Cybersicherheitsrecht für die Bundesverwaltung

herausgegeben von

Prof. Dr. Lorenz Franck

Hochschule des Bundes für öffentliche Verwaltung, Brühl

Textausgaben Informationsrecht | Band III

2025

Vorwort

„Ein Blick ins Gesetz erleichtert die Rechtsfindung." Diese mal ironisch, mal grundehrlich gebrauchte Juristenweisheit gerät beim Informationssicherheitsrecht insgesamt und bei dessen Teilmenge Cybersicherheit an ihre Machbarkeitsgrenzen. Da es sich bei dem Thema um eine Querschnittsmaterie handelt, findet sich eine bunte Vielfalt an komplexen, in Einzelgesetzen verstreuten Vorschriften. Es gibt nicht das eine zentrale Gesetzbuch, anhand dessen der Rechtssuchende schnell und zielgerichtet ermitteln könnte, was im konkreten Fall gilt und was nicht.

Immerhin definiert Art. 2 Nr. 1 CSA nunmehr den Begriff „Cybersicherheit" als alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen. Hier reüssiert die Menschzentriertheit, die dem Datenschutzrecht als Urahn aller Informationssicherheitsrechte immer schon eigen war.

Angelehnt an den hergebrachten Begriff der „Kybernetik" werden im Cybersicherheitsrecht die Einflüsse des Menschen auf die Technik und gleichsam die Einflüsse der Technik auf den Menschen im Zusammenhang mit Mensch-Maschine-Kommunikation, -Interaktion und-Integration ganzheitlich mitgedacht. Das Cybersicherheitsrecht nähert sich insofern der freiheitsermöglichenden und -erhaltenden Funktion des Datenschutzrechts an. Eine Regulierung der Cybersicherheit ist dementsprechend kein Selbstzweck, sondern mündet, insbesondere in der öffentlichen Verwaltung, unmittelbar in effektiven Grundrechtsschutz.

Die vorliegende Sammlung enthält u.a. die NIS2-RL. In einer idealen Welt hätte es des Abdrucks wohl nicht bedurft. Bis zum 17. Oktober 2024 hatten die Mitgliedsstaaten Zeit, die Richtlinie in nationales Recht umzusetzen. Dies ist in Deutschland allerdings nicht passiert. Wohl oder übel stellt sich nun die Frage nach einer unmittelbaren Anwendbarkeit hinreichend konkreter NIS2-Vorschriften. Das ist nicht lediglich von akademischem Interesse, etwa in den Veranstaltungen des Studienganges Digital Administration & Cyber Security an der Hochschule des Bundes, sondern zeitigt auch ganz praktische Auswirkungen für die öffentliche Verwaltung.

Brühl im Mai 2025

Lorenz Franck

Inhaltsverzeichnis

Vorwort 3
Inhaltsverzeichnis 5

Unionales Cybersicherheitsrecht

CSA 7
NIS2-RL 32

Nationales Cybersicherheitsrecht

BSIG 86
BSI-KritisV 129
BSI-ZertV 177
BSI-ITSiKV 188
TKG (Auszug) 194
AtG (Auszug) 200
EnWG (Auszug) 201

Geheimschutz & Geheimnisschutz

SÜG 204
VSA (Anhang zu § 35 SÜG) 233
SÜFV 282
SatDSiG 288
HinSchG 304

Strafrecht

StGB (Auszug) 329

VERORDNUNG (EU) 2019/881 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 17. April 2019

über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit)

(Text von Bedeutung für den EWR)

Inhaltsübersicht

TITEL I
ALLGEMEINE BESTIMMUNGEN

Art. 1 Gegenstand und Geltungsbereich

Art. 2 Begriffsbestimmungen

TITEL II
ENISA (AGENTUR DER EUROPÄISCHEN UNION FÜR CYBERSICHERHEIT)

[Vom Abdruck wurde abgesehen.]

TITEL III
ZERTIFIZIERUNGSRAHMEN FÜR DIE CYBERSICHERHEIT

Art. 46 Europäischer Zertifizierungsrahmen für die Cybersicherheit

Art. 47 Das fortlaufende Arbeitsprogramm der Union für die europäische Cybersicherheitszertifizierung

Art. 48 Auftrag für ein europäisches Schema für die Cybersicherheitszertifizierung

Art. 49 Ausarbeitung, Annahme und Überarbeitung der europäischen Schemata für die Cybersicherheitszertifizierung

Art. 50 Website zu europäischen Schemata für die Cybersicherheitszertifizierung

Art. 51 Sicherheitsziele der europäischen Schemata für die Cybersicherheitszertifizierung

Art. 52 Vertrauenswürdigkeitsstufen der europäischen Schemata für die Cybersicherheitszertifizierung

Art. 53 Selbstbewertung der Konformität

Art. 54 Elemente der europäischen Schemata für die Cybersicherheitszertifizierung

Art. 55 Ergänzende Informationen über die Cybersicherheit von zertifizierten IKT-Produkten, -Diensten und -Prozessen

Art. 56 Cybersicherheitszertifizierung

Art. 57 Nationale Cybersicherheitszertifizierungsschemata und Cybersicherheitszertifikate
Art. 58 Nationale Behörden für die Cybersicherheitszertifizierung
Art. 59 Gegenseitige Begutachtung
Art. 60 Konformitätsbewertungsstellen
Art. 61 Notifikation
Art. 62 Europäische Gruppe für die Cybersicherheitszertifizierung
Art. 63 Beschwerderecht
Art. 64 Recht auf einen wirksamen gerichtlichen Rechtsbehelf
Art. 65 Sanktionen

TITEL IV
SCHLUSSBESTIMMUNGEN

Art. 66 Ausschussverfahren
Art. 67 Bewertung und Überarbeitung
Art. 68 Aufhebung und Rechtsnachfolge
Art. 69 Inkrafttreten

[Vom Abdruck der Erwägungsgründe wurde abgesehen.]

TITEL I
ALLGEMEINE BESTIMMUNGEN

Artikel 1
Gegenstand und Geltungsbereich

(1) Um das ordnungsgemäße Funktionieren des Binnenmarkts zu gewährleisten und um gleichzeitig in der Union ein hohes Niveau in der Cybersicherheit, bei der Fähigkeit zur Abwehr gegen Cyberangriffe und beim Vertrauen in die Cybersicherheit zu erreichen, wird in dieser Verordnung Folgendes festgelegt:

a) die Ziele, Aufgaben und organisatorischen Aspekte der ENISA (Agentur der Europäischen Union für Cybersicherheit) und

b) ein Rahmen für die Festlegung europäischer Schemata für die Cybersicherheitszertifizierung, mit dem Ziel, für IKT- Produkte und -Dienste und -Prozesse in der Union ein angemessenes Maß an Cybersicherheit zu gewährleisten und mit dem Ziel, eine Fragmentierung des Binnenmarkts bei Zertifizierungsschemata, in der Union zu verhindern.

Der Rahmen nach Unterabsatz 1 Buchstabe b gilt unbeschadet der in anderen Rechtsakten der Union festgelegten Bestimmungen in Bezug auf eine freiwillige oder verbindliche Zertifizierung.

(2) Von dieser Verordnung unberührt bleiben die Zuständigkeiten der Mitgliedstaaten für Tätigkeiten in Bezug auf die öffentliche Sicherheit, die Landesverteidigung, die nationale Sicherheit und das staatliche Handeln im strafrechtlichen Bereich.

Artikel 2
Begriffsbestimmungen

Für die Zwecke dieser Verordnung gelten folgende Begriffsbestimmungen:

1. „Cybersicherheit“ bezeichnet alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen;
2. „Netz- und Informationssystem“ bezeichnet ein Netz- und Informationssystem im Sinne des Artikels 4 Nummer 1 der Richtlinie (EU) 2016/1148;
3. „nationale Strategie für die Sicherheit von Netz- und Informationssystemen“ bezeichnet eine nationale Strategie für die Sicherheit von Netz- und Informationssystemen im Sinne des Artikels 4 Nummer 3 der Richtlinie (EU) 2016/1148;
4. „Betreiber wesentlicher Dienste“ bezeichnet einen Betreiber wesentlicher Dienste im Sinne des Artikels 4 Nummer 4 der Richtlinie (EU) 2016/1148;
5. „Anbieter digitaler Dienste“ bezeichnet einen Anbieter digitaler Dienste im Sinne des Artikels 4 Nummer 6 der Richtlinie (EU) 2016/1148;
6. „Sicherheitsvorfall“ bezeichnet einen Sicherheitsvorfall im Sinne des Artikels 4 Nummer 7 der Richtlinie (EU) 2016/1148;
7. „Bewältigung von Sicherheitsvorfällen“ bezeichnet die Bewältigung von Sicherheitsvorfällen im Sinne des Artikels 4 Nummer 8 der Richtlinie (EU) 2016/1148;
8. „Cyberbedrohung“ bezeichnet einen möglichen Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte;
9. „europäisches Schema für die Cybersicherheitszertifizierung“ bezeichnet ein umfassendes Paket von Vorschriften, technischen Anforderungen, Normen und Verfahren, die auf Unionsebene festgelegt werden und für die Zertifizierung oder Konformitätsbewertung von bestimmten IKT-Produkten, -Diensten und -Prozessen gelten;
10. „nationales Schema für die Cybersicherheitszertifizierung“ bezeichnet ein umfassendes, von einer nationalen Behörde ausgearbeitetes und erlassenes Paket von Vorschriften, technischen Anforderungen, Normen und Verfahren, die für die Zertifizierung oder Konformitätsbewertung von IKT-Produkten, -Diensten und -Prozessen gelten, die von diesem Schema erfasst werden;
11. „europäisches Cybersicherheitszertifikat“ bezeichnet ein von der maßgeblichen Stelle ausgestelltes Dokument, in dem bescheinigt wird, dass ein bestimmtes IKT-Produkt, ein bestimmter IKT-Dienst oder ein bestimmter IKT-Prozess im Hinblick auf die Erfüllung besonderer Sicherheitsanforderungen, die in einem europä-

ischen Schema für die Cybersicherheitszertifizierung festgelegt sind, bewertet wurde;

12. „IKT-Produkt“ bezeichnet ein Element oder eine Gruppe von Elementen eines Netz- oder Informationssystems;

13. „IKT-Dienst“ bezeichnet einen Dienst, der vollständig oder überwiegend aus der Übertragung, Speicherung, Abfrage oder Verarbeitung von Informationen mittels Netz- und Informationssystemen besteht;

14. „IKT-Prozess“ bezeichnet jegliche Tätigkeiten, mit denen ein ITK-Produkt oder -Dienst konzipiert, entwickelt, bereitgestellt oder gepflegt werden soll;

15. „Akkreditierung“ bezeichnet die Akkreditierung im Sinne des Artikels 2 Nummer 10 der Verordnung (EG) Nr. 765/2008;

16. „nationale Akkreditierungsstelle“ bezeichnet eine nationale Akkreditierungsstelle im Sinne des Artikels 2 Nummer 11 der Verordnung (EG) Nr. 765/2008;

17. „Konformitätsbewertung“ bezeichnet eine Konformitätsbewertung im Sinne des Artikels 2 Nummer 12 der Verordnung (EG) Nr. 765/2008;

18. „Konformitätsbewertungsstelle“ bezeichnet eine Konformitätsbewertungsstelle im Sinne des Artikels 2 Nummer 13 der Verordnung (EG) Nr. 765/2008;

19. „Norm“ bezeichnet eine Norm im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 1025/2012;

20. „technische Spezifikation“ bezeichnet ein Dokument, in dem die technischen Anforderungen, denen ein IKT-Prozess, -Produkt oder -Dienst genügen muss oder ein diesbezügliches Konformitätsbewertungsverfahren vorgeschrieben sind;

21. „Vertrauenswürdigkeitsstufe“ bezeichnet die Grundlage für das Vertrauen darin, dass ein IKT-Produkt, -Dienst oder -Prozess den Sicherheitsanforderungen eines spezifischen europäischen Schemas für die Cybersicherheitszertifizierung genügt, gibt an, auf welchem Niveau das IKT-Produkt, der IKT-Dienst oder der IKT-Prozess, bei der Bewertung eingestuft wurde, misst jedoch als solche nicht die Sicherheit des IKT-Produkts, -Dienstes oder -Prozesses;

22. „Selbstbewertung der Konformität“ bezeichnet eine Maßnahme eines Herstellers oder Anbieters von IKT-Produkten, -Diensten oder -Prozessen zur Bewertung, ob diese IKT- Produkte, -Dienste oder -Prozesse die Anforderungen, die in einem spezifischen europäischen Schema für die Cybersicherheitszertifizierung festgelegt sind, erfüllen.

