Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung

- Ein Cheatsheet aus der DORA-Werkstatt -

DISCLAIMER: Das Cheatsheet dient als Orientierungshilfe für einen ersten Überblick über die Inhalte und Anforderungen des deutschen Umsetzungsgesetzes zur europäischen NIS-2-Richtlinie. Das Cheatsheet ist nicht rechtsverbindlich und ersetzt keine juristische Prüfung.

LEGENDE:
- Farbige Abschnitte kennzeichnen übergeordnete Teile bzw. Kapitel des Umsetzungsgesetzes.
- Weiß hinterlegte Zeilen enthalten zusammengefasste, gesetzliche Anforderungen mit hoher Relevanz für Wirtschaftsunternehmen.
- Grau hinterlegte Zeilen enthalten gesetzliche Anforderungen, die sich vor allem an öffentliche Stellen und Behörden richten und für Wirtschaftsunternehmen nur nachrangige Bedeutung haben

#	Titel	Kurzbeschreibung
Art. 1	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz – BSIG)	
Teil 1	Allgemeine Vorschriften	
§ 1	*Bundesamt für Sicherheit in der Informationstechnik*	*§ 1 ordnet das Bundesamt für Sicherheit in der Informationstechnik (BSI) als Bundesbehörde ein*
§ 2	*Begriffsbestimmungen*	*§ 2 enthält zentrale Definitionen im Rahmen des Gesetzes*
Teil 2	Das Bundesamt	
Kap. 1	*Aufgaben und Befugnisse*	*§ 3 bis § 19 enthalten Anforderungen, Aufgaben und Befugnisse des Bundesamts für Sicherheit in der Informationstechnik (BSI)*
Kap. 2	*Datenverarbeitung*	*§ 20 – § 27 enthalten Regelung zur Verarbeitung von personenbezogenen Daten durch das BSI*
Teil 3	Sicherheit in der Informationstechnik von Einrichtungen	
Kap. 1	Anwendungsbereich	

§ 28	Besonders wichtige Einrichtungen und wichtige Einrichtungen	**§ 28 regelt, welche Organisationen als „besonders wichtige Einrichtungen“ und „wichtige Einrichtungen“ gelten**
		• Siehe nächste Seite
		• Unternehmen müssen sich selbst in die „richtige“ Einrichtungsart einordnen. Nebentätigkeiten können dabei unberücksichtigt bleiben, wenn sie für die Gesamttätigkeit unerheblich sind
		• Unternehmen verschiedener Sektoren und Branchen werden von der Verpflichtung zur Umsetzung ausgewählter Paragrafen ausgenommen
		• Keine Umsetzungsverpflichtung für die §§ 30, 31, 32, 35, 36, 38, 39, 61, 62 für
		  • Anbieter öffentlicher Telekommunikationsdienste
		  • Betreiber öffentlicher Telekommunikationsnetze
		  • Bestimmte Unternehmen aus dem Energiesektor
		• Keine Umsetzungsverpflichtung für die §§ 30, 31, 32, 35, 36, 38, 39 für
		  • Finanzunternehmen nach DORA
		  • die Gesellschaft für Telematik
		  • Betreiber von Diensten der Telematikinfrastruktur
		• Keine Umsetzungsverpflichtung für § 32 für
		  • Bestimmte Betreiber kritischer Anlagen im Finanzsektor (Abhängig von bestimmendem Einfluss/ tatsächlicher Sachherrschaft)

© Copyright 2026 | Dr. Marlen Hofmann| All rights reserved | Nutzung für interne, nicht-kommerzielle Zwecke gestattet.

