur Unterrichtung des Haushaltsausschusses des Deutschen Bundestags über die Anwendung des § 7 an den Koordinator oder die Koordinatorin für Informationssicherheit in der Bundesverwaltung übertragen.

Zu § 56 (Ermächtigung zum Erlass von Rechtsverordnungen)

Zu Absätzen

Mit der Änderung der Verordnungsermächtigung in den Absätzen § 56 wird Beteiligung relevanter zivilgesellschaftlicher Akteure gemäß dem bisherigen § 10 BSIG vorgesehen. Die darüber hinaus vorgesehene Anhörung von geeigneten Vertretern der Wissenschaft beim Erlass von Rechtsverordnungen nach Absatz 1 und Absatz 2 gewährleistet, dass auch deren Expertise in dem Verfahren berücksichtigt wird. Insbesondere bei Fragen, die über die Festlegung des jeweiligen

Verwaltungsverfahrens in den Rechtsverordnungen hinausgehen, kann diese Expertise von Bedeutung sein.

Zu Absatz 7

Mit Absatz 7 wird eine Ermächtigung zum Erlass von Rechtsverordnungen zur Bestimmung, welche kritischen Komponenten der Prüfung nach § 41 Absatz 1 unterfallen, durch das Bundesministerium des Innern und für Heimat eingeführt. Dabei ist das Einvernehmen mit dem für den jeweiligen Sektor in § 41 Absatz 1 genannten Bundesministerium herzustellen. Dadurch wird gewährleistet, dass die Expertise des für den Sektor zuständigen Bundesministeriums bei der Bestimmung von kritischen Komponenten angemessen berücksichtigt wird.

In Satz 2 werden die Voraussetzungen für den Erlass der Rechtsverordnung nach Absatz 7 konkretisiert. Ein IKT-Produkt kann danach als kritische Komponente im Sinne von § 2 Nummer 23 BSI-Gesetz bestimmt werden, wenn sie in kritischen Anlagen im Sinne von § 2 Nummer 22 BSI-Gesetz eingesetzt wird, sie eine kritische Funktion realisiert und eine Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit der Komponente zu einer Beeinträchtigung der Funktionsfähigkeit kritischer Anlagen oder zu anderen Beeinträchtigungen der öffentlichen Ordnung oder Sicherheit führen könnte. Satz 3 sieht ein Vorschlagsrecht der in § 41 Absatz 1 genannten Bundesministerien vor.

Zu § 58

Die bereits bestehende Berichtspflicht des Bundesministeriums des Innern und für Heimat an den zuständigen Ausschuss des Deutschen Bundestages wird erweitert. Es wird klargestellt, dass der Bericht insbesondere auch zur Ausübung der Fachaufsicht, zu Inhalt und Ausübung der Zielvereinbarung sowie zu Einzelweisungen von erheblicher Bedeutung und ihrer jeweiligen Begründung auszuführen hat. Gemeint sind dabei nicht erhebliche Weisungen, z.B. zur Übernahme oder Begleitung eines einzelnen Termins oder zur Beantwortung einzelner parlamentarischer Fragen oder Pressefragen, sondern Vorgänge von erheblicher Bedeutung, die einer politischen Weisung im Einzelfall bedürfen, oder Vorgängen, die von den Vorgaben der Zielvereinbarung abweichen.

Zu § 61 Absatz 11

In Absatz 11 wird eine Korrektur in Anlehnung an den Wortlaut von Artikel 35 der NIS-2-Richtlinie vorgenommen.

Zu § 65

Die Änderungen sind Folgeänderungen zu Anpassungen in § 41.

Zu Anlage 1 (Sektoren besonders wichtiger und wichtiger Einrichtungen)

Zu Nummer 5.2.1, Spalte D

Es wird nunmehr auf die Abwasserdefinition des allgemeineren, und dadurch für den Rechtsanwender in der Regel geläufigeren, Wasserhaushaltsgesetzes (WHG) verwiesen

und nicht mehr auf die des spezielleren Abwasserabgabengesetzes (AbwAG). Eine Änderung der von der Einrichtungsartendefinition umfassten Einrichtungen ist damit nicht verbunden.

Zu Anlage 2 (Sektoren wichtiger Einrichtungen)

Zu Nummer 3.1.1, Spalte D

Die hier vorgenommene Einschränkung erfolgt aufgrund einer Auslegung nach Sinn und Zweck sowie einer historischen Auslegung zum persönlichen Anwendungsbereich der NIS-2-Richtlinie. Aus den Materialien zum Rechtsetzungsverfahren wie der Folgenschätzung der Europäischen Kommission geht hervor, dass eine Beschränkung auf gefährliche Chemikalien beabsichtigt und eine Einbeziehung von Unternehmen, die chemische Elemente jeglicher Art herstellen oder vertreiben, wie Apotheken, Lebensmittelgeschäfte, etc., nicht beabsichtigt war. Damit wird eine präzisere Eingrenzung des Anwendungsbereichs erreicht und unnötige Belastungen der Wirtschaft vermieden.