TITEL II
ENISA (AGENTUR DER EUROPÄISCHEN UNION FÜR CYBERSICHERHEIT)

[Vom Abdruck wurde abgesehen.]

TITEL III
ZERTIFIZIERUNGSRAHMEN FÜR DIE CYBERSICHERHEIT

Artikel 46
Europäischer Zertifizierungsrahmen für die Cybersicherheit

(1) Der europäische Zertifizierungsrahmen für die Cybersicherheit wird geschaffen, um die Voraussetzungen für einen funktionierenden Binnenmarkt zu verbessern, indem die Cybersicherheit in der Union erhöht wird und indem im Hinblick auf die Schaffung eines digitalen Binnenmarkts für IKT-Produkte, -Dienste und -Prozesse ein harmonisierter Ansatz auf Unionsebene für europäische Schemata für die Cybersicherheitszertifizierung ermöglicht wird.

(2) Der europäische Zertifizierungsrahmen für die Cybersicherheit legt einen Mechanismus fest, mit dem europäische Schemata für die Cybersicherheitszertifizierung geschaffen werden und mit dem bescheinigt wird, dass die nach einem solchen Schema bewerteten IKT-Produkte, -Dienste und -Prozesse den festgelegten Sicherheitsanforderungen genügen, um die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von gespeicherten, übermittelten oder verarbeiteten Daten, Funktionen oder Diensten, die von diesen Produkten, Diensten und Prozessen angeboten oder über diese zugänglich gemacht werden, während deren gesamten Lebenszyklus zu schützen.

Artikel 47
Das fortlaufende Arbeitsprogramm der Union für die europäische Cybersicherheitszertifizierung

(1) Die Kommission veröffentlicht ein fortlaufendes Arbeitsprogramm der Union für die europäische Cybersicherheitszertifizierung (im Folgenden „fortlaufendes Arbeitsprogramm der Union"), in dessen Rahmen die strategischen Prioritäten für künftige europäische Schemata für die Cybersicherheitszertifizierung festgelegt werden sollen.

(2) Das fortlaufende Arbeitsprogramm der Union umfasst insbesondere eine Liste der IKT-Produkte, -Dienste und -Prozesse oder Kategorien davon, die von der Aufnahme in ein europäisches Schema für die Cybersicherheitszertifizierung profitieren können.

(3) Die Aufnahme bestimmter IKT-Produkte, -Dienste und -Prozesse oder bestimmter Kategorien davon in das fortlaufende Arbeitsprogramm der Union muss aus einem oder mehreren der folgenden Gründe gerechtfertigt sein:

a) Verfügbarkeit und Entwicklung nationaler Schemata für die Cybersicherheitszertifizierung für bestimmte Kategorien von IKT-Produkten, -Diensten oder -Prozessen, insbesondere im Hinblick auf das Risiko der Fragmentierung;

b) einschlägige Politik oder einschlägiges Recht der Union oder der Mitgliedstaaten;

c) Nachfrage auf dem Markt;

d) Entwicklungen in der Cyberbedrohungslandschaft;

e) Beauftragung mit der Ausarbeitung eines bestimmten möglichen Schemas durch die Europäische Gruppe für die Cybersicherheitszertifizierung.

(4) Die Kommission trägt den Stellungnahmen der Europäischen Gruppe für die Cybersicherheitszertifizierung und der Gruppe der Interessenträger für die Cybersicherheitszertifi-

zierung zum Entwurf des fortlaufenden Arbeitsprogramm der Union gebührend Rechnung.

(5) Das erste fortlaufende Arbeitsprogramm der Union wird spätestens am 28. Juni 2020 vorgelegt. Das fortlaufende Arbeitsprogramm der Union mindestens alle drei Jahre, und bei Bedarf öfter aktualisiert.

Artikel 48
Auftrag für ein europäisches Schema für die Cybersicherheitszertifizierung

(1) Die Kommission kann die ENISA damit beauftragen, ein mögliches Schema auszuarbeiten oder ein bestehendes europäisches Schema für die Cybersicherheitszertifizierung auf der Grundlage des fortlaufenden Arbeitsprogramm der Union zu überarbeiten.

(2) In entsprechend begründeten Fällen kann die Kommission oder die Europäische Gruppe für die Cybersicherheitszertifizierung die ENISA damit beauftragen, ein mögliches Schema auszuarbeiten oder ein bestehendes europäisches Schema für die Cybersicherheitszertifizierung, das nicht im fortlaufenden Arbeitsprogramm der Union enthalten ist, zu überarbeiten. Das fortlaufende Arbeitsprogramm der Union wird entsprechend aktualisiert.

Artikel 49
Ausarbeitung, Annahme und Überarbeitung der europäischen Schemata für die Cybersicherheitszertifizierung

(1) Auf Auftrag der Kommission arbeitet die ENISA gemäß Artikel 48 ein mögliches Schema aus, das den in den Artikeln 51, 52und 54 festgelegten Anforderungen genügt.

(2) nach einem Auftrag der Europäischen Gruppe für die Cybersicherheitszertifizierung gemäß Artikel 48 Absatz 2 kann die ENISA ein mögliches Schema ausarbeiten, das den in den Artikeln 51, 52und 54 festgelegten Anforderungen genügt. Lehnt die ENISA einen solchen Auftrag ab, so muss sie dies begründen. Jede Entscheidung, einen Auftrag abzulehnen, wird vom Verwaltungsrat getroffen.

(3) Bei der Ausarbeitung der möglichen Schemata konsultiert die ENISA alle in Frage kommenden Interessenträger im Wege eines förmlichen, offenen, transparenten und inklusiven Konsultationsprozesses.

(4) Für jedes mögliche Schema setzt die ENISA eine Ad-hoc-Arbeitsgruppe nach Artikel 20 Absatz 4 ein, damit sie der ENISA spezifische Beratung und Sachkenntnis bereitstellt.

(5) Die ENISA arbeitet eng mit der Europäischen Gruppe für die Cybersicherheitszertifizierung zusammen. Die Europäische Gruppe für die Cybersicherheitszertifizierung leistet der ENISA Unterstützung und fachliche Beratung bei der Ausarbeitung des möglichen Schemas und gibt eine Stellungnahme zu dem möglichen Schema ab.

(6) Die ENISA berücksichtigt die Stellungnahme der Europäischen Gruppe für die Cybersicherheitszertifizierung weitestgehend, bevor sie der Kommission das nach den Absätzen 3, 4 und 5 ausgearbeitete mögliche Schema vorlegt. Diese Stellungnahme der Europäischen Gruppe für die Cybersicherheitszertifizierung ist weder bindend, noch hindert das Fehlen einer solchen Stellungnahme die ENISA daran, das mögliche Schema der Kommission vorzulegen.

(7) Auf der Grundlage des von der ENISA ausgearbeiteten möglichen Schemas kann die Kommission Durchführungsrechtsakte erlassen, in denen für IKT-Produkte, -Dienste und -Prozesse, die die Anforderungen der Artikel 51, 52 und 54 erfüllen, ein europäisches Schema

für die Cybersicherheitszertifizierung festgelegt wird. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 66 Absatz 2 genannten Prüfverfahren erlassen.

(8) Die ENISA bewertet mindestens alle fünf Jahre jedes angenommene europäische Schema für die Cybersicherheitszertifizierung, wobei sie die Rückmeldungen seitens der Interessenträger berücksichtigt. Erforderlichenfalls kann die Kommission oder die Europäische Gruppe für die Cybersicherheitszertifizierung die ENISA damit beauftragen, den Prozess der Ausarbeitung eines überarbeiteten möglichen Schemas nach Artikel 48 und nach dem vorliegenden Artikel einzuleiten.

Artikel 50
Website zu europäischen Schemata für die Cybersicherheitszertifizierung

(1) Die ENISA unterhält eine eigene Website, auf der sie über die europäischen Schemata für die Cybersicherheitszertifizierung, die europäischen Cybersicherheitszertifikate und EU-Konformitätserklärungen — was Information in Bezug auf nicht mehr gültige Schemata für die Cybersicherheitszertifizierung und widerrufene und abgelaufene europäische Cybersicherheitszertifikate und EU-Konformitätserklärungen einschließt — und die Ablage für Links zu den Informationen zur Cybersicherheit gemäß Artikel 55 informiert und für diese wirbt.

(2) Gegebenenfalls sollten auf der Website gemäß Absatz 1 auch die nationalen Cybersicherheitszertifizierungsschemata angegeben werden, die durch ein europäisches Schema für die Cybersicherheitszertifizierung ersetzt wurden.

Artikel 51
Sicherheitsziele der europäischen Schemata für die Cybersicherheitszertifizierung

Es wird ein europäisches Schema für die Cybersicherheitszertifizierung konzipiert, um — soweit zutreffend — mindestens die folgenden Sicherheitsziele zu verwirklichen:

a) Gespeicherte, übermittelte oder anderweitig verarbeitete Daten werden während des gesamten Lebenszyklus des IKT-Produkts, -Dienstes oder -Prozesses gegen eine zufällige oder unbefugte Speicherung, Verarbeitung oder Preisgabe sowie gegen einen zufälligen oder unbefugten Zugriff geschützt.

b) Gespeicherte, übermittelte oder anderweitig verarbeitete Daten werden während des gesamten Lebenszyklus des IKT-Produkts, -Dienstes oder -Prozesses vor Zerstörung, Verlust, Änderung oder Nichtverfügbarkeit — gleich, ob sie zufällig oder unbefugt erfolgt sind — geschützt.

c) Befugte Personen, Programme oder Maschinen haben nur Zugriff auf die Daten, Dienste oder Funktionen, zu denen sie zugangsberechtigt sind.

d) Bekannte Abhängigkeiten und Sicherheitslücken werden ermittelt und dokumentiert.

e) Es wird protokolliert, auf welche Daten, Dienste oder Funktionen zu welchem Zeitpunkt von wem zugegriffen wurde und welche Daten, Funktionen oder Dienste zu welchem Zeitpunkt von wem genutzt oder anderweitig verarbeitet worden sind.

f) Es kann überprüft werden, auf welche Daten, Dienste oder Funktionen zu welchem Zeitpunkt und von wem zugegriffen wurde oder wer zu welchem Zeitpunkt Daten, Dienste oder Funktionen genutzt oder anderweitig verarbeitet hat.

g) Es wird nachgeprüft, dass IKT-Produkte, -Dienste und -Prozesse keine bekannten Sicherheitslücken aufweisen.

h) Bei einem physischen oder technischen Sicherheitsvorfall werden die Daten, Dienste und Funktionen zeitnah wieder verfügbar gemacht und der Zugang zu ihnen zeitnah wieder hergestellt.

i) Es wird nachgeprüft, dass IKT-Produkte, -Dienste und -Prozesse sind durch Voreinstellungen und Technikgestaltung sicher sind.

j) IKT-Produkte, -Dienste und -Prozesse werden mit aktueller Software und Hardware, die keine allgemein bekannten Sicherheitslücken aufweisen, bereitgestellt und mit Mechanismen für sichere Updates ausgestattet.