	Sektor	Branchen und Organisationen	Keine NIS-2 Einrichtung	Wichtige Einrichtung	Besonders wichtige Einrichtung
	Betreiber kritischer Anlagen	Siehe „Verordnung zur Bestimmung kritischer Anlagen nach dem BSI-Gesetz“ (ehemals BSI-Kritisverordnung)	n/a	n/a	Sind immer besonders wichtige Einrichtung
	Staat	Diverse Einrichtungen der Bundesverwaltung	Diverse	n/a	Diverse
Anlage 1	**Digitale Infrastruktur**	• Qualifizierte Vertrauensdiensteanbieter • Top Level Domain Name Registries • DNS-Diensteanbieter	n/a	n/a	Sind immer besonders wichtige Einrichtung
		(nicht-qualifizierte) Vertrauensdiensteanbieter	n/a	Sind immer wichtige Einrichtung	n/a
		• Anbieter öffentlicher Telekommunikationsdienste • Betreiber öffentlicher Telekommunikationsnetze	n/a	< 50 Mitarbeiter **UND** Umsatz ≤ 10 Mio. € **ODER** Bilanzsumme ≤ 10 Mio. €	≥ 50 Mitarbeiter **ODER** Umsatz > 10 Mio. € **UND** Bilanzsumme > 10 Mio. €
		Bestimmte Unternehmen der digitalen Infrastruktur: • Betreiber von Internet Exchange Points • Anbieter von Cloud-Computing-Diensten • Anbieter von Rechenzentrumsdiensten • Betreiber von Content Delivery Networks • Managed Services Provider • Managed Security Services Provider	< 50 Mitarbeiter **ODER** Umsatz ≤ 10 Mio. € **ODER** Bilanzsumme ≤ 10 Mio. €	≥ 50 - 249 Mitarbeiter **ODER** Umsatz > 10 Mio. € **UND** Bilanzsumme > 10 Mio. €	≥ 250 Mitarbeiter **ODER** Umsatz > 50 Mio. € **UND** Bilanzsumme > 43 Mio. €
	Energie	Bestimmte Unternehmen in den Branchen: • Stromversorgung, • Fernwärme/ Fernkälte, • Kraftstoff und Heizöl, • Gasversorgung			
	Transport und Verkehr	Bestimmte Unternehmen in den Branchen: • Luftverkehr, • Schienenverkehr, • Schifffahrt • Straßenverkehr			
	Finanzwesen	Bestimmte Unternehmen in den Branchen: • Bankwesen • Finanzmarktinfrastrukturen			
	Gesundheit	Bestimmte Unternehmen aus dem Sektor Gesundheit			
	Wasser	Bestimmte Unternehmen in den Branchen • Trinkwasserversorgung • Abwasserbeseitigung			
	Weltraum	Betreiber von Bodeninfrastrukturen			
Anlage 2	**Chemie**	Ausgewählte Unternehmen aus Produktion, Herstellung und Handel mit chemischen Stoffen	< 50 Mitarbeiter **ODER** Umsatz ≤ 10 Mio. € **ODER** Bilanzsumme ≤ 10 Mio. €	≥ 50 Mitarbeiter **ODER** Umsatz > 10 Mio. € **UND** Bilanzsumme > 10 Mio. €	Gelten pauschal nicht als besonders wichtige Einrichtungen
	Transport und Verkehr	Post- & Kurierdienste			
	Abfall	Unternehmen der Abfallbewirtschaftung			
	Lebensmittel	Ausgewählte Unternehmen aus Produktion, Verarbeitung und Vertrieb von Lebensmitteln			
	Produktion	Unternehmen aus verarbeitendem Gewerbe/ Produktion: • Hersteller von Medizinprodukten und In-vitro-Diagnostika, • Hersteller von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen • Hersteller von elektrischen Ausrüstungen, • Maschinenbau • Hersteller von Kraftwagen und -teilen • Sonstiger Fahrzeugbau			
	Sektor Digitale Dienste	• Online-Marktplätze • Suchmaschinen • Soziale Netzwerke			
	Forschung	Forschungseinrichtungen			

© Copyright 2026 | Dr. Marlen Hofmann| All rights reserved | Nutzung für interne, nicht-kommerzielle Zwecke gestattet.

