Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz - BSIG)

BSIG

Ausfertigungsdatum: 02.12.2025

Vollzitat:

"BSI-Gesetz vom 2. Dezember 2025 (BGBl. 2025 I Nr. 301, S. 2)"

Ersetzt G 206-2 v. 14.8.2009 I 2821 (BSIG 2009)

Fußnote

(+++ Nachgewiesener Text noch nicht dokumentarisch bearbeitet +++)
(+++ EU-Vollzitate: vgl. Liste EU-Rechtsakte G v. 2.12.2025 I Nr. 301 +++)

Das G wurde als Artikel 1 des G v. 2.12.2025 I Nr. 301 vom Bundestag beschlossen. Es tritt gem. Art. 30 dieses G am 6.12.2025 in Kraft.

Inhaltsübersicht

Teil 1
Allgemeine Vorschriften

§ 1 Bundesamt für Sicherheit in der Informationstechnik

Das Bundesamt für Sicherheit in der Informationstechnik (Bundesamt) ist eine Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern. Es ist die zentrale Stelle für Informationssicherheit auf nationaler Ebene. Seine Aufgaben führt das Bundesamt auf Grundlage wissenschaftlich-technischer Erkenntnisse durch.

§ 2 Begriffsbestimmungen

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;
2. „berechtigte Zugangsnachfrager“

a) das Bundesamt,

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 Ziffer ii der NIS-2-Richtlinie bestimmt haben,

c) Strafverfolgungsbehörden,

d) die Polizeien des Bundes und der Länder und

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;

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;

6. „Cyberbedrohung“ eine Cyberbedrohung nach Artikel 2 Nummer 8 der Verordnung (EU) 2019/881;

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

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;

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 aufgrund der besonderen technischen Merkmale der Cyberbedrohung erheblich zu beeinträchtigen; eine Beeinträchtigung ist erheblich, wenn sie erheblichen materiellen oder immateriellen Schaden verursachen kann;

11. „erheblicher Sicherheitsvorfall“ ein Sicherheitsvorfall, der

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,

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;

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;

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;

17. „Informationssicherheit“ der angemessene Schutz der Vertraulichkeit, Integrität und Verfügbarkeit 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;
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,
    b) nur der Zusammenschaltung autonomer Systeme dient und
    c) nicht voraussetzt, dass
        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;
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;
23. „kritische Komponenten“ IKT-Produkte, die in einer Rechtsverordnung aufgrund von § 56 Absatz 7 und 8 als kritische Komponenten bestimmt werden.
24. „kritische Dienstleistung“ eine Dienstleistung zur Versorgung der Allgemeinheit in den Sektoren Energie, Transport und Verkehr, Finanzwesen, Leistungen der Sozialversicherung sowie der Grundsicherung für Arbeitsuchende, 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 Managed Service Provider, 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;
27. „NIS-2-Richtlinie“ die Richtlinie (EU) 2022/2555 in der jeweils geltenden Fassung;
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;
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
    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;

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;
33. „qualifizierter Vertrauensdienst“ ein qualifizierter Vertrauensdienst nach Artikel 3 Nummer 17 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;
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;
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;
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
    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;
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;
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;
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 langanhaltende negative Auswirkungen auf die Erbringung von Diensten im gesamten Binnenmarkt haben können, führen kann;
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.

Fußnote

(+++ EU-Vollzitate: vgl. Liste EU-Rechtsakte G v. 2.12.2025 I Nr. 301 +++)

Teil 2
Das Bundesamt

Kapitel 1
Aufgaben und Befugnisse

§ 3 Aufgaben des Bundesamtes

(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;
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 den Artikeln 14 und 15 der NIS-2-Richtlinie wahrnehmen;
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;
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 die Einhaltung dieser Sicherheitsanforderungen überprüfen;
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;
10. Konformität im Bereich der IT-Sicherheit von informationstechnischen Systemen und Komponenten mit technischen Richtlinien des Bundesamtes prüfen und bestätigen;
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;
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;
15. IT-Sicherheitsprodukte und IT-Sicherheitsdienstleistungen für Einrichtungen der Bundesverwaltung bereitstellen;
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 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 den §§ 30 und 44, bereitstellen;
18. Unterstützung
    a) der Polizeien und Strafverfolgungsbehörden des Bundes und der Länder bei der Wahrnehmung ihrer gesetzlichen Aufgaben,
    b) der Verfassungsschutzbehörden des Bundes und der Länder 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 den Verfassungsschutzgesetzen des Bundes und der Länder beziehungsweise dem MAD-Gesetz anfallen,
    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;
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, die Länder 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;
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;
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;
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;

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;
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 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.

(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.

Fußnote

(+++ EU-Vollzitate: vgl. Liste EU-Rechtsakte G v. 2.12.2025 I Nr. 301 +++)

§ 4 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.

(2) Das Bundesamt hat zur Wahrnehmung dieser Aufgabe

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,
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.

§ 5 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.

(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) 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 ist. 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,
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,
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.

(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
2. aufgrund von Vereinbarungen des Bundesamtes mit Dritten nicht übermittelt werden dürfen.

(5) Sonstige gesetzliche Meldepflichten, Regelungen zum Geheimschutz, gesetzliche Übermittlungshindernisse und Übermittlungsregelungen bleiben unberührt.

(6) Das Bundesamt veröffentlicht am 6. Dezember 2026 eine Verfahrensbeschreibung zur Durchführung der Absätze 1 bis 3.

§ 6 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.

(2) Das Bundesamt gibt Teilnahmebedingungen für den Informationsaustausch und die Plattformnutzung zwischen den Teilnehmenden vor.

§ 7 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. 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
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) 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.