Artikel 52
Vertrauenswürdigkeitsstufen der europäischen Schemata für die Cybersicherheitszertifizierung

(1) Ein europäisches Schema für die Cybersicherheitszertifizierung kann für IKT-Produkte, -Dienste und -Prozesse eine oder mehrere der Vertrauenswürdigkeitsstufen „niedrig", „mittel" und/oder „hoch" angeben. Die Vertrauenswürdigkeitsstufe muss in einem angemessenen Verhältnis zu dem mit der beabsichtigten Verwendung eines IKT-Produkts, -Dienstes oder -Prozesses verbundenen Risiko im Hinblick auf die Wahrscheinlichkeit und die Auswirkungen eines Sicherheitsvorfalls stehen.

(2) Europäische Cybersicherheitszertifikate und EU-Konformitätserklärungen beziehen sich auf die jeweilige Vertrauenswürdigkeitsstufe, die im europäischen Schema für die Cybersicherheitszertifizierung angegeben ist, nach dem das europäische Cybersicherheitszertifikat oder die EU-Konformitätserklärung ausgestellt wurde.

(3) Die jeder Vertrauenswürdigkeitsstufe entsprechenden Sicherheitsanforderungen, einschließlich der entsprechenden Sicherheitsfunktionen und der entsprechenden Strenge und Gründlichkeit für die Bewertung, die das IKT-Produkt, der IKT-Dienst oder der IKT-Prozess durchlaufen muss, werden in dem jeweiligen europäischen Schema für die Cybersicherheitszertifizierung festgelegt.

(4) Das Zertifikat oder die EU-Konformitätserklärung nimmt Bezug auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen, deren Zweck in der Minderung oder Prävention der Gefahr von Cybersicherheitsvorfällen besteht.

(5) Ein europäisches Cybersicherheitszertifikat oder eine EU-Konformitätserklärung für die Vertrauenswürdigkeitsstufe „niedrig" bietet die Gewissheit, dass die IKT-Produkte, -Dienste und -Prozesse, für welche dieses Zertifikat oder diese EU-Konformitätserklärung ausgestellt wird, die entsprechenden Sicherheitsanforderungen einschließlich der Sicherheitsfunktionen erfüllen und einer Bewertung unterzogen wurden, die darauf ausgerichtet ist, die bekannten grundlegenden Risiken für Sicherheitsvorfälle und Cyberangriffe möglichst gering zu halten. Die durchzuführende Bewertung beinhaltet mindestens eine Überprüfung der

technischen Dokumentation. Ist eine solche Prüfung nicht geeignet, werden alternative Prüfungen mit gleicher Wirkung durchgeführt;

(6) Ein europäisches Cybersicherheitszertifikat für die Vertrauenswürdigkeitsstufe „mittel" bietet die Gewissheit, dass die IKT-Produkte, -Dienste und -Prozesse, für welche dieses Zertifikat ausgestellt wird, die entsprechenden Sicherheitsanforderungen einschließlich der Sicherheitsfunktionen erfüllen und einer Bewertung unterzogen wurden, die darauf ausgerichtet ist, bekannte Cybersicherheitsrisiken und das Risiko von Cybersicherheitsvorfällen und Cyberangriffen seitens Akteuren mit begrenzten Fähigkeiten und Ressourcen möglichst gering zu halten. Die durchzuführende Bewertung beinhaltet mindestens Folgendes: eine Überprüfung, die zeigt, dass keine allgemein bekannten Sicherheitslücken vorliegen, und die Prüfung, dass die IKT-Produkte, -Dienste und -Prozesse die erforderlichen Sicherheitsfunktionen korrekt durchführen. Falls diese Bewertungstätigkeiten nicht geeignet sind, werden alternative Tätigkeiten mit gleicher Wirkung durchgeführt;

(7) Ein europäisches Cybersicherheitszertifikat für die Vertrauenswürdigkeitsstufe „hoch" bietet die Gewissheit, dass die IKT-Produkte, -Dienste und -Prozesse, für welche dieses Zertifikat ausgestellt wird, die entsprechenden Sicherheitsanforderungen einschließlich der Sicherheitsfunktionen erfüllen und dass sie einer Bewertung unterzogen wurden, die darauf ausgerichtet ist, das Risiko von dem neuesten Stand der Technik entsprechenden Cyberangriffen durch Akteure mit umfangreichen Fähigkeiten und Ressourcen möglichst gering zu halten. Die durchzuführenden Bewertungstätigkeiten beinhaltet das Folgende; eine Nachprüfung, die zeigt, dass keine allgemein bekannten Sicherheitslücken vorliegen; eine Prüfung, die zeigt, dass die IKT-Produkte, -Dienste und -Prozesse die erforderlichen Sicherheitsfunktionen entsprechend dem neuesten Stand der Technik ordnungsgemäß durchführen, und eine Beurteilung ihrer Widerstandsfähigkeit gegen kompetente Angreifer mittels Penetrationstests Falls diese Bewertungstätigkeiten nicht geeignet sind, alternative Tätigkeiten durchgeführt.

(8) In einem europäischen Schema für die Cybersicherheitszertifizierung können je nach Strenge und Gründlichkeit der verwendeten Evaluierungsmethode mehrere Bewertungsniveaus angegeben werden. Jedes Bewertungsniveau entspricht einer der Vertrauenswürdigkeitsstufen und wird durch eine entsprechende Kombination von Vertrauenswürdigkeitskomponenten definiert.

Artikel 53
Selbstbewertung der Konformität

(1) Ein europäisches Schema für die Cybersicherheitszertifizierung kann die Durchführung einer Selbstbewertung der Konformität unter der alleinigen Verantwortung des Herstellers oder Anbieters von IKT-Produkten, -Diensten und -Prozessen zulassen. Die Selbstbewertung der Konformität ist nur für IKT-Produkte, -Dienste und -Prozesse mit niedrigem Risiko erlaubt, die der Vertrauenswürdigkeitsstufe „niedrig" entsprechen.

(2) Der Hersteller oder Anbieter von IKT-Produkten, -Diensten und -Prozessen kann eine EU-Konformitätserklärung ausstellen, die bestätigt, dass die Erfüllung der im Schema festgelegten Anforderungen nachgewiesen wurde. Durch die Ausstellung einer solchen Erklärung übernimmt der Hersteller oder Anbieter der IKT-Produkte, -Dienste und -Prozesse die Verantwortung dafür, dass das IKT-Produkt, der IKT-Dienst oder der IKT-Prozess den in diesem Schema festgelegten Anforderungen entspricht.

(3) Der Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen hält die EU-Konformitätserklärung, die technische Dokumentation und alle weiteren einschlägigen Informationen in Bezug auf die Konformität der IKT-Produkte oder -Dienste mit dem Schema während eines Zeitraums, der im entsprechenden europäischen Schema für die Cybersicherheitszertifizierung festgelegt ist, für die in Artikel 58 genannte nationale Behörde für die Cybersicherheitszertifizierung bereit. Eine Kopie der EU-Konformitätserklärung ist der nationalen Behörde für die Cybersicherheitszertifizierung und der ENISA vorzulegen.

(4) Sofern im Unionsrecht oder im Recht der Mitgliedstaaten nicht anders bestimmt, ist die Ausstellung einer EU-Konformitätserklärung freiwillig.

(5) Die ausgestellte EU-Konformitätserklärung wird in allen Mitgliedstaaten anerkannt.

Artikel 54
Elemente der europäischen Schemata für die Cybersicherheitszertifizierung

(1) Ein europäisches Schema für die Cybersicherheitszertifizierung muss mindestens folgende Elemente enthalten:

a) den Gegenstand und Umfang des Zertifizierungsschemas, einschließlich der Art oder Kategorie der erfassten IKT-Produkte, -Dienste und -Prozesse;

b) eine eindeutige Beschreibung des Zwecks des Schemas und der Art und Weise, wie die ausgewählten Normen, Bewertungsmethoden und Vertrauenswürdigkeitsstufen mit den Erfordernissen der vorgesehenen Nutzer des Schemas in Einklang gebracht wurden;

c) eine Bezugnahme auf die für die Bewertung maßgeblichen internationalen, europäischen oder nationalen Normen oder, wenn keine solchen Normen verfügbar oder geeignet sind, auf technische Spezifikationen, die die Auflagen des Anhangs II der Verordnung (EU) Nr. 1025/2012 erfüllen, oder — wenn solche Spezifikationen nicht verfügbar sind — auf die im europäischen Schema für die Cybersicherheitszertifizierung festgelegten technischen Spezifikationen oder Cybersicherheitsanforderungen;

d) gegebenenfalls eine oder mehrere Vertrauenswürdigkeitsstufen;

e) die Angabe, ob eine Selbstbewertung der Konformität im Rahmen des Schemas zulässig ist;

f) falls anwendbar, spezielle oder zusätzliche Anforderungen an die Konformitätsbewertungsstellen, um deren technische Kompetenz für die Evaluierung der Cybersicherheitsanforderungen zu gewährleisten;

g) besondere Bewertungskriterien und -methoden — wie auch Bewertungsarten — für den Nachweis, dass die in Artikel 51 festgelegten Sicherheitsziele eingehalten werden;

h) falls anwendbar, für die Zertifizierung erforderliche Informationen, die ein Antragsteller der Konformitätsbewertungsstelle vorzulegen oder auf andere Weise zur Verfügung zu stellen hat;

i) Bedingungen für die Verwendung von Siegeln oder Kennzeichen, sofern das Schema solche vorsieht;

j) Vorschriften für die Überwachung der Einhaltung der mit dem europäischen Cybersicherheitszertifikat oder der EU-Konformitätserklärung verbundenen Anforderungen an IKT-Produkte, -Dienste und -Prozesse, einschließlich der Mechanismen für den Nachweis der beständigen Einhaltung der festgelegten Cybersicherheitsanforderungen;

k) falls anwendbar, Bedingungen für die Ausstellung, Aufrechterhaltung, Fortführung und Verlängerung eines europäischen Cybersicherheitszertifikats sowie Bedingungen für die Ausweitung oder Verringerung des Zertifizierungsumfangs;

l) Vorschriften, wie mit IKT-Produkten, -Diensten und -Prozessen zu verfahren ist, die zertifiziert wurden oder für die eine EU-Konformitätserklärung ausgestellt wurde, die aber den Anforderungen des Schemas nicht genügen;

m) Vorschriften für die Meldung und Behandlung bislang nicht erkannter Cybersicherheitslücken von IKT-Produkten und -Diensten und -Prozessen;

n) falls anwendbar, Vorschriften für die Konformitätsbewertungsstellen über die Aufbewahrung von Aufzeichnungen;

o) Angabe nationaler oder internationaler Schemata für die Cybersicherheitszertifizierung für dieselbe Art oder Kategorie von IKT-Produkten, -Diensten und -Prozessen, Sicherheitsanforderungen, Evaluierungskriterien und -methoden und Vertrauenswürdigkeitsstufen;

p) Inhalt und Format des europäischen Cybersicherheitszertifikats oder der EU-Konformitätserklärungen, die auszustellen sind;

q) die Dauer der Verfügbarkeit der EU-Konformitätserklärung, der technischen Dokumentation und aller weiteren bereitzuhaltenden Informationen des Herstellers oder Anbieters von IKT-Produkten, -Diensten und -Prozessen;

r) die maximale Gültigkeitsdauer der nach diesem Schema ausgestellten europäischen Cybersicherheitszertifikate;

s) eine Offenlegungspolitik für nach diesem Schema ausgestellte, geänderte oder entzogene europäische Cybersicherheitszertifikate;

t) Bedingungen für die auf Gegenseitigkeit beruhende Anerkennung von Zertifizierungsschemata von Drittländern;

u) falls anwendbar, Regeln für etwaige im Schema vorgesehene Verfahren zur gegenseitigen Begutachtung für die Behörden oder Stellen, die im Einklang mit Artikel 56 Absatz 6 europäische Cybersicherheitszertifikate für die Vertrauenswürdigkeitsstufe „hoch“ ausstellen. Diese Verfahren gelten unbeschadet der gegenseitigen Begutachtung gemäß Artikel 59;

v) Format und Verfahren, die von den Herstellern oder Anbietern von IKT-Produkten, -Diensten und -Prozessen bei der Bereitstellung und Aktualisierung der ergänzenden Informationen zur Cybersicherheit gemäß Artikel 55 zu befolgen sind.