#	Titel	Kurzbeschreibung
§ 29	*Einrichtungen der Bundesverwaltung*	*§ 29 regelt die Behandlung von Einrichtungen der Bundesverwaltung*
Kap. 2	Risikomanagement, Melde-, Registrierungs-, Nachweis- und Unterrichtungspflichten	

§ 30	Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	**§ 30 enthält Vorgaben zu technischen und organisatorischen Sicherheitsmaßnahmen.**
		• Die Maßnahmen müssen dokumentiert sowie angemessen und proportional zu Größe der Einrichtung und Risikogehalt sein
		• Die Maßnahmen sollen sich am Stand der Technik und an EU-/ISO-Normen orientieren
		• Mindestens sind folgende Maßnahmen umzusetzen
		  • Etablierung von IKT-Risikoanalysen
		  • Umsetzung von IKT-Sicherheitsmaßnahmen in IKT-Systemen
		  • Management von IKT-bezogenen Vorfällen
		  • Management der IKT-Geschäftsfortführung inkl. IKT-Wiederanlauf und -Wiederherstellung
		  • Krisenmanagement, bei Bedarf inkl. gesicherten Notfallkommunikationssystemen
		  • IKT-Drittparteienrisikomanagement
		  • Etablierung von Richtlinien und Prozessen zur sicheren Beschaffung, Entwicklung und Wartung von IKT-Systemen
		  • Schwachstellenmanagement
		  • Schulung und Sensibilisierung von Mitarbeitenden
		  • Umsetzung und Management von kryptografischen Maßnahmen
		  • Management der Personalsicherheit,
		  • Berechtigungsmanagement
		  • IKT-Assetmanagement
		  • Multi-Faktor-Authentifizierung, Netzwerksicherheit/ sichere Kommunikation
		• Die verpflichtende Verwendung zertifizierter IKT-Produkte und -Dienste ist möglich
		• Es können branchenspezifische Sicherheitsstandards vorgeschlagen und anerkannt werden

§ 31	Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen	**§ 31 verschärft die Anforderungen aus § 30 speziell für Betreiber kritischer Anlagen.** • Bei Betreibern kritischer Anlagen können höhere Sicherheitsstandards erforderlich sein und als verhältnismäßig gelten • Betreiber kritischer Anlagen müssen Systeme zur Angriffserkennung (z. B. SIEM, IDS, IPS, Logserver, etc.) einsetzen • Der Stand der Technik ist zu berücksichtigen
§ 32	Meldepflichten	**§ 32 enthält Meldepflichten für bei erheblichen Sicherheitsvorfällen.** • Erstmeldung innerhalb von 24 Stunden nach Kenntniserlangung • Hauptmeldung innerhalb von 72 Stunden mit erster Bewertung und Auswirkungen • Abschlussmeldung innerhalb eines Monats (oder Fortschrittsmeldung, wenn Vorfall noch andauert) • auf Anforderung sind Zwischenmeldungen abzugeben
§ 33	Registrierungspflicht	§ **33 enthält Pflichten zur Registrierung bei der gemeinsamen Meldestelle** • Organisationen müssen sich spätestens 3 Monate nach Einstufung als wichtige/besonders wichtige Einrichtung registrieren • Es werden bestimmte registrierungsrelevante Informationen festgelegt. Änderungen daran müssen anlassbezogen und jährlich gemeldet werden • Das BSI kann Einrichtungen selbst registrieren, wenn diese ihrer Pflicht nicht nachkommen

© Copyright 2026 | Dr. Marlen Hofmann| All rights reserved | Nutzung für interne, nicht-kommerzielle Zwecke gestattet.

#	Titel	Kurzbeschreibung
§ 34	Besondere Registrierungspflicht für bestimmte Einrichtungsarten	**§ 34 regelt besondere Registrierungspflichen für die in § 60 genannten Einrichtungen** • DNS-Diensteanbieter, Top Level Domain Name Registries, Domain-Name-Registry-Dienstleister, • Anbieter von Cloud-Computing-Diensten und Anbieter von Rechenzentrumsdiensten, • Betreiber von Content Delivery Networks, • Managed Service Provider und Managed Security Service Provider • Anbieter von Online-Marktplätzen, Online-Suchmaschinen oder Plattformen für Dienste sozialer Netzwerke