(4) Das Bundesamt informiert über das Ergebnis seiner Kontrolle nach den Absätzen 1 bis 3

1. den jeweiligen überprüften Betreiber,
2. die oder den Informationssicherheitsbeauftragten des Ressorts und
3. die zuständige Rechts- und Fachaufsicht.

(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.

(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 für Digitales und Staatsmodernisierung 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 für Digitales und Staatsmodernisierung und dem Bundesministerium der Verteidigung.

(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.

Fußnote

(+++ EU-Vollzitate: vgl. Liste EU-Rechtsakte G v. 2.12.2025 I Nr. 301 +++)

§ 8 Abwehr von Schadprogrammen und 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,
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.

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.

(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.

(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,
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
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

1. zur Abwehr des Schadprogramms der sonstigen erheblichen Gefahren für die Kommunikationstechnik des Bundes,
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.

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.

(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

1. an die Polizeien des Bundes und der Länder zur Abwehr einer Gefahr für die öffentliche Sicherheit, die unmittelbar von einem Schadprogramm ausgeht,
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.

(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,
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,
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 2 Nummer 1 und 2 bedarf der vorherigen gerichtlichen Zustimmung. Für das Verfahren nach Satz 2 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 2 Nummer 3 und 4 erfolgt nach Anordnung des Bundesministeriums des Innern. Die §§ 9 bis 16 des Artikel 10-Gesetzes gelten entsprechend.

(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 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.

(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, 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,
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 Innenausschuss des Deutschen Bundestages über die Anwendung dieser Vorschrift.

Fußnote

(+++ EU-Vollzitate: vgl. Liste EU-Rechtsakte G v. 2.12.2025 I Nr. 301 +++)

§ 9 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.

(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.

§ 10 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 Satz 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.

§ 11 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.

(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.

(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. Zugang zu den in Verfahren nach Absatz 1 geführten Akten wird Dritten nicht gewährt.

(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.

(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.

(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 Paragraphen die Vorgaben aufgrund des Atomgesetzes Vorrang.

§ 12 Bestandsdatenauskunft

(1) Das Bundesamt darf zur Erfüllung seiner gesetzlichen Aufgabe nach § 3 Absatz 1 Satz 1 Nummer 1, 2, 20, 24 oder 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.

(3) Der aufgrund eines Auskunftsverlangens Verpflichtete hat die zur Auskunftserteilung erforderlichen Daten unverzüglich und vollständig zu übermitteln.

(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.

(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

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.

(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.

§ 13 Warnungen

(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:

a) Warnungen vor Schwachstellen und anderen Sicherheitsrisiken in informationstechnischen Produkten und Diensten,

b) Warnungen vor Schadprogrammen,

c) Warnungen bei einem Verlust oder einem unerlaubten Zugriff auf Daten,

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

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.

(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
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.

(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
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.

§ 14 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.

(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.

(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.

§ 15 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 zur Detektion von bekannten Schwachstellen und anderen Sicherheitsrisiken Abfragen an den Schnittstellen öffentlich erreichbarer informationstechnischer Systeme zu öffentlichen Telekommunikationsnetzen durchführen,

1. um festzustellen, ob diese Schnittstellen unzureichend geschützt und dadurch in ihrer Sicherheit oder Funktionsfähigkeit gefährdet sein können, oder
2. wenn die Einrichtungen der Bundesverwaltung, der besonders wichtigen oder der wichtigen Einrichtungen die entsprechenden Einrichtungen darum ersuchen.

Erlangt das Bundesamt dabei Informationen, die durch Artikel 10 des Grundgesetzes geschützt sind, darf es diese nur zum Zwecke der Übermittlung nach § 8 Absatz 6 und 7 verarbeiten. Sofern die Voraussetzungen des § 8 Absatz 6 und 7 nicht vorliegen, sind Informationen, die durch Artikel 10 des Grundgesetzes geschützt sind, unverzüglich zu löschen.

(2) Wird durch Abfragen gemäß Absatz 1 Satz 1 eine bekannte Schwachstelle oder ein anderes Sicherheitsrisiko eines informationstechnischen Systems erkannt, informiert das Bundesamt als allgemeine Meldestelle für die Sicherheit in der Informationstechnik nach § 5 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.

(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.

(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.

§ 16 Anordnungen von Maßnahmen des Bundesamtes gegenüber Anbietern von Telekommunikationsdiensten

(1) Zur Abwehr erheblicher Gefahren für die in Absatz 3 genannten Schutzgüter kann das Bundesamt anordnen, dass ein Anbieter von öffentlich zugänglichen Telekommunikationsdiensten im Sinne des Telekommunikationsgesetzes

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,

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 die Bundesnetzagentur ins Benehmen zu setzen. 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) Zur Abwehr erheblicher Gefahren für die in Absatz 3 genannten Schutzgüter kann das Bundesamt technische Befehle zur Bereinigung von einem konkret benannten Schadprogramm an betroffene informationstechnische Systeme verteilen. Absatz 1 Satz 2 und 3 gilt entsprechend. Der betroffene Diensteanbieter ist verpflichtet, das Bundesamt bei der Umsetzung nach Satz 1 zu unterstützen und insbesondere alle notwendigen Auskünfte zu erteilen, die zur Erstellung und Verteilung des Befehls notwendig sind.

(3) 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,
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.

(4) 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.