(2) Die für das europäische Schema für die Cybersicherheitszertifizierung festgelegten Anforderungen stehen in Einklang mit allen geltenden rechtlichen Anforderungen, vor allem jenen, die sich aus dem harmonisierten Unionsrecht ergeben.

(3) Soweit dies in einem bestimmten Rechtsakt der Union so festgelegt ist, kann eine Zertifizierung oder eine EU-Konformitätserklärung, die auf der Grundlage eines europäischen Schemas für die Cybersicherheitszertifizierung ausgestellt wurde, dafür verwendet werden kann, die Vermutung zu begründen, dass eine Übereinstimmung mit den Anforderungen jenes Rechtsakts gegeben ist.

(4) Fehlt harmonisiertes Unionsrecht, so kann das Recht der Mitgliedstaaten auch festlegen, dass ein europäisches Schema für die Cybersicherheitszertifizierung dafür verwendet werden kann, die Vermutung zu begründen, dass eine Übereinstimmung mit den gesetzlichen Anforderungen gegeben ist.

Artikel 55
Ergänzende Informationen über die Cybersicherheit von zertifizierten IKT-Produkten, -Diensten und -Prozessen

(1) Hersteller oder Anbieter von zertifizierten IKT-Produkten, -Diensten oder -Prozessen oder von IKT-Produkten, -Diensten und -Prozessen, für die eine EU-Konformitätserklärung ausgestellt wurde, machen folgende ergänzende Cybersicherheitsangaben der Öffentlichkeit zugänglich:

a) Leitlinien und Empfehlungen zur Unterstützung der Endnutzer bei der sicheren Konfiguration, der Installation, der Bereitstellung, dem Betrieb und der Wartung der IKT-Produkte oder -Dienste;

b) Zeitraum, während dessen den Endnutzern eine Sicherheitsunterstützung angeboten wird, insbesondere in Bezug auf die Verfügbarkeit von cybersicherheitsbezogenen Aktualisierungen;

c) Kontaktangaben des Herstellers oder Anbieters und zulässige Verfahren für den Erhalt von Informationen über Sicherheitslücken von Endnutzern und im Bereich der IT-Sicherheit tätigen Wissenschaftlern;

d) Verweis auf Online-Register mit öffentlich offengelegten Sicherheitslücken in Bezug auf das IKT-Produkt, den IKT-Dienst oder den IKT-Prozess und gegebenenfalls relevante Cybersicherheitsratgeber.

(2) Die in Absatz 1 aufgeführten Angaben werden in elektronischer Form bereitgestellt und bleiben mindestens bis zum Ablauf des jeweiligen EU-Cybersicherheitszertifikats oder der EU-Konformitätserklärung verfügbar und werden bei Bedarf aktualisiert.

Artikel 56
Cybersicherheitszertifizierung

(1) Für IKT-Produkte, -Dienste, und -Prozesse die auf der Grundlage eines nach Artikel 49 angenommenen europäischen Schemas für die Cybersicherheitszertifizierung zertifiziert wurden, gilt die Vermutung der Einhaltung der Anforderungen dieses Schemas.

(2) Sofern im Unionsrecht oder im Recht der Mitgliedstaaten nicht anders bestimmt, ist die Cybersicherheitszertifizierung freiwillig.

(3) Die Kommission bewertet regelmäßig die Effizienz und Nutzung der angenommenen europäischen Cybersicherheitszertifizierungsschemata sowie die Frage, ob ein bestimmtes europäisches Cybersicherheitszertifizierungsschema durch das einschlägige Unionsrecht verbindlich vorgeschrieben werden soll, um ein angemessenes Maß an Cybersicherheit von

IKT-Produkten, -Diensten und -Prozessen in der Union sicherzustellen und das Funktionieren des Binnenmarktes zu verbessern. Die erste Bewertung findet bis zum 31. Dezember 2023 statt und danach nachfolgende Bewertungen finden mindestens alle zwei Jahre statt.

Die Kommission stellt auf der Grundlage der Ergebnisse der Bewertung fest, welche IKT-Produkte, -Dienste und -Prozesse, die unter ein bestehendes Zertifizierungsschema fallen, unter ein verpflichtendes Zertifizierungsschema fallen müssen.

Die Kommission konzentriert sich dabei vorrangig auf die Sektoren, die in Anhang II der Richtlinie (EU) 2016/1148 aufgeführt sind und die spätestens zwei Jahre nach der Annahme des ersten europäischen Cybersicherheitszertifizierungsschemas bewertet werden.

Bei der Vorbereitung der Bewertung verfährt die Kommission wie folgt:

a) Sie berücksichtigt die Auswirkungen der Maßnahmen auf die Hersteller oder Anbieter solcher IKT-Produkte, -Dienste und -Prozesse und auf die Nutzer hinsichtlich der Kosten dieser Maßnahmen und des gesellschaftlichen oder wirtschaftlichen Nutzens, der sich aus dem erwarteten höheren Maß an Sicherheit für die betreffenden IKT-Produkte, -Dienste und -Prozesse ergibt;

b) sie berücksichtigt das Bestehen und die Umsetzung von Rechtsvorschriften der Mitgliedstaaten und von Drittländern;

c) sie führt eine offene, transparente und inklusive Konsultation mit allen relevanten Interessenträgern und mit den Mitgliedstaaten durch;

d) sie berücksichtigt die Umsetzungsfristen sowie die Übergangsmaßnahmen oder -zeiträume und insbesondere in Hinblick auf die möglichen Auswirkungen der Maßnahme auf die Anbieter oder Hersteller von IKT-Produkten, -Diensten und -Prozessen, einschließlich KMU;

e) sie schlägt die schnellste und effizienteste Art und Weise für die Durchführung des Übergangs von freiwilligen zu obligatorischen Zertifizierungsschemata vor.

(4) Die in Artikel 60 genannten Konformitätsbewertungsstellen stellen ein europäisches Cybersicherheitszertifikat nach diesem Artikel mit der Vertrauenswürdigkeitsstufe „niedrig“ oder „mittel“ auf der Grundlage der Kriterien des nach Artikel 49 durch die Kommission angenommenen europäischen Schemas für die Cybersicherheitszertifizierung aus.

(5) Abweichend von Absatz 4 kann in hinreichend begründeten Fällen ein europäisches Schema für die Cybersicherheitszertifizierung vorsehen, dass ein im Rahmen dieses Schemas erteiltes europäisches Cybersicherheitszertifikat nur von einer öffentlichen Stelle auszustellen ist. Bei einer solchen Stelle muss es sich um eine der folgenden Stellen handeln:

a) eine nationale Behörde für die Cybersicherheitszertifizierung nach Artikel 58 Absatz 1;

b) eine als Konformitätsbewertungsstelle akkreditierte öffentliche Stelle nach Artikel 60 Absatz 1.

(6) Ist im Rahmen eines europäischen Schemas für die Cybersicherheitszertifizierung nach Artikel 49 die Vertrauenswürdigkeitsstufe „hoch“ erforderlich, so kann das europäische Cybersicherheitszertifikat nach diesem Schema nur von einer nationalen Behörde für die Cybersicherheitszertifizierung oder in den folgenden Fällen von einer Konformitätsbewertungsstelle ausgestellt werden:

a) wenn die nationale Behörde für die Cybersicherheitszertifizierung zuvor für jedes einzelne, von einer Konformitätsbewertungsstelle ausgestellte europäische Cybersicherheitszertifikat ihre Zustimmung erteilt hat oder

b) wenn die nationale Behörde für die Cybersicherheitszertifizierung die Aufgabe der Ausstellung solcher europäischen Cybersicherheitszertifikate zuvor allgemein einer Konformitätsbewertungsstelle übertragen hat.

(7) Die natürliche oder juristische Person, die ihre IKT-Produkte, -Dienste oder -Prozesse zur Zertifizierung einreicht, hat der in Artikel 58 genannten nationalen Behörde für die Cybersicherheitszertifizierung — sofern diese Behörde die Stelle ist, die das europäische Cybersicherheitszertifikat erteilt — oder der in Artikel 60 genannten Konformitätsbewertungsstelle alle für das Zertifizierungsverfahren notwendigen Informationen vorzulegen.

(8) Der Inhaber eines europäischen Cybersicherheitszertifikats informiert die in Absatz 7 genannte Behörde oder Stelle über etwaige später festgestellte Sicherheitslücken oder Unregelmäßigkeiten hinsichtlich der Sicherheit des zertifizierten IKT-Produkts, -Dienstes oder -Prozesses, die sich auf die mit der Zertifizierung verbundenen Anforderungen auswirken könnten. Die Behörde oder Stelle leitet diese Informationen unverzüglich an die betreffende nationale Behörde für die Cybersicherheitszertifizierung weiter.

(9) Ein europäisches Cybersicherheitszertifikat wird für die im jeweiligen europäischen Zertifizierungsschema für Cybersicherheit festgelegte Dauer erteilt und kann verlängert werden, sofern die einschlägigen Voraussetzungen weiterhin erfüllt sind.

(10) Ein nach diesem Artikel ausgestelltes europäisches Cybersicherheitszertifikat wird in allen Mitgliedstaaten anerkannt.

Artikel 57
Nationale Cybersicherheitszertifizierungsschemata und Cybersicherheitszertifikate

(1) Unbeschadet des Absatzes 3 dieses Artikels werden nationale Schemata für die Cybersicherheitszertifizierung und die zugehörigen Verfahren für die IKT-Produkte, -Dienste und -Prozesse, die unter ein europäisches Schema für die Cybersicherheitszertifizierung fallen, ab dem Zeitpunkt unwirksam, der in dem nach Artikel 49 Absatz 7 erlassenen Durchführungsrechtsakt festgelegt ist. Nationale Schemata für die Cybersicherheitszertifizierung und die zugehörigen Verfahren für die IKT-Produkte, -Dienste und-Prozesse, die nicht unter ein europäisches Schema für die Cybersicherheitszertifizierung fallen, bleiben bestehen.

(2) Die Mitgliedstaaten führen keine neuen nationalen Schemata für die Cybersicherheitszertifizierung von IKT-Produkten, -Diensten und -Prozessen ein, die unter ein geltendes europäisches Schema für die Cybersicherheitszertifizierung fallen.

(3) Vorhandene Zertifikate, die auf der Grundlage nationaler Schemata für die Cybersicherheitszertifizierung ausgestellt wurden und unter ein europäisches Schema für die Cybersicherheitszertifizierung fallen, bleiben bis zum Ende ihrer Geltungsdauer gültig.

(4) Um die Fragmentierung des Binnenmarkts zu vermeiden, unterrichten die Mitgliedstaaten die Kommission und die Europäische Gruppe für die Cybersicherheitszertifizierung über die Absicht zur Ausarbeitung neuer nationaler Schemata für die Cybersicherheitszertifizierung.

Artikel 58
Nationale Behörden für die Cybersicherheitszertifizierung

(1) Jeder Mitgliedstaat benennt eine oder mehrere nationale Behörden für die Cybersicherheitszertifizierung in seinem Hoheitsgebiet oder im Einverständnis mit einem anderen Mitgliedstaat eine oder mehrere nationale Behörden für die Cybersicherheitszertifizierung mit Sitz in diesem anderen Mitgliedstaat, als für die Aufsichtsaufgaben im benennenden Mitgliedstaat zuständig.

(2) Jeder Mitgliedstaat teilt der Kommission den Namen der benannten nationalen Behörden für Cybersicherheitszertifizierung mit. Sofern ein Mitgliedstaat mehr als eine Behörde benennt, teilt er der Kommission auch die Aufgaben mit, die diesen Behörden jeweils zugewiesen wurden.