§ 35	Unterrichtungspflichten	**§ 35 regelt, wann Unternehmen ihre Kunden bzw. Nutzer über Sicherheitsvorfälle oder Cyberbedrohungen informieren müssen.**
		• Das BSI kann anordnen, dass betroffene Kunden unverzüglich über erhebliche Sicherheitsvorfälle informiert werden
		• Unternehmen aus folgenden Sektoren müssen Kunden zusätzlich über Bedrohung und empfohlene Gegenmaßnahmen informieren
		  • Finanzwesen
		  • Leistungen der Sozialversicherung sowie Grundsicherung für Arbeitsuchende
		  • digitale Infrastruktur
		  • Verwaltung von IKT-Diensten
		  • Digitale Dienste
		  • Informationspflicht gilt nur, wenn die Interessen der Kunden überwiegen

§ 36	Rückmeldungen des Bundesamtes gegenüber meldenden Einrichtungen	**§ 36 regelt, wie das BSI auf Meldungen von Unternehmen nach § 32 reagiert.** • Bestätigung des Meldungseingangs möglichst innerhalb von 24 Stunden • Auf Wunsch erhalten Unternehmen Hinweise und operative Unterstützung zu Abhilfemaßnahmen • Bei Vorfall von öffentlichem Interesse ggf. Anordnung einer öffentlichen Information
§ 37	Ausnahmebescheid	**§ 37 ermöglicht Ausnahmen von NIS-2-Pflichten für bestimmte Einrichtungen in sicherheitsrelevanten Bereichen.**
§ 38	Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen	**§ 38 legt besondere Pflichten für die Geschäftsleitung fest.** • Geschäftsleitung ist verantwortlich für die Umsetzung und Überwachung der Maßnahmen nach § 30 • Pflichtverletzungen können zu Haftung gegenüber der eigenen Einrichtung führen • Geschäftsleitung muss an Schulungen zu IT-Sicherheitsrisiken und Risikomanagement teilnehmen
§ 39	Nachweispflichten für Betreiber kritischer Anlagen	**§ 39 regelt, wie Betreiber kritischer Anlagen die Umsetzung der Sicherheitsmaßnahmen aus § 30 belegen müssen.** • regelmäßiger Nachweis alle drei Jahre durch Audit, Prüfung oder Zertifizierung gegenüber dem BSI • BSI kann Mängelbeseitigungsplan und Nachweise der Umsetzung verlangen • Übergangsregeln für frühere KRITIS-Betreiber
§ 40	Nationale Verbindungsstelle sowie zentrale Melde- und Anlaufstelle für besonders wichtige und wichtige Einrichtungen	**§ 40 legt fest, dass das BSI die zentrale nationale Stelle für Meldungen und Koordination nach NIS-2 ist.**
§ 41	Untersagung des Einsatzes kritischer Komponenten	**§ 41 ermöglicht Behörden, den Betreibern von kritischen Anlagen den Einsatz von bestimmten Herstellern oder Komponenten zu verbieten.**
§ 42	*Auskunftsverlangen*	*§ 42 regelt die Verweigerung des allgemeinen Informationszugangs zu NIS-2-Aufsichtsunterlagen und -verfahren.*
Kap. 3	Informationssicherheit der Einrichtungen der Bundesverwaltung	
§ 43	*Informationssicherheitsmanagement*	*§ 43 verpflichtet Behörden zur Einführung eines Informationssicherheitsmanagements.*
§ 44	*Vorgaben des Bundesamtes*	*§ 44 legt Mindeststandards für Behörden fest (IT-Grundschutz, BSI-Standards).*

© Copyright 2026 | Dr. Marlen Hofmann| All rights reserved | Nutzung für interne, nicht-kommerzielle Zwecke gestattet.