(5) Das Bundesamt darf Daten, die von einem Anbieter von öffentlich zugänglichen Telekommunikationsdiensten nach Absatz 1 Satz 1 Nummer 1 und Absatz 4 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 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

1. unerlaubten Zugriffen auf die für diese digitalen Dienste genutzten technischen Einrichtungen oder
2. Störungen, auch soweit sie durch äußere Angriffe bedingt sind,

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 Anordnungen von Maßnahmen des Bundesamtes gegenüber Herstellern von IKT-Produkten

Soweit erforderlich, kann das Bundesamt von einem Hersteller, dessen 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 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.

Kapitel 2
Datenverarbeitung

§ 20 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.

(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
   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
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

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
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.

Fußnote

(+++ EU-Vollzitate: vgl. Liste EU-Rechtsakte G v. 2.12.2025 I Nr. 301 +++)

§ 21 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.

Fußnote

(+++ EU-Vollzitate: vgl. Liste EU-Rechtsakte G v. 2.12.2025 I Nr. 301 +++)

§ 22 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 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

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.

Fußnote

(+++ EU-Vollzitate: vgl. Liste EU-Rechtsakte G v. 2.12.2025 I Nr. 301 +++)

§ 23 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. die Auskunftserteilung die ordnungsgemäße Erfüllung der Aufgaben gefährden würde, die in der Zuständigkeit des Bundesamtes liegen,
2. die Auskunftserteilung
   a) die öffentliche Sicherheit oder die Gewährleistung der Netz- und Informationssicherheit gefährden 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

und deswegen das Interesse der betroffenen Person an der Auskunftserteilung zurücktreten muss.

(2) § 34 Absatz 2 bis 4 des Bundesdatenschutzgesetzes gilt entsprechend.

Fußnote

(+++ EU-Vollzitate: vgl. Liste EU-Rechtsakte G v. 2.12.2025 I Nr. 301 +++)

§ 24 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.

(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.

Fußnote

(+++ EU-Vollzitate: vgl. Liste EU-Rechtsakte G v. 2.12.2025 I Nr. 301 +++)

§ 25 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 ergänzend zu den in Absatz 3 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht, wenn

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.

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.

Fußnote

(+++ EU-Vollzitate: vgl. Liste EU-Rechtsakte G v. 2.12.2025 I Nr. 301 +++)

§ 26 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

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.

Fußnote

(+++ EU-Vollzitate: vgl. Liste EU-Rechtsakte G v. 2.12.2025 I Nr. 301 +++)

§ 27 Widerspruchsrecht

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
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.

Fußnote

(+++ EU-Vollzitate: vgl. Liste EU-Rechtsakte G v. 2.12.2025 I Nr. 301 +++)

Teil 3
Sicherheit in der Informationstechnik von Einrichtungen

Kapitel 1
Anwendungsbereich

§ 28 Besonders wichtige Einrichtungen und wichtige Einrichtungen

(1) Als besonders wichtige Einrichtung gelten

1. Betreiber kritischer Anlagen,
2. qualifizierte Vertrauensdiensteanbieter, Top Level Domain Name Registries oder DNS-Diensteanbieter,
3. Anbieter öffentlich zugänglicher Telekommunikationsdienste oder Betreiber öffentlicher Telekommunikationsnetze, die
   a) mindestens 50 Mitarbeiter beschäftigen oder
   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 und die einer der in Anlage 1 bestimmten Einrichtungsarten zuzuordnen sind, und
   a) mindestens 250 Mitarbeiter beschäftigen oder
   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.

(2) Als wichtige Einrichtungen gelten

1. Vertrauensdiensteanbieter,
2. Anbieter öffentlich zugänglicher Telekommunikationsdienste oder Betreiber öffentlicher Telekommunikationsnetze, die
   a) weniger als 50 Mitarbeiter beschäftigen und
   b) einen Jahresumsatz oder eine Jahresbilanzsumme von jeweils 10 Millionen Euro oder weniger aufweisen,
3. sonstige natürliche oder juristische Personen oder rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft, die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbieten und die einer der in den Anlagen 1 und 2 bestimmten Einrichtungsarten zuzuordnen sind und
   a) mindestens 50 Mitarbeiter beschäftigen oder
   b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen.

Davon ausgenommen sind besonders wichtige Einrichtungen und Einrichtungen der Bundesverwaltung.

(3) Bei der Zuordnung zu einer der Einrichtungsarten nach den Anlagen 1 und 2 können solche Geschäftstätigkeiten unberücksichtigt bleiben, die im Hinblick auf die gesamte Geschäftstätigkeit der Einrichtung vernachlässigbar sind.

(4) Bei der Bestimmung von Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme nach den Absätzen 1 und 2 ist außer für rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft die Empfehlung der Kommission (2003/361/EG) mit Ausnahme von Artikel 3 Absatz 4 des Anhangs anzuwenden. 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.

(5) Die §§ 30, 31, 32, 35, 36, 38, 39, 61 und 62 gelten nicht für besonders wichtige Einrichtungen und wichtige Einrichtungen, die

1. ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen oder
2. Energieversorgungsnetze, Energieanlagen oder digitale Energiedienste nach dem Energiewirtschaftsgesetz betreiben und den Regelungen der §§ 5c bis 5e 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. Im Fall, dass der Betrieb einer Energieanlage nach Satz 1 Nummer 2 einer in Satz 1 aufgeführten besonders wichtigen und wichtigen Einrichtung im Hinblick auf die gesamte Geschäftstätigkeit dieser Einrichtung eine Nebentätigkeit darstellt, findet dieser Absatz keine Anwendung.

(6) Die §§ 30, 31, 32, 35, 36, 38 und 39 gelten nicht für

1. Finanzunternehmen nach Artikel 2 Absatz 2 der Verordnung (EU) 2022/2554 und Unternehmen, für die die Anforderungen der Verordnung (EU) 2022/2554 aufgrund von § 1a Absatz 2 und 2a 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.