(3) Unbeschadet des Artikels 56 Absatz 5 Buchstabe a und Absatz 6 ist jede nationale Behörde für die Cybersicherheitszertifizierung im Hinblick auf ihre Organisation, Finanzierungsentscheidungen, Rechtsform und Entscheidungsfindung unabhängig von den Stellen, die sie beaufsichtigt.

(4) Die Mitgliedstaaten stellen sicher, dass die Tätigkeiten der nationalen Behörden für die europäische Cybersicherheitszertifizierung im Zusammenhang mit der Ausstellung von Zertifikaten nach Artikel 56 Absatz 5 Buchstabe a und Absatz 6 von den Aufsichtstätigkeiten nach diesem Artikel streng getrennt sind und dass diese Tätigkeiten unabhängig voneinander durchgeführt werden.

(5) Die Mitgliedstaaten stellen sicher, dass die nationalen Behörden für die Cybersicherheitszertifizierung eine angemessene Ausstattung zur Ausübung ihrer Befugnisse und zur wirksamen und effizienten Wahrnehmung ihrer Aufgaben besitzen.

(6) Im Hinblick auf eine wirksame Durchführung dieser Verordnung ist es angemessen, dass die nationalen Behörden für die Cybersicherheitszertifizierung in der Europäischen Gruppe für die Cybersicherheitszertifizierung in aktiver, wirksamer, effizienter und sicherer Weise mitarbeiten.

(7) Die nationalen Behörden für die Cybersicherheitszertifizierung haben folgende Aufgaben:

a) Überwachung und Durchsetzung der Vorschriften im Rahmen der europäischen Schemata für die Cybersicherheitszertifizierung gemäß Artikel 54 Absatz 1 Buchstabe j im Hinblick auf die Beobachtung der Übereinstimmung der IKT-Produkte, -Dienste und -Prozesse mit den Anforderungen der in ihrem jeweiligen Hoheitsgebiet ausgestellten europäischen Cybersicherheitszertifikate in Zusammenarbeit mit anderen zuständigen Marktüberwachungsbehörden;

b) Überwachung und Durchsetzung der Verpflichtungen der in ihrem jeweiligen Hoheitsgebiet niedergelassenen Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen, die eine Selbstbewertung der Konformität durchführen, insbesondere Überwachung und Durchsetzung der Verpflichtungen dieser Hersteller oder Anbieter nach Artikel 53 Absätze 2 und 3 und nach dem entsprechenden europäischen Schema für die Cybersicherheitszertifizierung;

c) unbeschadet des Artikels 60 Absatz 3 aktive Unterstützung der nationalen Akkreditierungsstellen bei der Überwachung und Beaufsichtigung der Tätigkeiten der Konformitätsbewertungsstellen für die Zwecke dieser Verordnung;

d) Überwachung und Beaufsichtigung der Tätigkeiten der in Artikel 56 Absatz 5 genannten öffentlichen Stellen;

e) gegebenenfalls Ermächtigung der Konformitätsbewertungsstellen nach Artikel 60 Absatz 3 und Beschränkung, Aussetzung oder Widerruf bestehender Ermächtigungen, wenn die Konformitätsbewertungsstellen gegen die Anforderungen dieser Verordnung verstoßen;

f) Bearbeitung von Beschwerden, die von natürlichen oder juristischen Personen in Bezug auf europäische Cybersicherheitszertifikate, die von der nationalen Behörde für die Cybersicherheitszertifizierung ausgestellt wurden, oder in Bezug auf europäische Cybersicherheitszertifikate, die nach Artikel 56 Absatz 6 von Konformitätsbewertungsstellen ausgestellt wurden, oder in Bezug auf EU-Konformitätserklärungen nach Artikel 53 eingereicht werden, und Untersuchung des Beschwerdegegenstands in angemessenem Umfang, und Unterrichtung des Beschwerdeführers über die Fortschritte und das Ergebnis der Untersuchung innerhalb einer angemessenen Frist;

g) Vorlage eines zusammenfassenden Jahresberichts über die ausgeführten Tätigkeiten gemäß den Buchstaben b, c und d dieses Absatzes oder gemäß Absatz 8 an die ENISA und die Europäische Gruppe für die Cybersicherheitszertifizierung;

h) Zusammenarbeit mit anderen nationalen Behörden für die Cybersicherheitszertifizierung und anderen öffentlichen Stellen; dies beinhaltet auch den Informationsaustausch über die etwaige Nichtkonformität von IKT-Produkten, -Diensten und -Prozessen mit den Anforderungen dieser Verordnung oder mit den Anforderungen bestimmter europäischer Schemata für die Cybersicherheitszertifizierung; und

i) Verfolgung einschlägiger Entwicklungen auf dem Gebiet der Cybersicherheitszertifizierung.

(8) Jede nationale Behörde für die Cybersicherheitszertifizierung hat mindestens die folgenden Befugnisse:

a) Sie kann die Konformitätsbewertungsstellen, die Inhaber europäischer Cybersicherheitszertifikate und die Aussteller von EU-Konformitätserklärungen auffordern, ihr sämtliche Auskünfte zu erteilen, die sie für die Erfüllung ihrer Aufgaben benötigt;

b) sie kann Untersuchungen in Form von Rechnungsprüfungen bei den Konformitätsbewertungsstellen, den Inhabern europäischer Cybersicherheitszertifikate und den Ausstellern von EU-Konformitätserklärungen durchführen, um deren Einhaltung der Bestimmungen dieses Titels zu überprüfen;

c) sie kann im Einklang mit dem nationalen Recht geeignete Maßnahmen ergreifen, um sicherzustellen, dass die Konformitätsbewertungsstellen, die Inhaber von europäischen Cybersicherheitszertifikaten und die Aussteller von EU-Konformitätserklärungen den Anforderungen dieser Verordnung oder eines europäischen Schemas für die Cybersicherheitszertifizierung genügen;

d) sie erhält Zugang zu den Räumlichkeiten von Konformitätsbewertungsstellen und von Inhabern europäischer Cybersicherheitszertifikate zum Zweck der Durchführung von Untersuchungen im Einklang mit den Verfahrensvorschriften der Union oder des Mitgliedstaats;

e) sie kann im Einklang mit dem nationalen Recht europäische Cybersicherheitszertifikate widerrufen, die von den nationalen Behörden für die Cybersicherheitszertifizierung oder europäische Cybersicherheitszertifikate, die nach Artikel 56 Absatz 6 von den Konformitätsbewertungsstellen ausgestellt wurden, wenn diese Zertifikate den Anforderungen dieser Verordnung oder eines europäischen Schemas für die Cybersicherheitszertifizierung nicht genügen;

f) sie kann im Einklang mit dem nationalen Recht Sanktionen nach Artikel 65 verhängen und die unverzügliche Beendigung von Verstößen gegen die in dieser Verordnung festgelegten Verpflichtungen anordnen.

(9) Die nationalen Behörden für die Cybersicherheitszertifizierung arbeiten untereinander und mit der Kommission zusammen, indem sie insbesondere Informationen, Erfahrungen und bewährte Verfahren im Zusammenhang mit der Cybersicherheitszertifizierung und technischen Fragen in Bezug auf die Cybersicherheit von IKT-Produkten -Diensten und -Prozessen austauschen.

Artikel 59
Gegenseitige Begutachtung

(1) Um in der gesamten Union gleichwertige Standards in Bezug auf die europäischen Cybersicherheitszertifikate und EU-Konformitätserklärungen zu erreichen, unterliegen die nationalen Behörden für die Cybersicherheitszertifizierung einer gegenseitigen Begutachtung.

(2) Die gegenseitige Begutachtung erfolgt auf der Grundlage fundierter und transparenter Bewertungskriterien und -verfahren und erstreckt sich insbesondere auf die Strukturen, Personalressourcen und Verfahren betreffenden Anforderungen sowie auf Vertraulichkeit und Beschwerden.

(3) Die gegenseitige Begutachtung umfasst die Bewertung folgender Aspekte:

a) gegebenenfalls die Frage, ob bei den Tätigkeiten der nationalen Behörden für die europäische Cybersicherheitszertifizierung im Zusammenhang mit der Ausstellung von Zertifikaten nach Artikel 56 Absatz 5 Buchstabe a und Absatz 6 eine strenge Trennung der Aufgaben und Zuständigkeiten von den Aufsichtstätigkeiten nach Artikel 58 gewahrt wird und beide Tätigkeiten unabhängig voneinander durchgeführt werden;

b) die Verfahren für die Überwachung und Durchsetzung der Vorschriften für die Beobachtung der Übereinstimmung von IKT-Produkten, -Diensten und -Prozessen mit den europäischen Cybersicherheitszertifikaten nach Artikel 58 Absatz 7 Buchstabe a;

c) die Verfahren für die Überwachung und Durchsetzung der Verpflichtungen der Hersteller und Anbieter von IKT-Produkten -Diensten oder -Prozessen nach Artikel 58 Absatz 7 Buchstabe b;

d) die Verfahren für die Überwachung, Genehmigung und Beaufsichtigung der Tätigkeiten der Konformitätsbewertungsstellen;

e) gegebenenfalls die Frage, ob das Personal von Behörden oder Stellen, die gemäß Artikel 56 Absatz 6 Zertifikate für die Vertrauenswürdigkeitsstufe „hoch“ ausstellen, über die erforderlichen Sachkenntnisse verfügt.

(4) Die gegenseitige Begutachtung erfolgt durch mindestens zwei nationale Behörden für die Cybersicherheitszertifizierung anderer Mitgliedstaaten und die Kommission, und sie wird mindestens einmal alle fünf Jahre durchgeführt. Die ENISA kann sich an der gegenseitigen Begutachtung beteiligen.

(5) Die Kommission kann Durchführungsrechtsakte erlassen, um einen Plan für die gegenseitige Begutachtung festzulegen, der sich auf einen Zeitraum von mindestens fünf Jahren erstreckt, und darin die Kriterien für die Zusammensetzung des die gegenseitige Begutachtung durchführenden Teams, die Methode für die gegenseitige Begutachtung und den Zeitplan, die Häufigkeit und die übrigen damit verbundenen Aufgaben vorzugeben. Beim Erlass dieser Durchführungsrechtsakte trägt die Kommission den Erwägungen der Europäischen Gruppe für die Cybersicherheitszertifizierung angemessen Rechnung. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 66 Absatz 2 genannten Prüfverfahren erlassen.

(6) Die Europäische Gruppe für die Cybersicherheitszertifizierung prüft die Ergebnisse der gegenseitigen Begutachtung, erstellt eine Zusammenfassung, die der Öffentlichkeit zugänglich gemacht werden kann, und erlässt erforderlichenfalls Leitlinien oder Empfehlungen zu den von den betreffenden Stellen zu ergreifenden Maßnahmen.

Artikel 60
Konformitätsbewertungsstellen

(1) Die Konformitätsbewertungsstellen werden von den nach der Verordnung (EG) Nr. 765/2008 benannten nationalen Akkreditierungsstellen akkreditiert. Diese Akkreditierung wird nur ausgestellt, wenn die Konformitätsbewertungsstelle die im Anhang der vorliegenden Verordnung aufgeführten Anforderungen erfüllt.

(2) Hat eine nationale Behörde für die Cybersicherheitszertifizierung nach Artikel 56 Absatz 5 Buchstabe a und Absatz 6 ein europäisches Cybersicherheitszertifikat ausstellt, so wird die Zertifizierungsstelle der nationalen Behörde für die Cybersicherheitszertifizierung nach Absatz 1 des vorliegenden Artikels als Konformitätsbewertungsstelle akkreditiert.

(3) Sind in einem europäischen Schema für die Cybersicherheitszertifizierung spezifische oder zusätzliche Anforderungen gemäß Artikel 54 Absatz 1 Buchstabe f festgelegt, so darf nur solchen Konformitätsbewertungsstellen von der nationalen Behörde für die Cybersicherheitszertifizierung die Befugnis erteilt werden, Aufgaben im Rahmen dieses Schemas wahrzunehmen, die diese Anforderungen einhalten.