#	Titel	Kurzbeschreibung
§ 45	*Informationssicherheitsbeauftragte der Einrichtungen der Bundesverwaltung*	*§ 45 verpflichtet jede Bundesbehörde zur Bestellung eines Informationssicherheitsbeauftragten.*
§ 46	*Informationssicherheitsbeauftragte der Ressorts*	*§ 46 regelt Informationssicherheitsbeauftragte auf Ministeriumsebene.*
§ 47	*Wesentliche Digitalisierungsvorhaben und Kommunikationsinfrastrukturen des Bundes*	*§ 47 betrifft große Digitalisierungsprojekte und Netzinfrastrukturen des Bundes.*
§ 48	*Amt des Koordinators für Informationssicherheit*	*§ 48 bestimmt die Leitung des BSI als Koordinator für Informationssicherheit der Bundesregierung.*
Teil 4	Datenbanken der Domain-Name-Registrierungsdaten	
§ 49	Pflicht zum Führen einer Domain-Registrierungsdatenbank	**§ 49 verpflichtet TLD-Registries und Registry-Dienstleister zum Führen einer korrekten Domain-Registrierungsdatenbank.**
§ 50	Verpflichtung zur Zugangsgewährung	**§ 50 regelt den Zugang zu Domain-Registrierungsdaten für berechtigte Anfragende.** • Zugang ist bei berechtigtem Interesse unverzüglich, spätestens innerhalb von 72 Stunden zu gewähren • Offenlegungsprozesse müssen bis 06.03.2026 veröffentlicht werden
§ 51	Kooperationspflicht	**§ 51 verpflichtet TLD-Registries und Registry-Dienstleister zur Zusammenarbeit.**
Teil 5	Zertifizierung, Konformitätserklärung und Kennzeichen	
§ 52	Zertifizierung	**§ 52 regelt die Zertifizierung von IT-Produkten, Dienstleistungen, Personen und IT-Sicherheitsdienstleistern durch das BSI.** • BSI ist nationale Zertifizierungsstelle für IT-Sicherheit • Zertifikate können für Produkte, Leistungen, Personen und IT-Sicherheitsdienstleister beantragt werden • Prüfung kann durch anerkannte sachverständige Stellen erfolgen • Zertifikat wird nur erteilt, wenn Sicherheitskriterien erfüllt sind und keine sicherheitspolitischen Einwände bestehen • EU-Zertifikate anderer Stellen können anerkannt werden, wenn gleichwertiges Sicherheitsniveau besteht
§ 53	Konformitätsbewertung und Konformitätserklärung	**§ 53 ermöglicht Selbstbewertung und Konformitätserklärungen auf Basis technischer Richtlinien** • Für bestimmte IKT-Produkte, IKT-Dienste und IKT-Prozesse kann das BSI eine Selbstbewertung durch Hersteller, Anbieter, Personen oder IT-Sicherheitsdienstleister zulassen • Der Aussteller der Konformitätserklärung übernimmt Verantwortung, dass die Anforderungen erfüllt sind
§ 54	Nationale Behörde für Cybersicherheitszertifizierung	**§ 54 regelt die Rolle des BSI im europäischen Cybersicherheitszertifizierungssystem** • Das BSI ist die nationale Zertifizierungsbehörde nach EU-Cybersecurity Act und erhält die damit verbundenen Aufgaben, Kompetenzen und Verantwortungen
§ 55	Freiwilliges IT-Sicherheitskennzeichen	**§ 55 führt ein freiwilliges IT-Sicherheitskennzeichen für Verbraucherprodukte ein. Es informiert über IT-Sicherheitsmerkmale, nicht über Datenschutz.** • Das freiwillige Kennzeichen basiert auf Herstellererklärung zur Einhaltung festgelegter IT-Sicherheitsanforderungen • Die Verwendung darf erst nach Antrag und Plausibilitätsprüfung durch das BSI erfolgen • Das Kennzeichen wird am Produkt oder elektronisch bereitgestellt und verweist auf BSI-Informationsseite
Teil 6	Verordnungsermächtigungen, Grundrechtseinschränkungen und Berichtspflichten	
§ 56	*Ermächtigung zum Erlass von Rechtsverordnungen*	*§ 56 legt fest, wie und durch wen weitere Regelungen zu NIS 2 erlassen werden können*
§ 57	*Einschränkung von Grundrechten*	*§ 57 stellt klar, dass bestimmte Vorschriften des Gesetzes in das Fernmeldegeheimnis eingreifen können.*

© Copyright 2026 | Dr. Marlen Hofmann| All rights reserved | Nutzung für interne, nicht-kommerzielle Zwecke gestattet.