(7) § 32 gilt nicht für Betreiber kritischer Anlagen, soweit sie eine Anlage für Unternehmen nach Absatz 6 Nummer 1 betreiben.

(8) 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.

(9) 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
2. durch vergleichbare landesrechtliche Vorschriften unter Bezugnahme auf diesen Absatz reguliert werden.

Fußnote

(+++ EU-Vollzitate: vgl. Liste EU-Rechtsakte G v. 2.12.2025 I Nr. 301 +++)

§ 29 Einrichtungen der Bundesverwaltung

(1) Einrichtungen der Bundesverwaltung im Sinne dieses Gesetzes sind, mit Ausnahme der Institutionen der Sozialen Sicherung und der Deutschen Bundesbank,

1. Bundesbehörden,
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.

(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.

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

Kapitel 2
Risikomanagement, Melde-, Registrierungs-, Nachweis- und Unterrichtungspflichten

§ 30 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 in 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:

1. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik,
2. Bewältigung von Sicherheitsvorfällen,
3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern,
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,
7. grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik,
8. Konzepte und Prozesse für den Einsatz von kryptographischen Verfahren,
9. Erstellung von Konzepten für die Sicherheit des Personals, die Zugriffskontrolle und für die Verwaltung von IKT-Systemen, -Produkten und -Prozessen,
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

(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.

(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 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.

(6) Besonders wichtige Einrichtungen und wichtige Einrichtungen 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.

(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 enthaltene 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 und veröffentlicht diese auf seiner Internetseite. Die Feststellung erfolgt

1. im Einvernehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe;
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. Aus Gründen des öffentlichen Interesses werden für die Feststellung keine Gebühren oder Auslagen für die Tätigkeit des Bundesamtes erhoben.

(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 gilt entsprechend.

Fußnote

(+++ EU-Vollzitate: vgl. Liste EU-Rechtsakte G v. 2.12.2025 I Nr. 301 +++)

§ 31 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.

(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.

§ 32 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. 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;
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:
    a) eine ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen;
    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;
    d) gegebenenfalls die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls.

Die Verpflichtung nach Satz 1 gilt frühestens ab Einrichtung des Meldewegs.

(2) Dauert der Sicherheitsvorfall zum in Absatz 1 Satz 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.

(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.

(6) Das Bundesamt kann meldenden Einrichtungen nach Maßgabe des § 36 Absatz 1 Angebote zu deren Unterstützung bei der Behebung des Sicherheitsvorfalls machen.

§ 33 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 folgende Angaben zu übermitteln:

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,
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
5. die für die Tätigkeiten, aufgrund derer die Registrierung erfolgt, zuständigen Aufsichtsbehörden des Bundes und der Länder.

(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 die ermittelten 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.

(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 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.

(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 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. Name der Einrichtung;
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 sie nicht in der Europäischen Union niedergelassen ist, Anschrift 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
6. die öffentlichen IP-Adressbereiche der Einrichtung.

(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 Paragraphen 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.

§ 35 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.

(2) Einrichtungen nach Absatz 1 Satz 1 aus den Sektoren Finanzwesen, Leistungen der Sozialversicherung sowie Grundsicherung für Arbeitsuchende, 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 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.

(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.

§ 37 Ausnahmebescheid

(1) Das Bundesministerium des Innern kann auf Vorschlag des Bundeskanzleramtes, des Bundesministeriums der Justiz und für Verbraucherschutz, des Bundesministeriums für Verteidigung, des Bundesministeriums der Finanzen, der Ministerien für Inneres und der 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 Ressort im Einvernehmen, im Fall der Ministerien für Inneres und der Justiz der Länder im Benehmen.

(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
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.

(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 den §§ 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.

(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 Satz 1 Nummer 1 oder 2 von einem Widerruf abgesehen werden.

§ 38 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.

(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.

(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 Nachweispflichten für Betreiber kritischer Anlagen

(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.

(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,
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.

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. Betreiber kritischer Anlagen, die bis zum Inkrafttreten dieses Gesetzes Betreiber Kritischer Infrastrukturen waren, und deren Nachweisfrist 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, innerhalb von zwölf Monaten nach Inkrafttreten dieses Gesetzes abgelaufen wäre, können in diesem Zeitraum einen Nachweis nach den bisher geltenden Vorgaben erbringen.

§ 40 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.

(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 Ziffer 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.

(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,
2. in Zusammenarbeit mit den zuständigen Aufsichtsbehörden und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe die Relevanz der Informationen nach Nummer 1 für die Verfügbarkeit kritischer Dienstleistungen zu analysieren,
3. das Lagebild bezüglich der Sicherheit in der Informationstechnik von kritischen Anlagen, besonders wichtigen Einrichtungen und wichtigen Einrichtungen kontinuierlich zu aktualisieren und
4. unverzüglich die nachfolgenden Personen oder Stellen zu unterrichten:
   a) die Betreiber kritischer Anlagen über sie betreffende Informationen nach den Nummern 1 bis 3 nach § 33 Absatz 1 Nummer 2 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 und
   c) das Auswärtige Amt über nach § 32 Absatz 1 gemeldete erhebliche Sicherheitsvorfälle mit internationalem Bezug 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.

(4) Zur Wahrnehmung seiner Aufgabe als zentrale Anlaufstelle hat das Bundesamt

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 Satz 1 Nummer 2 genannten Anfragen zu erstellen und dabei die in Absatz 1 genannten Stellen zu beteiligen oder Antworten der in Absatz 2 Satz 1 genannten Stellen an die in Absatz 2 Satz 1 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.

(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.