(4) Die Akkreditierung nach Absatz 1wird den Konformitätsbewertungsstellen für eine Höchstdauer von fünf Jahren erteilt und kann unter denselben Bedingungen verlängert werden, sofern die Konformitätsbewertungsstelle die Anforderungen dieses Artikels weiterhin erfüllt. Die nationalen Akkreditierungsstellen treffen innerhalb einer angemessenen Frist alle angebrachten Maßnahmen, um die nach Absatz 1 erteilte Akkreditierung einer Konformitätsbewertungsstelle zu beschränken, auszusetzen oder zu widerrufen, wenn die Voraussetzungen für die Akkreditierung nicht oder nicht mehr erfüllt sind oder wenn die Konformitätsbewertungsstelle gegen diese Verordnung verstößt.

Artikel 61
Notifikation

(1) Für jedes europäische Schema für die Cybersicherheitszertifizierung notifizieren die nationalen Behörden für die Cybersicherheitszertifizierung der Kommission die Konformitäts-

bewertungsstellen, die für die Erteilung von Zertifikaten entsprechend den in Artikel 52 genannten Vertrauenswürdigkeitsstufen akkreditiert und gegebenenfalls nach Artikel 60 Absatz 3 ermächtigt wurden. Die nationalen Behörden für die Cybersicherheitszertifizierung teilt der Kommission etwaige diesbezügliche Änderungen unverzüglich mit.

(2) Ein Jahr nach Inkrafttreten eines europäischen Schemas für die Cybersicherheitszertifizierung veröffentlicht die Kommission im Amtsblatt der Europäischen Union eine Liste der nach diesem Schema notifizierten Konformitätsbewertungsstellen.

(3) Geht der Kommission nach Ablauf der in Absatz 2 genannten Frist eine Notifikation zu, so veröffentlicht sie die Änderungen der Liste der notifizierten Konformitätsbewertungsstellen innerhalb von zwei Monaten ab dem Zeitpunkt des Eingangs dieser Notifikation im Amtsblatt der Europäischen Union.

(4) Eine nationale Behörde für die Cybersicherheitszertifizierung kann bei der Kommission die Streichung einer von dieser Behörde notifizierten Konformitätsbewertungsstelle aus der in Absatz 2 genannten Liste beantragen. Die Kommission veröffentlicht die entsprechenden Änderungen der Liste innerhalb eines Monats ab dem Zeitpunkt, zu dem der Antrag der nationalen Behörde für die Cybersicherheitszertifizierung eingegangen ist, im Amtsblatt der Europäischen Union.

(5) Die Kommission kann im Wege von Durchführungsrechtsakten Einzelheiten, Form und Verfahren für die Notifikationen nach Absatz 1 festlegen. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 66 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 62
Europäische Gruppe für die Cybersicherheitszertifizierung

(1) Die Europäische Gruppe für die Cybersicherheitszertifizierung wird eingesetzt.

(2) Die Europäische Gruppe für die Cybersicherheitszertifizierung setzt sich aus Vertretern der nationalen Behörden für die Cybersicherheitszertifizierung oder Vertretern anderer einschlägiger nationaler Behörden zusammen. Ein Mitglied der Europäischen Gruppe für die Cybersicherheitszertifizierung darf nicht mehr als zwei Mitgliedstaat vertreten.

(3) Interessenträger und maßgebliche Dritte können zur Teilnahme an den Sitzungen der Europäischen Gruppe für die Cybersicherheitszertifizierung und zur Beteiligung an ihrer Arbeit eingeladen werden.

(4) Die Europäische Gruppe für die Cybersicherheitszertifizierung hat folgende Aufgaben:

a) Sie berät und unterstützt die Kommission bei ihren Tätigkeiten zur Gewährleistung einer einheitlichen Umsetzung und Anwendung dieses Titels — insbesondere in Bezug auf das fortlaufende Arbeitsprogramm der Union — in politischen Fragen der Cybersicherheitszertifizierung, bei der Koordinierung von Politikkonzepten und bei der Ausarbeitung europäischer Schemata für die Cybersicherheitszertifizierung;

b) sie unterstützt und berät die ENISA bei der Ausarbeitung eines möglichen Schemas nach Artikel 49 und arbeitet hierbei mit der ENISA zusammen;

c) sie gibt nach Artikel 49 eine Stellungnahme zu den von der ENISA vorbereiteten möglichen Schemata ab;

d) sie beauftragt die ENISA mit der Ausarbeitung von möglichen Schemata nach Artikel 48 Absatz 2;

e) sie gibt an die Kommission gerichtete Stellungnahmen zur Pflege und Überprüfung vorhandener europäischer Schemata für die Cybersicherheitszertifizierung ab;

f) sie prüft die einschlägigen Entwicklungen auf dem Gebiet der Cybersicherheitszertifizierung und tauscht Informationen über und bewährte Verfahren für Cybersicherheitszertifizierungsschemata aus;

g) sie erleichtert die Zusammenarbeit zwischen den nationalen Behörden für die Cybersicherheitszertifizierung nach diesem Titel im Wege des Kapazitätsaufbaus und des Informationsaustauschs, insbesondere durch die Festlegung von Methoden für einen effizienten Austausch von Informationen über Fragen der Cybersicherheitszertifizierung;

h) sie leistet Unterstützung bei der Anwendung des Mechanismus der gegenseitigen Begutachtung gemäß den Regeln, die in einem europäischen Cybersicherheitszertifizierungsschema nach Artikel 54 Absatz 1 Buchstabe u festgelegt wurden;

i) sie erleichtert die Anpassung europäischer Schemata für die Cybersicherheitszertifizierung an international anerkannte Normen, indem sie unter anderem bestehende europäische Schemata für die Cybersicherheitszertifizierung überprüft und der ENISA erforderlichenfalls Empfehlungen unterbreitet, sich mit den einschlägigen internationalen Normungsorganisationen in Verbindung zu setzen, um Unzulänglichkeiten oder Lücken in verfügbaren international anerkannten Normen anzugehen.

(5) Die Kommission nimmt gemäß Artikel 8 Absatz 1 Buchstabe e die Sekretariatsgeschäfte der Europäischen Gruppe für die Cybersicherheitszertifizierung wahr, und führt mit Unterstützung der ENISA ihren Vorsitz.

Artikel 63
Beschwerderecht

(1) Natürliche und juristische Personen haben das Recht, bei dem Aussteller eines europäischen Cybersicherheitszertifikats oder — wenn sich die Beschwerde gegen ein von einer Konformitätsbewertungsstelle nach Artikel 56 Absatz 6 ausgestelltes europäischen Cybersicherheitszertifikat richtet — bei der zuständigen nationalen Behörde für die Cybersicherheitszertifizierung eine Beschwerde einzulegen.

(2) Die Behörde oder Stelle, bei der die Beschwerde eingelegt wurde, unterrichtet den Beschwerdeführer über den Stand des Verfahrens und die getroffene Entscheidung und informiert den Beschwerdeführer über die Möglichkeit eines wirksamen gerichtlichen Rechtsbehelfs nach Artikel 64.

Artikel 64
Recht auf einen wirksamen gerichtlichen Rechtsbehelf

(1) Jede natürliche oder juristische Person hat unbeschadet eines anderweitigen verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs das Recht auf einen wirksamen gerichtlichen Rechtsbehelf in Bezug auf

a) Entscheidungen einer Behörde oder einer Stelle gemäß Artikel 63 Absatz 1, gegebenenfalls auch in Bezug auf die mangelnde Erteilung, Verweigerung der Erteilung oder Anerkennung eines europäischen Cybersicherheitszertifikats, das diese natürliche oder juristische Person innehat bzw. beantragt hat;

b) Untätigkeit im Anschluss an eine Beschwerde bei einer Behörde oder Stelle gemäß Artikel 63 Absatz 1.

(2) Verfahren nach diesem Artikel werden bei den Gerichten des Mitgliedstaats eingeleitet, in dem die Behörde oder Stelle, gegen die der Rechtsbehelf gerichtet ist, ihren Sitz hat.

Artikel 65
Sanktionen

Die Mitgliedstaaten erlassen Vorschriften über Sanktionen, die bei Verstößen gegen diesen Titel und bei Verstößen gegen die europäischen Schemata für die Cybersicherheitszertifizierung zu verhängen sind, und treffen alle für die Anwendung der Sanktionen erforderlichen Maßnahmen. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen unverzüglich mit und melden ihr etwaige spätere Änderungen.

TITEL IV
SCHLUSSBESTIMMUNGEN

Artikel 66
Ausschussverfahren

(1) Die Kommission wird von einem Ausschuss unterstützt. Dieser Ausschuss ist ein Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.

(2) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 5 Absatz 4 Buchstabe b der Verordnung (EU) Nr. 182/2011.

Artikel 67
Bewertung und Überarbeitung

(1) Bis zum 28. Juni 2024 und danach alle fünf Jahre bewertet die Kommission die Wirkung, Wirksamkeit und Effizienz der ENISA und ihrer Arbeitsmethoden und prüft, ob das Mandat der ENISA möglicherweise geändert werden muss und welche finanziellen Auswirkungen eine solche Änderung hätte. In der Bewertung werden alle Rückmeldungen an die ENISA in Bezug auf ihre Tätigkeiten berücksichtigt. Gelangt die Kommission zu der Auffassung, dass Ziele, Mandat und Aufgaben der ENISA deren Tätigkeit nicht länger rechtfertigen können, kann sie eine Änderung dieser Verordnung im Hinblick auf die für die ENISA geltenden Bestimmungen vorschlagen.

(2) Die Bewertung erstreckt sich auch auf die Wirkung, Wirksamkeit und Effizienz der Bestimmungen des Titels III dieser Verordnung im Hinblick auf die Ziele, für IKT-Produkte, -Dienste und -Prozesse in der Union ein angemessenes Maß an Cybersicherheit und einen besser funktionierenden Binnenmarkt zu gewährleisten.

(3) Bei der Bewertung wird beurteilt, ob wesentliche Anforderungen an die Cybersicherheit für den Zugang zum Binnenmarkt erforderlich sind, damit keine IKT-Produkte, -Dienste und -Prozesse auf den Unionsmarkt gelangen, die den grundlegenden Anforderungen an die Cybersicherheit nicht entsprechen.

(4) Die Kommission übermittelt bis zum 28. Juni 2024 und danach alle fünf Jahre den Bericht über die Bewertung zusammen mit ihren Schlussfolgerungen dem Europäischen Parlament, dem Rat und dem Verwaltungsrat. Die Ergebnisse des Berichts werden öffentlich bekannt gemacht.

Artikel 68
Aufhebung und Rechtsnachfolge

(1) Die Verordnung (EU) Nr. 526/2013 wird mit Wirkung vom 27. Juni 2019 aufgehoben.

(2) Bezugnahmen auf die Verordnung (EU) Nr. 526/2013 und auf die durch jene Verordnung errichtete ENISA gelten als Bezugnahmen auf die vorliegende Verordnung und auf die durch die vorliegende Verordnung errichtete ENISA.

(3) Die durch die vorliegende Verordnung errichtete ENISA ist in Bezug auf das Eigentum und alle Abkommen, rechtlichen Verpflichtungen, Beschäftigungsverträge, finanziellen Verpflichtungen und Verbindlichkeiten die Rechtsnachfolgerin der durch die Verordnung (EU) Nr. 526/2013 errichteten ENISA. Alle vom Verwaltungsrat und vom Exekutivrat gemäß der Verordnung (EU) Nr. 526/2013 getroffenen Entscheidungen bleiben gültig, sofern sie der vorliegenden Verordnung nicht zuwiderlaufen.

(4) Die ENISA wird zum 27. Juni 2019 für unbegrenzte Zeit errichtet.