#	Titel	Kurzbeschreibung
§ 58	*Berichtspflichten des Bundesamtes*	*§ 58 regelt die Berichts- und Informationspflichten des BSI gegenüber Ministerien, Bundestag und EU*
Teil 7	Aufsicht	
§ 59	Zuständigkeit des Bundesamtes	**§ 59 legt fest, dass das BSI Aufsichtsbehörde für wichtige und besonders wichtige Einrichtungen sowie Betreiber kritischer Anlagen in Deutschland ist.**
§ 60	*Zentrale Zuständigkeit in der Europäischen Union für bestimmte Einrichtungsarten*	*§ 60 regelt, wann das BSI in der EU „Lead Authority" ist.*
§ 61	Aufsichts- und Durchsetzungsmaßnahmen für besonders wichtige Einrichtungen	**§ 61 enthält die Befugnisse des BSI gegenüber besonders wichtigen Einrichtungen.** • kann Audits/Prüfungen/Zertifizierungen anordnen und regelmäßige Nachweise und Mängelbeseitigungspläne verlangen • kann Räume betreten, Unterlagen verlangen und Überprüfungen durchführen • kann bei Verstößen weitreichende Maßnahmen treffen bis hin zur Aussetzung von Genehmigungen und Untersagung der Tätigkeit von Geschäftsleitungen
§ 62	Aufsichts- und Durchsetzungsmaßnahmen für wichtige Einrichtungen	**§ 62 regelt die Durchsetzung der Vorgaben gegenüber wichtigen Einrichtungen.** • bei Verdacht auf Verstöße kann BSI die Umsetzung der Pflichten überprüfen • BSI kann Maßnahmen nach § 61 anwenden (abgestuft gegenüber besonders wichtigen Einrichtungen)
§ 63	Verwaltungszwang	**§ 63 Regelt die Höhe von Zwangsgeldern, die durch das BSI verhängt werden können: bis 100.000 €**
§ 64	*Zuwiderhandlungen durch Institutionen der sozialen Sicherung*	*§ 64 enthält besondere Regeln für Träger der sozialen Sicherung.*
Teil 8	Bußgeldvorschriften	

§ 65	Bußgeldvorschriften	**§ 65 regelt, welche Verstöße sanktioniert werden und in welcher Höhe.**
		• Geahndet werden können unter anderem
		  • fehlende oder verspätete Umsetzung von Risikomanagementmaßnahmen
		  • Verstöße gegen Meldepflichten bei Sicherheitsvorfällen
		  • fehlende oder verspätete Registrierung/Änderungsmitteilungen
		  • Nichtbefolgung von Anordnungen des BSI
		• Bußgeldrahmen
		  • besonders wichtige Einrichtungen: bis 10 Mio. €
		  • wichtige Einrichtungen: bis 7 Mio. €
		  • besondere Tatbestände auch mit anderen Beträgen
		  • besonders wichtige Einrichtungen > 500 Mio. € Umsatz: bis 2 % des weltweiten Jahresumsatzes
		  • wichtige Einrichtungen > 500 Mio. € Umsatz: bis 1,4 % des weltweiten Jahresumsatzes

Anlage 1 Sektoren besonders wichtiger und wichtiger Einrichtungen		
Anlage 2 Sektoren wichtiger Einrichtungen		
Art. 2 – Art. 7	*Änderung diverser Gesetze*	*Die Art. 2 – 7 enthalten kleinere formale Änderungen an weiteren Gesetzen und zur Aufnahme von Verweisen auf das BSI-Gesetz gemäß Art. 1* • *Änderung des BND-Gesetzes* • *Änderung der Sicherheitsüberprüfungsfeststellungsverordnung* • *Änderung des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes* • *Änderung der Gleichstellungsbeauftragtenwahlverordnung* • *Änderung des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme* • *Änderung der BSI-Zertifizierungs- und -Anerkennungsverordnung*

© Copyright 2026 | Dr. Marlen Hofmann| All rights reserved | Nutzung für interne, nicht-kommerzielle Zwecke gestattet.