§ 41 Untersagung des Einsatzes kritischer Komponenten

(1) Das Bundesministerium des Innern kann gegenüber dem Betreiber kritischer Anlagen den Einsatz von kritischen Komponenten eines Herstellers im Benehmen mit dem Bundesministerium für Wirtschaft und Energie im Sektor Energie, dem Bundesministerium für Wirtschaft und Energie sowie dem Bundesministerium für Forschung, Technologie und Raumfahrt im Sektor Weltraum, dem Bundesministerium für Digitales und Staatsmodernisierung in den Sektoren Informationstechnik und Telekommunikation, dem Bundesministerium für Verkehr in den Sektoren 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 in den Sektoren Sozialversicherungsträger sowie Grundsicherung für Arbeitsuchende und dem Bundesministerium für Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit in den Sektoren Wasser sowie Siedlungsabfallentsorgung sowie dem Auswärtigen Amt untersagen oder Anordnungen dazu erlassen, wenn der Einsatz die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt.

(2) Hat das Bundesministerium des Innern einem Betreiber kritischer Anlagen den Einsatz einer kritischen Komponente untersagt oder eine Anordnung dazu erlassen, kann es im Benehmen mit dem in Absatz 1 genannten Bundesministerium

1. dem Betreiber kritischer Anlagen auch den zukünftigen Einsatz weiterer kritischer Komponenten desselben Herstellers und desselben Komponententyps untersagen oder Anordnungen dazu erlassen,
2. allen Betreibern kritischer Anlagen den Einsatz derselben kritischen Komponente desselben Herstellers sowie von weiteren kritischen Komponenten desselben Komponententyps desselben Herstellers untersagen oder Anordnungen dazu erlassen.

(3) Die Entscheidung nach Satz 1 Nummer 2 ergeht als Allgemeinverfügung. Widerspruch und Klage gegen eine Untersagung oder Anordnung nach den Absätzen 1 und 2 Satz 1 haben keine aufschiebende Wirkung.

(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) Der Betreiber kritischer Anlagen ist zur Mitwirkung bei der Ermittlung des Sachverhalts verpflichtet. Dafür hat er auf Verlangen alle für das Verfahren erheblichen Tatsachen vollständig und wahrheitsgemäß mitzuteilen und die ihm bekannten Beweismittel anzugeben.

§ 42 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.

Kapitel 3
Informationssicherheit der Einrichtungen der Bundesverwaltung

§ 43 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. Die Einrichtungen der Bundesverwaltung weisen dem Bundesamt die Erfüllung der Anforderungen nach Satz 1 spätestens fünf Jahre nach Inkrafttreten dieses Gesetzes und anschließend regelmäßig nach seinen Vorgaben nach.

(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.

(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.

(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 Satz 3 sind der Bundesnachrichtendienst und das Bundesamt für Verfassungsschutz.

(6) Das Bundesministerium des Innern erlässt im Einvernehmen mit den Ressorts allgemeine Verwaltungsvorschriften zur Durchführung des Absatzes 5.

§ 44 Vorgaben des Bundesamtes

(1) Die Einrichtungen der Bundesverwaltung müssen Mindestanforderungen zum Schutz der in der Bundesverwaltung verarbeiteten Informationen erfüllen. Die Mindestanforderungen ergeben sich aus den BSI-Standards und dem Grundschutzkompendium (IT-Grundschutz) sowie aus den Mindeststandards für die Sicherheit in der Informationstechnik des Bundes (Mindeststandards) in den jeweils geltenden Fassungen. Die jeweils geltenden Fassungen werden auf der Internetseite des Bundesamtes veröffentlicht. Die Mindeststandards legt das Bundesamt im Benehmen mit den Ressorts und weiteren obersten Bundesbehörden fest. Der IT-Grundschutz und die Mindeststandards werden durch das Bundesamt regelmäßig evaluiert und entsprechend dem Stand der Technik sowie unter Berücksichtigung der Erfahrungen aus der Praxis und aus der Beratung und Unterstützung nach Absatz 3 fortentwickelt; dabei wird der Umsetzungsaufwand soweit möglich minimiert. Das Bundesamt wird den IT-Grundschutz bis zum 1. Januar 2026 modernisieren und fortentwickeln. Für die Verpflichtung nach Satz 1 gelten die Ausnahmen nach § 7 Absatz 6 und 7 entsprechend.

(2) Durch die Umsetzung der Mindestanforderungen nach Absatz 1 Satz 1 ist 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 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) Das Bundesamt berät die Einrichtungen der Bundesverwaltung auf Ersuchen bei der Umsetzung und Einhaltung der Mindestanforderungen nach Absatz 1 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 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) Für die Einrichtungen der Bundesverwaltung kann das Bundesministerium des Innern 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 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.

(2) Für die Erfüllung ihrer Aufgaben ist eine zielgerichtete Befähigung der Informationssicherheitsbeauftragten der Einrichtungen der Bundesverwaltung notwendig. Die Informationssicherheitsbeauftragen 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 jeweils zuständigen Informationssicherheitsbeauftragten 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.

§ 46 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 seinem oder ihrem 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.

(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.

(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. Er oder sie darf von seiner oder ihrer jeweiligen Einrichtung wegen der Erfüllung seiner oder ihrer Aufgaben nicht abberufen oder benachteiligt werden.

§ 47 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.

(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.

(3) In der Regel bestellt diejenige Einrichtung den Informationssicherheitsbeauftragten nach Satz 1, die für die Steuerung des Digitalisierungsvorhabens oder die 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 für Digitales und Staatsmodernisierung.

(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.