Zu Artikel 3 (Änderung SÜFV), Artikel 5 (Änderung GleibWV), Artikel 7 (Änderung BSI-ZertV), Artikel 9 (Änderung BSI-ITSiKV), Artikel 12 (Änderung PassDEÜV), Artikel 13 (Änderung PauswV), Artikel 15 (Änderung KassenSichV), Artikel 22 (Änderung DiGAV), Artikel 27 (Änderung KHSFV) und Artikel 28 (Änderung AWV)

Betreffend dieser Änderungen von Rechtsverordnungen wird zur Begründung in Drucksache 20/13184 wie folgt ergänzt:

Die vorgesehenen Änderungen entsprechen den im Gemeinsamen Rundschreiben des Bundesministeriums des Innern und des Bundesministeriums der Justiz vom 21. März 2006 aus Anlass der Entscheidungen des Bundesverfassungsgerichts vom 13. und 27. September 2005 (2 BvF 2/03 und 2 BvL 11/02) zusammengefassten Voraussetzungen nach der Rechtsprechung des Bundesverfassungsgerichts für die Änderung von Rechtsverordnungen durch den Gesetzgeber. Insbesondere (i) erfolgt die Änderung der Rechtsverordnungen im Rahmen der Änderung eines Sachbereichs durch den Gesetzgeber, vorliegend die BSIG-Novelle nach Artikel 1 dieses Gesetzes, (ii) werden die grundgesetzlichen Regeln über die Gesetzgebung angewendet, eine Zustimmungspflicht liegt nicht vor und (iii) die Grenzen der jeweiligen gesetzlichen Ermächtigungsgrundlage werden eingehalten. Die Einhaltung der sich aus der vorgenannten Rechtsprechung des Bundesverfassungsgerichts ergebende Vorgabe, dass Änderungen von Rechtsverordnungen in Gesetz auf das Ausmaß zu beschränken sind, das unmittelbar durch die Änderungen im Gesetzesrecht veranlasst ist, wird durch die BSIG-Novelle nach Artikel 1 dieses Gesetzes bedingten Folgeänderungen eingehalten.

Zu Artikel 4 (BGebV BMI)

Die im Entwurf vorgesehenen Folgeänderungen entfallen, da die Rechtsverordnung gegenwärtig überarbeitet wird und die Folgeänderungen im Rahmen dieser Überarbeitung Berücksichtigung finden können.

Zu Artikel 8 (BSI-KritisV)

Um die unterbrechungsfreie Identifizierung von KRITIS-Betreibern zu gewährleisten, werden die sich aus der Novelle des BSI-Gesetzes (Artikel 1) ergebenden Folgeänderungen in der BSI-KritisV umgesetzt. Da aufgrund der bereits abgelaufenen Richtlinienumsetzungsfrist eine Übergangsphase zwischen Verkündung des Gesetzes und seinem Inkrafttreten nicht mehr vorgesehen werden kann, ist eine entsprechende Eilbedürftigkeit der Änderung der BSI-KritisV gegeben. Die ursprünglich geplante Neuverkündung der BSI-KritisV nach Inkrafttreten dieses Gesetzes ist damit für die unterbrechungsfreie Identifizierung von KRITIS-Betreibern nicht mehr erforderlich.

Auch die hier vorgesehenen Änderungen entsprechen den oben Zu Artikel 3 u.a. dargelegten Voraussetzungen der Rechtsprechung des Bundesverfassungsgerichts für die Änderung von Rechtsverordnungen durch den Gesetzgeber. Insbesondere (i) erfolgt die Änderung der BSI-KritisV im Rahmen der Änderung eines Sachbereichs durch den Gesetzgeber, vorliegend die BSIG-Novelle nach Artikel 1 dieses Gesetzes, (ii) werden die grundgesetzlichen Regeln über die Gesetzgebung angewendet, eine Zustimmungspflicht liegt weiterhin nicht vor und (iii) die Grenzen der gesetzlichen Ermächtigungsgrundlage (nunmehr § 54 Absatz 4 BSI-Gesetz in der Fassung von Artikel 1) werden eingehalten. Die Einhaltung der Vorgabe, dass Änderungen von Rechtsverordnungen in Gesetz auf das Ausmaß zu beschränken sind, das unmittelbar durch die Änderungen im Gesetzesrecht veranlasst ist, wird nachstehend im Einzelnen dargelegt.

Zu Nummer 1, 6, 10 und 11

Diese Folgeänderungen berücksichtigen die Ersetzung des bisherigen Begriffs „Kritische Infrastrukturen“ (§ 2 Absatz 10 BSI-Gesetz) durch den der „kritischen Anlage“ (§ 2 Nummer 24 BSIG-E).