#	Titel	Kurzbeschreibung
Art. 8	Änderung der BSI-Kritisverordnung	**Art. 8 enthält Änderungen an der BSI-Kritisverordnung** • Umbenennung der BSI-Kritisverordnung in „Verordnung zur Bestimmung kritischer Anlagen nach dem BSI-Gesetz“ • Umbenennung von „Betreiber Kritischer Infrastrukturen“ in „Betreiber Kritischer Anlagen • Weitere kleinere inhaltliche sowie formale Anpassungen
Art. 9 – Art. 16	*Änderung diverser Gesetze*	*Die Art. 9 – 16 enthalten kleinere formale Änderungen an weiteren Gesetzen und zur Aufnahme von Verweisen auf das BSI-Gesetz gemäß Art. 1* • *Änderung der BSI-IT-Sicherheitskennzeichenverordnung* • *Änderung des De-Mail-Gesetzes* • *Änderung des E-Government-Gesetzes* • *Änderung der Passdatenerfassungs- und Übermittlungsverordnung* • *Änderung der Personalausweisverordnung* • *Änderung des Hinweisgeberschutzgesetzes* • *Änderung der Kassensicherungsverordnung* • *Änderung des Atomgesetzes*
Art. 17	Änderung des Energiewirtschaftsgesetzes	**Art. 17 enthält Änderungen am EnwG** • Neuaufnahme eines Paragraphs zu “IT-Sicherheit im Anlagen- und Netzbetrieb, Festlegungskompetenz” • Anforderungen an den Risikomanagementrahmen von Betreibern von Energieversorgungsnetzen, Energieanlagen, digitalin Energiediensten • Anpassungen am IT-Sicherheitskatalog • Zuständigkeiten für das Meldewesen von Sicherheitsvorfällen • Anforderungen und Pflichten der Geschäftsleitung
Art. 18 – Art. 24	*Änderung diverser Gesetze*	*Die Art. 18 – 24 enthalten kleinere formale Änderungen an weiteren Gesetzen und zur Aufnahme von Verweisen auf das BSI-Gesetz gemäß Art. 1* • *Änderung des Messstellenbetriebsgesetzes* • *Änderung des Energiesicherungsgesetzes* • *Änderung des Wärmeplanungsgesetzes* • *Änderung des Fünften Buches Sozialgesetzbuch* • *Änderung der Digitale Gesundheitsanwendungen-Verordnung* • *Änderung der Verordnung zum Barrierefreiheitsstärkungsgesetz* • *Änderung des Elften Buches Sozialgesetzbuch*
Art. 25	Änderung des Telekommunikationsgesetzes	**Art. 25 enthält Änderungen am TKG** • Einführung neuer Definition zu Sicherheitsvorfällen sowie Netz- und Informationssystemen im Telekommunikationssektor • Umbenennung von „Betreiber Kritischer Infrastrukturen“ in „Betreiber Kritischer Anlagen • Umbenennung von „Kritischen Infrastruktur“ in „Kritische Anlage“ • Ergänzungen zum Thema „Stand der Technik“ • Anforderungen an den Risikomanagementrahmen von Betreibern öffentlicher Telekommunikationsnetze und -dienste • Zuständigkeiten für das Meldewesen von Sicherheitsvorfällen • Anforderungen und Pflichten der Geschäftsleitung
Art. 26 – Art. 28	*Änderung diverser Gesetze*	*Die Art. 26 – 28 enthalten kleinere formale Änderungen an weiteren Gesetzen und zur Aufnahme von Verweisen auf das BSI-Gesetz gemäß Art. 1* • *Änderung der Krankenhausstrukturfonds-Verordnung* • *Änderung der Außenwirtschaftsverordnung* • *Änderung des Vertrauensdienstegesetzes*
Art. 29	Außerkrafttreten	**Art. 29 besagt, dass das bisherige BSI-Gesetz von 2009 vollständig aufgehoben wird.**
Art. 30	Inkrafttreten	**Art. 30 regelt, dass das neue BSI-Gesetz ab dem Tag nach Verkündung gilt und keine Übergangsfristen vorgesehen sind.**

© Copyright 2026 | Dr. Marlen Hofmann| All rights reserved | Nutzung für interne, nicht-kommerzielle Zwecke gestattet.