§ 48 Amt des Koordinators für Informationssicherheit

(1) Die Leitung des Bundesamtes für Sicherheit in der Informationstechnik nimmt die Aufgaben der Koordinatorin oder des Koordinators der Bundesregierung für Informationssicherheit wahr. Die Fachaufsicht über das Bundesamt in Bezug auf seine Rolle als Koordinatorin oder Koordinator für Informationssicherheit liegt beim Bundesministerium für Digitales und Staatsmodernisierung.

(2) Die Koordinatorin oder der Koordinator koordiniert das operative Informationssicherheitsmanagement des Bundes. Im Benehmen mit den obersten Bundesbehörden entwickelt sie oder er Programme zur Gewährleistung der Informationssicherheit des Bundes und schreibt diese fort.

(3) Auf Basis der durch das Bundesamt erhaltenen Informationen wahrt die Koordinatorin oder der Koordinator den Überblick über den Stand der Informationssicherheit in der Bundesverwaltung. Auf dieser Grundlage beaufsichtigt sie oder er die Umsetzung der Programme zur Gewährleistung der Informationssicherheit des Bundes.

(4) Die Koordinatorin oder der Koordinator unterstützt die Ressorts bei der Umsetzung der Vorgaben nach diesem Gesetz und wirkt gemeinsam mit dem Bundesministerium für Digitales und Staatsmodernisierung im Benehmen mit dem Bundesministerium des Innern auf ein angemessenes Verhältnis zwischen dem Einsatz von Informationstechnik und Informationssicherheit hin.

(5) Zur Wahrnehmung ihrer oder seiner Aufgaben hat die Koordinatorin oder der Koordinator ein direktes halbjährliches Vortragsrecht vor den zuständigen Ausschüssen des Deutschen Bundestages zu den in den Absätzen 1 bis 3 benannten Themen.

(6) Die Koordinatorin oder der Koordinator wird bei allen Gesetzes-, Verordnungs- und sonstigen wichtigen Vorhaben beteiligt, soweit sie Fragen der Informationssicherheit berühren.

Teil 4
Datenbanken der Domain-Name-Registrierungsdaten

§ 49 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.

(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;
2. das Datum der Registrierung;
3. den Namen des Domain-Inhabers, seine E-Mail-Adresse und Telefonnummer;
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 6. März 2026 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.

§ 50 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 seiner 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.

(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 6. März 2026 öffentlich zugänglich zu machen.

(3) Das Auskunftsverfahren bei Bestandsdaten gemäß § 22 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes bleibt unberührt.

(4) Das Bundesamt kann die Erfüllung der Vorgaben überprüfen.

§ 51 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.

Teil 5
Zertifizierung, Konformitätserklärung und Kennzeichen

§ 52 Zertifizierung

(1) Das Bundesamt ist nationale Zertifizierungsstelle der Bundesverwaltung für IT-Sicherheit.

(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 die Bewertung können durch vom Bundesamt nach Absatz 7 anerkannte sachverständige Stellen erfolgen.

(4) Das Sicherheitszertifikat wird erteilt, wenn

1. die informationstechnischen Systeme, Komponenten, Produkte oder Schutzprofile den vom Bundesamt festgelegten Kriterien entsprechen und
2. das Bundesministerium des Innern die Erteilung des Zertifikats nicht nach Absatz 5 untersagt hat.

Vor Erteilung des Sicherheitszertifikats legt das Bundesamt den Vorgang dem Bundesministerium des Innern zur Prüfung nach Absatz 5 vor.

(5) Das Bundesministerium des Innern 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.

(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
2. das Bundesministerium des Innern 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.

(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.

§ 53 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 vornimmt. 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-Sicherheitsdienstleisters 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

1. den Inhalt und das Format der Konformitätserklärung,
2. Nachweise und Verfahren, die die Angaben der Konformitätserklärung belegen,
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,
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 -Dienst, den -Prozess, die Person oder die IT-Sicherheitsdienstleistung oder
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.

(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.

(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 seiner 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
3. Konformitätserklärungen nach Absatz 1 für ungültig erklären.

(6) Für Maßnahmen nach Absatz 4 kann das Bundesamt Gebühren erheben, sofern es aufgrund von Anhaltspunkten tätig geworden ist, die berechtigte Zweifel an der Einhaltung der Anforderungen der Technischen Richtlinie oder dieses Paragraphen begründeten.

§ 54 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.

(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.

(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.

(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 diesem Paragraphen 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,

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.

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,

1. sofern die Voraussetzungen des maßgeblichen europäischen Schemas für die Cybersicherheitszertifizierung nach Artikel 54 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.

Fußnote

(+++ EU-Vollzitate: vgl. Liste EU-Rechtsakte G v. 2.12.2025 I Nr. 301 +++)

§ 55 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.

(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
2. einer Information des Bundesamtes über sicherheitsrelevante IT-Eigenschaften des Produktes (Sicherheitsinformation).

(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.

(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,
2. die Herstellererklärung plausibel und durch die beigefügten Unterlagen ausreichend belegt ist und
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.

(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.

(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
2. die Freigabe des IT-Sicherheitskennzeichens widerrufen.

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.

Teil 6
Verordnungsermächtigungen, Grundrechtseinschränkungen und Berichtspflichten

§ 56 Ermächtigung zum Erlass von Rechtsverordnungen

(1) Das Bundesministerium des Innern bestimmt nach Anhörung der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, das Nähere über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen nach § 52 und deren Inhalt.

(2) Das Bundesministerium des Innern bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie und dem Bundesministerium für Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit 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.

(3) Das Bundesministerium des Innern bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Finanzen, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium der Verteidigung, dem Bundesministerium für Landwirtschaft, Ernährung und Heimat, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr, dem Bundesministerium für Forschung, Technologie und Raumfahrt, dem Bundesministerium für Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit und dem Bundesministerium für Digitales und Staatsmodernisierung 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.