Zu Nummer 2

Die Begriffsbestimmungen „Betreiber“ und „kritische Dienstleistung“ entfallen im Wege einer Folgeänderung, da diese nun in § 28 Absatz 7 BSIG-E und § 2 Nummer 24 BSIG-E enthalten sind.

Zu Nummer 3, 4, 5, 7, 8, 9

Diese Folgeänderungen berücksichtigen den Umstand, dass der bisherige Sektor „Finanz- und Versicherungswesen“ (§ 10 Absatz 1 BSI-Gesetz) in die Sektoren „Finanzwesen“ und „Sozialversicherungsträger sowie Grundsicherung für Arbeitssuchende“ aufgespalten wurde, wobei private Versicherungsdienstleistungen entfallen sind (§ 54 Absatz 4 in Verbindung mit § 2 Nummer 24 BSIG-E). Eine inhaltliche Änderung, mit Ausnahme der Folgeänderung Wegfall der privaten Versicherungsdienstleistungen, erfolgt nicht. Es handelt sich lediglich um eine Verschiebung des neu geschaffenen Sektors „Sozialversicherungsträger sowie Grundsicherung für Arbeitssuchende“ in einen eigenen Paragraphen sowie einen dazugehörigen Anhang.

Zu Nummer 6, 12

Diese Folgeänderungen berücksichtigen die neue Fundstelle der Verordnungsermächtigung (§ 54 Absatz 4 BSIG-E) sowie die Nennung der KRITIS-Sektoren (§ 2 Nummer 24 BSIG-E).

Zu Artikel 17 (EnWG)

Zu § 3 Nr. 1e und Nr.11a

Die Regelungen enthalten Begriffsbestimmungen für „Digitale Energiedienste“ und „Betreiber digitaler Energiedienste“.

Zu § 5c (ENWG n.F. aus aktuellem Entwurf NIS-2-Umsetzungsgesetz-IT-Sicherheit im Anlagen- und Netzbetrieb, Festlegungskompetenz)

Ziel der Neuregelung ist eine Konsolidierung der bisherigen Zuständigkeiten von BNetzA und BSI im Hinblick auf konventionelle und digitale Dienstleister im Sektor Energie.

Die Aufsicht über KRITIS-Betreiber im Sektor Strom hinsichtlich der Einhaltung von Cybersicherheitsmaßnahmen oblag bislang hauptsächlich der BNetzA. Ausgenommen waren lediglich „Anlagen oder Systeme zur Steuerung/Bündelung elektrischer Leistung“ (z.B. sog.

virtuelle Kraftwerke), für die die Aufsicht beim BSI lag. Die abstrakten Cybersicherheitsvorgaben des EnWG wurden dabei durch Sicherheitskataloge der BNetzA – im Benehmen mit dem BSI - konkretisiert.

Über die nunmehr vorgesehene Einvernehmensregelung bekommt das BSI größeren Einfluss auf die IT-Sicherheitsanforderungen im Sektor Energie. Das BSI wird dadurch in die Lage versetzt, ein einheitliches Sicherheitsniveau über alle KRITIS-Sektoren sicherzustellen und wird damit in seiner Rolle als zentrale Cybersicherheitsbehörde gestärkt.

Gleichzeitig bringt die Verlagerung der operativen Aufsicht, die im Wesentlichen der Sicherstellung der Einhaltung des IT-Sicherheitskatalogs dient, eine spürbare Entlastung des BSI.

Die weiteren Änderungen im EnWG sind Folgeänderungen aufgrund der veränderten Regelungssystematik im BSI-Gesetz.

Zu Artikel 26 (TKG)

Zu Nummer 3 bis 7

Hierbei handelt es sich um weitere Folgeänderung aufgrund der Änderung des Begriffs „Kritische Infrastruktur“ in § 2 Absatz 10 BSI-Gesetz zu „kritische Anlage“ in § 2 Nummer 22 BSIG-E.

Zu § § 165 Absatz 4 und § 167

Die Änderungen im TKG sind Folgeänderungen aufgrund der veränderten Regelungssystematik im BSI-Gesetz.

Zu Artikel 30 (Inkrafttreten, Außerkrafttreten)

In der Zusammenschau mit der Ermächtigung zum Erlass einer Rechtsverordnung nach § 5 Absatz 1 in Verbindung mit § 4 Absatz 3 des Dachgesetzes zur Stärkung der physischen Resilienz kritischer Anlagen (KRITIS-Dachgesetz) haben sich an der Gestaltung der Inkrafttretensregelung im bisherigen Artikel 33 Absatz 2 verfassungsrechtliche Zweifel ergeben, weshalb dieser zu streichen war. Die Änderungsbefehle der bisherigen Artikel 30 bis 32 sind daher entweder im KRITIS-DachG oder in einem separaten Änderungsgesetz, welches zeitgleich mit der vorgenannten Rechtsverordnung in Kraft tritt, zu berücksichtigen.