(4) Das Bundesministerium des Innern bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Finanzen, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium der Verteidigung, dem Bundesministerium für Landwirtschaft, Ernährung und Heimat, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr, dem Bundesministerium für Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit, dem Bundesministerium für Forschung, Technologie und Raumfahrt und dem Bundesministerium für Digitales und Staatsmodernisierung 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.

(5) Das Bundesministerium des Innern kann im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie und im Benehmen mit dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Landwirtschaft, Ernährung und Heimat, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr, dem Bundesministerium der Verteidigung, dem Bundesministerium für Umwelt, Klimaschutz, Naturschutz und nukleare Sicherheit, dem Bundesministerium für Forschung, Technologie und Raumfahrt und dem Bundesministerium für Digitales und Staatsmodernisierung 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.

(6) Das Bundesministerium des Innern 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.

(7) Das Bundesministerium des Innern kann durch Rechtsverordnungen, die nicht der Zustimmung des Bundesrates bedürfen, für jeweils einen der in § 2 Nummer 24 aufgeführten Sektoren im Einvernehmen mit dem in § 41 Absatz 1 für den jeweiligen Sektor genannten Bundesministerium kritische Komponenten im Sinne des § 2 Nummer 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 kritischer Anlagen oder zu anderen Beeinträchtigungen der öffentlichen Ordnung oder Sicherheit führen könnte.

(8) Die in § 41 Absatz 1 genannten Bundesministerien können dem Bundesministerium des Innern einen Vorschlag für den Erlass einer Rechtsverordnung im Sinne des Absatzes 7 vorlegen. Das Vorschlagsrecht betrifft nur den Sektor im Sinne des § 2 Nummer 24, für den das jeweilige Bundesministerium in § 41 Absatz 1 genannt wird.

§ 57 Einschränkung von Grundrechten

Das Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) wird durch die §§ 7, 8, 9, 11, 12, 15 und 16 eingeschränkt.

§ 58 Berichtspflichten des Bundesamtes

(1) Das Bundesamt unterrichtet das Bundesministerium des Innern über seine Tätigkeit.

(2) Die Unterrichtung nach Absatz 1 dient auch der Aufklärung der Öffentlichkeit durch das Bundesministerium des Innern 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 unterrichtet kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres den Innenausschuss des Deutschen Bundestages über die Anwendung dieses Gesetzes. Es geht dabei auch auf die Fortentwicklung des maßgeblichen Unionsrechts ein.

(4) Das Bundesamt legt der Agentur der Europäischen Union für Cybersicherheit jeweils zum 18. Januar, 18. April, 18. Juli und zum 18. Oktober eines jeden Jahres einen zusammenfassenden Bericht vor, der anonymisierte und aggregierte Daten zu erheblichen Sicherheitsvorfällen, erheblichen Cyberbedrohungen und Beinahevorfällen enthält, die gemäß § 32 und § 5 Absatz 2 gemeldet wurden.

(5) Das Bundesamt übermittelt zum 17. April 2027 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
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
Aufsicht

§ 59 Zuständigkeit des Bundesamtes

Das Bundesamt ist die zuständige Aufsichtsbehörde für die Einhaltung der Vorschriften in Teil 3

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
3. durch Einrichtungen der Bundesverwaltung.

§ 60 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.

(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.

(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.

(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.

§ 61 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.

(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.

(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.

(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 aufgrund 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.

(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.

(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
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

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.

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.

(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 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.

Fußnote

(+++ EU-Vollzitate: vgl. Liste EU-Rechtsakte G v. 2.12.2025 I Nr. 301 +++)

§ 62 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.

§ 63 Verwaltungszwang

Sofern das Bundesamt Zwangsgelder verhängt, beträgt deren Höhe abweichend von § 11 Absatz 3 des Verwaltungsvollstreckungsgesetzes bis zu 100 000 Euro.

§ 64 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.

Teil 8
Bußgeldvorschriften

§ 65 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.

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. einer vollziehbaren Anordnung nach

a) § 11 Absatz 6, § 16 Absatz 1 Satz 1 Nummer 1, auch in Verbindung mit Absatz 3, Nummer 2, § 17 Satz 1 oder § 39 Absatz 1 Satz 5,

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

d) § 35 Absatz 1 Satz 1 oder § 36 Absatz 2 Satz 1

zuwiderhandelt,

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,
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,
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,
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,
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 Satz 2 eine Mitteilung oder Angabe nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,
12. entgegen § 49 Absatz 3 Satz 1 eine dort genannte Vorgabe oderein dort genanntes Verfahren nicht vorhält,
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,
14. entgegen § 50 Absatz 1 Satz 1 einen Zugang nicht oder nicht rechtzeitig gewährt,
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,
16. entgegen § 53 Absatz 3 Satz 2 oder § 54 Absatz 2 Satz 2 tätig wird oder
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.

(4) Ordnungswidrig handelt, wer gegen die Verordnung (EU) 2019/881 in der Fassung vom 19. Dezember 2024 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
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:

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,
   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 11 mit einer Geldbuße bis zu fünf Millionen Euro,
3. in den Fällen des Absatzes 2 Nummer 1 Buchstabe a mit einer Geldbuße bis zu zwei Millionen Euro,
4. in den Fällen des Absatzes 1 und des Absatzes 2 Nummer 10 mit einer Geldbuße bis zu einer Million Euro,
5. 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
6. 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.

In den Fällen des Satzes 1 Nummer 3 und 4 ist § 30 Absatz 2 Satz 3 des Gesetzes über Ordnungswidrigkeiten anzuwenden.

(6) Gegenüber einer besonders wichtigen Einrichtung im Sinne des § 28 Absatz 1 Satz 1 mit einem Gesamtumsatz von mehr als 500 Millionen Euro kann abweichend von Absatz 5 Satz 1 Nummer 1 Buchstabe a, auch in Verbindung mit § 30 Absatz 2 Satz 2 des Gesetzes über Ordnungswidrigkeiten, 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 Gesamtumsatzes geahndet werden.

(7) Gegenüber einer wichtigen Einrichtung im Sinne des § 28 Absatz 2 Satz 1 mit einem Gesamtumsatz von mehr als 500 Millionen Euro kann abweichend von Absatz 5 Satz 1 Nummer 1 Buchstabe b, auch in Verbindung mit § 30 Absatz 2 Satz 2 des Gesetzes über Ordnungswidrigkeiten, 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 Gesamtumsatzes geahndet werden.

(8) Gesamtumsatz im Sinne der Absätze 6 und 7 ist die Summe aller Umsatzerlöse, die das Unternehmen, dem die besonders wichtige Einrichtung oder die wichtige Einrichtung angehört, in dem der Behördenentscheidung vorausgegangenen Geschäftsjahr weltweit erzielt hat. Der Gesamtumsatz kann geschätzt werden.

(9) § 17 Absatz 2 des Gesetzes über Ordnungswidrigkeiten ist in den Fällen des Absatzes 5 Satz 1 Nummer 1 sowie der Absätze 6 und 7 nicht anzuwenden.

(10) Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist

1. in den Fällen des Absatzes 2 Nummer 11 das Bundesministerium des Innern und
2. in den Fällen der Absätze 1, 3 und 4 sowie in den Fällen des Absatzes 2, die nicht in Nummer 1 genannt sind, das Bundesamt.

(11) 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.

Fußnote

(+++ EU-Vollzitate: vgl. Liste EU-Rechtsakte G v. 2.12.2025 I Nr. 301 +++)

Anlage 1

Sektoren besonders wichtiger und wichtiger Einrichtungen

(Fundstelle: BGBl. 2025 I Nr. 301, S. 43 - 46)

Spalte A	Spalte B	Spalte C	Spalte D
Nummer	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
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 Fernkälteversorgung	
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
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

Spalte A	Spalte B	Spalte C	Spalte D
Nummer	Sektor	Branche	Einrichtungsart
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, die für gewerbliche Zwecke genutzt werden
2.1.2			Flughafenleitungsorgane nach Artikel 2 Nummer 2 der Richtlinie 2009/12/EG, Flughäfen nach Artikel 2 Nummer 1 jener Richtlinie, einschließlich der in Anhang II Abschnitt 2 der Verordnung (EU) Nr. 1315/2013 aufgeführten Flughäfen des Kernnetzes, und Einrichtungen, die innerhalb von Flughäfen befindliche zugehörige Einrichtungen betreiben
2.1.3			ATM/ANS-Anbieter nach Artikel 2 Nummer 2 der Durchführungsverordnung (EU) 2017/373
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 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, einschließlich ihrer Hafenanlagen nach Artikel 2 Nummer 11 der Verordnung (EG) Nr. 725/2004, sowie Einrichtungen, die

Spalte A	Spalte B	Spalte C	Spalte D
Nummer	Sektor	Branche	Einrichtungsart
			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 Systems 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 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 2011/24/EU
4.1.2			EU-Referenzlaboratorien nach Artikel 15 der Verordnung (EU) 2022/2371
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

Spalte A	Spalte B	Spalte C	Spalte D
Nummer	Sektor	Branche	Einrichtungsart
			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 („Liste kritischer Medizinprodukte für Notlagen im Bereich der öffentlichen Gesundheit“) eingestuft werden
5	**Wasser**		
5.1		Trinkwasserversorgung	
5.1.1			Betreiber von Wasserversorgungsanlagen 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 § 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			Vertrauensdiensteanbieter
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

Spalte A	Spalte B	Spalte C	Spalte D
Nummer	Sektor	Branche	Einrichtungsart
			privaten Parteien befinden und von diesen verwaltet und betrieben werden und die Erbringung von weltraumgestützten Diensten unterstützen, ausgenommen Anbieter öffentlicher elektronischer Kommunikationsnetze

Fußnote

(+++ EU-Vollzitate: vgl. Liste EU-Rechtsakte G v. 2.12.2025 I Nr. 301 +++)

Anlage 2

Sektoren wichtiger Einrichtungen

(Fundstelle: BGBl. 2025 I Nr. 301, S. 47 - 48)

Spalte A	Spalte B	Spalte C	Spalte D
Nummer	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	**Abfall-bewirtschaftung**		
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 Nummer 9 und 11 der Verordnung (EG) Nr. 1907/2006 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 Verordnung unterliegen

Spalte A	Spalte B	Spalte C	Spalte D
Nummer	Sektor	Branche	Einrichtungsart
4	**Produktion, Verarbeitung und Vertrieb von Lebensmitteln**		
4.1.1			Lebensmittelunternehmen nach Artikel 3 Nummer 2 der Verordnung (EG) Nr. 178/2002, 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 herstellen, und Unternehmen, die In-vitro-Diagnostika nach Artikel 2 Nummer 2 der Verordnung (EU) 2017/746 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 („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	

Spalte A	Spalte B	Spalte C	Spalte D
Nummer	Sektor	Branche	Einrichtungsart
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

Fußnote

(+++ EU-Vollzitate: vgl. Liste EU-Rechtsakte G v. 2.12.2025 I Nr. 301 +++)