(5) Der nach Artikel 24 Absatz 4 der Verordnung (EU) Nr. 526/2013 ernannte Exekutivdirektor bleibt im Amt und übt die Funktion des Exekutivdirektors nach Artikel 20 der vorliegenden Verordnung für die restliche Dauer seiner Amtszeit aus. Die übrigen Bestimmungen seines Vertrags bleiben unverändert.

(6) Die nach Artikel 6 der Verordnung (EU) Nr. 526/2013 ernannten Mitglieder des Verwaltungsrats und ihre Stellvertreter bleiben im Amt und üben die Funktion des Verwaltungsrats nach Artikel 15 der vorliegenden Verordnung für die restliche Dauer ihrer Amtszeit aus.

Artikel 69
Inkrafttreten

(1) Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.

(2) Die Artikel 58, 60, 61, 63, 64und 65, gelten ab dem 28. Juni 2021.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.

ANHANG
ANFORDERUNGEN AN KONFORMITÄTSBEWERTUNGSSTELLEN

Konformitätsbewertungsstellen, die akkreditiert werden möchten, müssen folgende Anforderungen erfüllen:

1. Eine Konformitätsbewertungsstelle muss nach nationalem Recht gegründet und mit Rechtspersönlichkeit ausgestattet sein.

2. Bei einer Konformitätsbewertungsstelle muss es sich um einen unabhängigen Dritten handeln, der mit der Einrichtung oder den IKT-Produkten, -Diensten oder -Prozessen, die er bewertet, in keinerlei Verbindung steht.

3. Eine Stelle, die einem Wirtschaftsverband oder einem Fachverband angehört und die IKT-Produkte, -Dienste oder -Prozesse bewertet, an deren Entwurf, Herstellung, Bereitstellung, Montage, Verwendung oder Wartung Unternehmen beteiligt sind, die von diesem Verband vertreten werden, kann als Konformitätsbewertungsstelle gelten, sofern ihre Unabhängigkeit sowie die Abwesenheit jedweder Interessenkonflikte nachgewiesen sind.

4. Die Konformitätsbewertungsstellen, ihre oberste Leitungsebene und die für die Erfüllung der Konformitätsbewertungsaufgaben zuständigen Mitarbeiter dürfen weder Konstrukteur, Hersteller, Lieferant, Installateur, Käufer, Eigentümer, Verwender oder Wartungsbetrieb des zu bewertenden IKT-Produkts, -Dienstes oder -Prozesses noch Bevollmächtigter einer dieser Parteien sein. Dieses Verbot schließt nicht die Verwendung von bereits einer Konformitätsbewertung unterzogenen IKT-Produkten, die für die Tätigkeit der Konformitätsbewertungsstelle nötig sind, oder die Verwendung solcher IKT-Produkte zum persönlichen Gebrauch aus.

5. Die Konformitätsbewertungsstellen, ihre oberste Leitungsebene und die für die Erfüllung der Konformitätsbewertungsaufgaben zuständigen Mitarbeiter dürfen weder direkt an Entwurf, Herstellung bzw. Bau, Vermarktung, Installation, Verwendung oder Instandsetzung dieser IKT-Produkte, -Dienste oder -Prozesse beteiligt sein, noch die an diesen Tätigkeiten beteiligten Parteien vertreten. Die Konformitätsbewertungsstellen, ihre oberste Leitungsebene und die für die Erfüllung der Konformitätsbewertungsaufgaben zuständigen Mitarbeiter dürfen sich nicht mit Tätigkeiten befassen, die ihre Unabhängigkeit bei der Beurteilung oder ihre Integrität im Zusammenhang mit ihren Konformitätsbewertungstätigkeiten, beeinträchtigen können. Dieses Verbot gilt besonders für Beratungsdienste.

6. Falls eine Konformitätsbewertungsstelle Eigentum einer öffentlichen Stelle oder Einrichtung ist oder von dieser betrieben wird, sind die Unabhängigkeit und die Abwesenheit von Interessenkonflikten zwischen der nationalen Behörde für die Cybersicherheitszertifizierung und der Konformitätsbewertungsstelle sicherzustellen und zu dokumentieren.

7. Die Konformitätsbewertungsstellen müssen sicherstellen, dass die Tätigkeiten ihrer Zweigunternehmen oder Unterauftragnehmer die Vertraulichkeit, Objektivität oder Unparteilichkeit ihrer Konformitätsbewertungstätigkeiten nicht beeinträchtigen.

8. Die Konformitätsbewertungsstellen und ihre Mitarbeiter müssen die Konformitätsbewertungstätigkeiten mit höchster beruflicher Integrität und der erforderli-

chen fachlichen Kompetenz in dem betreffenden Bereich durchführen; sie dürfen keinerlei Einflussnahme durch Druck oder Vergünstigungen, auch finanzieller Art, ausgesetzt sein, die sich auf ihre Beurteilung oder die Ergebnisse ihrer Konformitätsbewertungsarbeit auswirken könnte, insbesondere keinem Druck und keiner Einflussnahme durch Personen oder Personengruppen, die ein Interesse am Ergebnis dieser Tätigkeiten haben.

9. Eine Konformitätsbewertungsstelle muss in der Lage sein, die bei der Konformitätsbewertung anfallenden Aufgaben, die ihr mit dieser Verordnung übertragen wurden, auszuführen, unabhängig davon, ob diese Aufgaben von ihr selbst oder in ihrem Namen und unter ihrer Verantwortung ausgeführt werden. Jegliche Unterauftragsvergabe oder die Inanspruchnahme von externem Personal sind angemessen zu dokumentieren, dürfen nicht über Vermittler erfolgen und bedürfen einer schriftlichen Vereinbarung, in der unter anderem Vertraulichkeitsaspekte und Interessenkonflikte geklärt werden. Die betreffende Konformitätsbewertungsstelle übernimmt die volle Verantwortung für die durchgeführten Aufgaben.

10. Eine Konformitätsbewertungsstelle muss jederzeit, für jedes Konformitätsbewertungsverfahren und für jede Art, Kategorie und Unterkategorie von IKT-Produkten -Diensten oder -Prozessen über Folgendes verfügen:

    a) das erforderliche Personal mit Fachkenntnis und ausreichender einschlägiger Erfahrung, um die bei der Konformitätsbewertung anfallenden Aufgaben zu erfüllen;

    b) Beschreibungen von Verfahren, nach denen die Konformitätsbewertung durchgeführt wird, um sicherzustellen, dass die Verfahren transparent sind und wiederholt werden können. Sie muss über angemessene Regelungen und Verfahren verfügen, bei denen zwischen den Aufgaben, die sie als nach Artikel 61 notifizierte Stelle wahrnimmt, und ihren anderen Tätigkeiten unterschieden wird;

    c) Verfahren zur Durchführung von Tätigkeiten, bei denen die Größe eines Unternehmens, die Branche, in der es tätig ist, seine Struktur, der Grad an Komplexität der jeweiligen Technologie der ICT-Produkte, -Dienste oder -Prozesse und der Umstand, dass es sich um Massenfertigung oder Serienproduktion handelt, gebührend berücksichtigt werden.

11. Eine Konformitätsbewertungsstelle muss über die erforderlichen Mittel zur angemessenen Erledigung der technischen und administrativen Aufgaben verfügen, die mit der Konformitätsbewertung verbunden sind, und Zugang zu allen benötigten Ausrüstungen und Einrichtungen haben.

12. Die Personen, die für die Durchführung der Konformitätsbewertungstätigkeiten zuständig sind, müssen Folgendes besitzen:

    a) eine solide Fach- und Berufsausbildung, die alle Tätigkeiten der Konformitätsbewertung umfasst;

    b) eine ausreichende Kenntnis der Anforderungen, die mit den durchzuführenden Konformitätsbewertungen verbunden sind, und die entsprechende Befugnis, solche Bewertungen durchzuführen;

c) angemessene Kenntnis und angemessenes Verständnis der geltenden Anforderungen und Prüfnormen;

d) die Fähigkeit zur Erstellung von Bescheinigungen, Protokollen und Berichten als Nachweis für durchgeführte Konformitätsbewertungen.

13. Die Unparteilichkeit der Konformitätsbewertungsstellen, ihrer obersten Führungsebene, des für Bewertungen zuständigen Personals der Konformitätsbewertungsstelle und ihrer Unterauftragnehmer muss gewährleistet sein.

14. Die Vergütung für die oberste Leitungsebene und das für Bewertungen zuständige Personal der Konformitätsbewertungsstelle darf sich nicht nach der Anzahl der durchgeführten Konformitätsbewertungen oder deren Ergebnissen richten.

15. Die Konformitätsbewertungsstellen müssen eine Haftpflichtversicherung abschließen, sofern die Haftpflicht nicht aufgrund des nationalen Rechts vom Mitgliedstaat übernommen wird oder der Mitgliedstaat selbst unmittelbar für die Konformitätsbewertung verantwortlich ist.

16. Die Konformitätsbewertungsstelle und ihre Mitarbeiter, Gremien, Tochterunternehmen, Unterauftragnehmer und alle verbundenen Stellen oder Mitarbeiter externer Gremien einer Konformitätsbewertungsstelle müssen die Vertraulichkeit wahren, und die Informationen, die sie bei der Durchführung ihrer Konformitätsbewertungsaufgaben nach dieser Verordnung oder nach einer nationalen Vorschrift zur Durchführung dieser Verordnung erhalten, fallen unter die berufliche Schweigepflicht, außer wenn eine Offenlegung aufgrund von Rechtsvorschriften der Union oder des Mitgliedstaats, denen diese Personen unterliegen, erforderlich ist und außer gegenüber den zuständigen Behörden der Mitgliedstaaten, in denen sie ihre Tätigkeiten ausüben. Die Rechte des geistigen Eigentums sind zu schützen. Die Konformitätsbewertungsstelle muss über dokumentierte Verfahren in Bezug auf die Anforderungen dieser Nummer verfügen.

17. Abgesehen von Nummer 16 schließen die Anforderungen dieses Anhangs in keiner Weise der Austausch von technischen Informationen und regulatorischen Leitlinien zwischen einer Konformitätsbewertungsstelle und einer Person, die eine Zertifizierung beantragt oder deren Beantragung in Erwägung zieht, aus.

18. Konformitätsbewertungsstellen müssen ihre Tätigkeiten im Einklang mit einer Reihe kohärenter, gerechter und angemessener Geschäftsbedingungen ausüben, wobei sie in Bezug auf Gebühren die Interessen der KMU berücksichtigen.

19. Die Konformitätsbewertungsstellen müssen die Anforderungen der einschlägigen Norm erfüllen, die gemäß der Verordnung (EG) Nr. 765/2008 für die Akkreditierung der Konformitätsbewertungsstellen, die die Zertifizierung von IKT-Produkten, -Diensten oder -Prozessen vornehmen, harmonisiert ist.

20. Die Konformitätsbewertungsstellen müssen sicherstellen, dass die für die Konformitätsbewertung eingesetzten Prüflabors den Anforderungen der einschlägigen Norm entsprechen, die gemäß der Verordnung (EG) Nr. 765/2008 für die Akkreditierung der Labors, die Tests durchführen, harmonisiert ist.

RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 14. Dezember 2022

über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)

(Text von Bedeutung für den EWR)

Inhaltsübersicht

KAPITEL I
ALLGEMEINE BESTIMMUNGEN

Art. 1 Gegenstand

Art. 2 Anwendungsbereich

Art. 3 Wesentliche und wichtige Einrichtungen

Art. 4 Sektorspezifische Rechtsakte der Union

Art. 5 Mindestharmonisierung

Art. 6 Begriffsbestimmungen

KAPITEL II
KOORDINIERTE RAHMEN FÜR DIE CYBERSICHERHEIT

Art. 7 Nationale Cybersicherheitsstrategie

Art. 8 Zuständige Behörden und zentrale Anlaufstellen

Art. 9 Nationale Rahmen für das Cyberkrisenmanagement

Art. 10 Computer-Notfallteams (CSIRTs)

Art. 11 Anforderungen an die CSIRTs sowie technische Kapazitäten und Aufgaben der CSIRTs

Art. 12 Koordinierte Offenlegung von Schwachstellen und eine europäische Schwachstellendatenbank

Art. 13 Zusammenarbeit auf nationaler Ebene

KAPITEL III
ZUSAMMENARBEIT AUF UNIONS- UND INTERNATIONALER EBENE

Art. 14 Kooperationsgruppe

Art. 15 CSIRTs-Netzwerk

Art. 16 Das Europäische Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe)

Art. 17 Internationale Zusammenarbeit

Art. 18 Bericht über den Stand der Cybersicherheit in der Union

Art. 19 Peer Reviews

KAPITEL IV
RISIKOMANAGEMENTMAßNAHMEN UND BERICHTSPFLICHTEN IM BEREICH DER CYBERSICHERHEIT

Art. 20 Governance

Art. 21 Risikomanagementmaßnahmen im Bereich der Cybersicherheit

Art. 22 Koordinierte Risikobewertungen in Bezug auf die Sicherheit kritischer Lieferketten auf Ebene der Union

Art. 23 Berichtspflichten

Art. 24 Nutzung der europäischen Schemata für die Cybersicherheitszertifizierung

Art. 25 Normung

KAPITEL V
ZUSTÄNDIGKEIT UND REGISTRIERUNG

Art. 26 Zuständigkeit und Territorialität

Art. 27 Register der Einrichtungen

Art. 28 Datenbank der Domänennamen-Registrierungsdaten

KAPITEL VI
INFORMATIONSAUSTAUSCH

Art. 29 Vereinbarungen über den Austausch von Informationen zur Cybersicherheit

Art. 30 Freiwillige Meldung relevanter Informationen

KAPITEL VII
AUFSICHT UND DURCHSETZUNG

Art. 31 Allgemeine Aspekte der Aufsicht und Durchsetzung

Art. 32 Aufsichts- und Durchsetzungsmaßnahmen in Bezug auf wesentliche Einrichtungen

Art. 33 Aufsichts- und Durchsetzungsmaßnahmen in Bezug auf wichtige Einrichtungen

Art. 34 Allgemeine Bedingungen für die Verhängung von Geldbußen gegen wesentliche und wichtige Einrichtungen

Art. 35 Verstöße mit Verletzungen des Schutzes personenbezogener Daten

Art. 36 Sanktionen

Art. 37 Amtshilfe

KAPITEL VIII
DELEGIERTE RECHTSAKTE UND DURCHFÜHRUNGSRECHTSAKTE

Art. 38 Ausübung der Befugnisübertragung

Art. 39 Ausschussverfahren

KAPITEL IX
SCHLUSSBESTIMMUNGEN

Art. 40 Überprüfung

Art. 41 Umsetzung

Art. 42 & 43 [Vom Abdruck wurde abgesehen]

Art. 44 Aufhebung

Art. 45 Inkrafttreten

[Vom Abdruck der Erwägungsgründe wurde abgesehen.]

KAPITEL I
ALLGEMEINE BESTIMMUNGEN

Artikel 1
Gegenstand

(1) In dieser Richtlinie werden Maßnahmen festgelegt, mit denen in der gesamten Union ein hohes gemeinsames Cybersicherheitsniveau sichergestellt werden soll, um so das Funktionieren des Binnenmarkts zu verbessern.

(2) Zu diesem Zweck wird in dieser Richtlinie Folgendes festgelegt:

a) die Pflicht für alle Mitgliedstaaten, nationale Cybersicherheitsstrategien zu verabschieden sowie zuständige nationale Behörden, Behörden für das Cyberkrisenmanagement, zentrale Anlaufstellen für Cybersicherheit (zentrale Anlaufstellen) und Computer-Notfallteams (CSIRT) zu benennen oder einzurichten;

b) Pflichten in Bezug auf das Cybersicherheitsrisikomanagement sowie Berichtspflichten für Einrichtungen der in den Anhang I oder II aufgeführten Arten sowie für Einrichtungen, die nach Richtlinie (EU) 2022/2557 als kritische Einrichtungen eingestuft wurden;

c) Vorschriften und Pflichten zum Austausch von Cybersicherheitsinformationen;

d) Aufsichts- und Durchsetzungspflichten für die Mitgliedstaaten.

Artikel 2
Anwendungsbereich

(1) Diese Richtlinie gilt für öffentliche oder private Einrichtungen der in den Anhang I oder II genannten Art, die nach Artikel 2 des Anhangs der Empfehlung 2003/361/EG als mittlere Unternehmen gelten oder die Schwellenwerte für mittlere Unternehmen nach Absatz 1 jenes Artikels überschreiten und ihre Dienste in der Union erbringen oder ihre Tätigkeiten dort ausüben.

Artikel 3 Absatz 4 des Anhangs dieser Empfehlung gilt nicht für die Zwecke dieser Richtlinie.

(2) Unabhängig von der Größe der Einrichtungen gilt diese Richtlinie auch für Einrichtungen der in den Anhang I oder II genannten Art, wenn

a) die Dienste erbracht werden von:

   i) Anbietern von öffentlichen elektronischen Kommunikationsnetzen oder von öffentlich zugänglichen elektronischen Kommunikationsdiensten;

   ii) Vertrauensdiensteanbietern;

   iii) Namenregistern der Domäne oberster Stufe und Domänennamensystem-Diensteanbietern;

b) es sich bei der Einrichtung in einem Mitgliedstaat um den einzigen Anbieter eines Dienstes handelt, der für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten unerlässlich ist;

c) sich eine Störung des von der Einrichtung erbrachten Dienstes wesentlich auf die öffentliche Ordnung, die öffentliche Sicherheit oder die öffentliche Gesundheit auswirken könnte;

d) eine Störung des von der Einrichtung erbrachten Dienstes zu einem wesentlichen Systemrisiko führen könnte, insbesondere in Sektoren, in denen eine solche Störung grenzübergreifende Auswirkungen haben könnte;

e) die Einrichtung aufgrund der besonderen Bedeutung, die sie auf nationaler oder regionaler Ebene für den betreffenden Sektor oder die betreffende Art des Dienstes oder für andere voneinander abhängige Sektoren in dem Mitgliedstaat hat, kritisch ist;

f) die Einrichtung eine Einrichtung der öffentlichen Verwaltung:

   i) von einem Mitgliedstaat gemäß nationalem Recht definierte Einrichtung der öffentlichen Verwaltung der Zentralregierung ist oder

   ii) von einem Mitgliedstaat gemäß nationalem Recht definierte Einrichtung der öffentlichen Verwaltung auf regionaler Ebene ist, die nach einer risikobasierten Bewertung Dienste erbringt, deren Störung erhebliche Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Tätigkeiten haben könnte.

(3) Unabhängig von der Größe der Einrichtungen gilt diese Richtlinie auch für Einrichtungen, die nach Richtlinie (EU) 2022/2557 als kritische Einrichtungen eingestuft wurden.

(4) Unabhängig von der Größe der Einrichtungen gilt diese Richtlinie auch für Einrichtungen, die Domänennamenregistrierungsdienste erbringen.

(5) Die Mitgliedstaaten können vorsehen, dass diese Richtlinie Anwendung findet auf:

a) Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene;

b) Bildungseinrichtungen, insbesondere wenn sie kritische Forschungstätigkeiten durchführen.

(6) Diese Richtlinie lässt die Zuständigkeit der Mitgliedstaaten in Bezug auf die Aufrechterhaltung der nationalen Sicherheit und ihre Befugnis, andere wesentliche staatliche Funktionen zu schützen, einschließlich der Wahrung der territorialen Unversehrtheit des Staates und der Aufrechterhaltung der öffentlichen Ordnung, unberührt.

(7) Diese Richtlinie gilt nicht für Einrichtungen der öffentlichen Verwaltung, die ihre Tätigkeiten in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung ausüben, einschließlich der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten.

(8) Zu diesem Zweck können die Mitgliedstaaten bestimmte Einrichtungen, die in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung tätig sind, einschließlich der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten, oder die Dienste ausschließlich für die in Absatz 7 dieses Artikels genannten Einrichtungen der öffentlichen Verwaltung erbringen, von den in Artikel 21 oder 23 festgelegten Verpflichtungen in Bezug auf diese Tätigkeiten oder Dienste ausnehmen. In solchen Fällen gelten die in Kapitel VII genannten Aufsichts- und Durchsetzungsmaßnahmen nicht für diese spezifischen Tätigkeiten oder Dienste. Wenn die Einrichtungen ausschließlich Tätigkeiten der in diesem Absatz genannten Art ausüben oder entsprechende Dienste erbringen, können die Mitgliedstaaten auch beschließen, diese Einrichtungen von den in den Artikeln 3 und 27 festgelegten Verpflichtungen auszunehmen.

(9) Die Absätze 7 und 8 finden keine Anwendung, wenn eine Einrichtung als Vertrauensdiensteanbieter auftritt.

(10) Diese Richtlinie gilt nicht für Einrichtungen, die die Mitgliedstaaten gemäß Artikel 2 Absatz 4 der Verordnung (EU) 2022/2554 vom Anwendungsbereich der genannten Verordnung ausgenommen haben.

(11) Die in dieser Richtlinie festgelegten Verpflichtungen umfassen nicht die Bereitstellung von Informationen, deren Offenlegung wesentlichen Interessen der Mitgliedstaaten im Bereich der nationalen Sicherheit, der öffentlichen Sicherheit oder der Verteidigung zuwiderlaufen würde.

(12) Diese Richtlinie gilt unbeschadet der Verordnung (EU) 2016/679, der Richtlinie 2002/58/EG, der Richtlinien 2011/93/EU (1) und 2013/40/EU (2) des Europäischen Parlaments und des Rates sowie der Richtlinie (EU) 2022/2557.

(13) Unbeschadet des Artikels 346 AEUV werden Informationen, die gemäß den Vorschriften der Union oder der Mitgliedstaaten, wie z. B. Vorschriften über das Geschäftsgeheimnis, vertraulich sind, mit der Kommission und anderen zuständigen Behörden im Einklang mit dieser Richtlinie nur ausgetauscht, wenn dieser Austausch für die Anwendung dieser Richtlinie erforderlich ist. Die auszutauschenden Informationen werden auf den zum Zweck dieses Informationsaustauschs relevanten und angemessenen Umfang beschränkt. Beim Infor-

mationsaustausch werden die Vertraulichkeit der Informationen gewahrt sowie die Sicherheit und die geschäftlichen Interessen der betreffenden kritischen Einrichtungen geschützt.

(14) Einrichtungen, die zuständige Behörden, die zentrale Anlaufstellen und die CSIRTs verarbeiten personenbezogene Daten, soweit dies für die Zwecke dieser Richtlinie erforderlich ist und im Einklang mit der Verordnung (EU) 2016/679, insbesondere auf der Grundlage von Artikel 6 der genannten Verordnung.

Die Verarbeitung personenbezogener Daten gemäß dieser Richtlinie durch Anbieter öffentlicher elektronischer Kommunikationsnetze oder Betreiber öffentlich zugänglicher elektronischer Kommunikationsdienste erfolgt im Einklang mit dem Datenschutzrecht der Union und dem Unionsrecht zum Schutz der Privatsphäre, insbesondere der Richtlinie 2002/58/EG.

Artikel 3
Wesentliche und wichtige Einrichtungen

(1) Für die Zwecke dieser Richtlinie gelten als wesentliche Einrichtungen:

a) Einrichtungen der in Anhang I aufgeführten Art, die die in Artikel 2 Absatz 1 des Anhangs der Empfehlung 2003/361/EG genannten Schwellenwerte für mittlere Unternehmen überschreiten;

b) qualifizierte Vertrauensdiensteanbieter und Domänennamenregister der Domäne oberster Stufe sowie DNS-Diensteanbieter, unabhängig von ihrer Größe;

c) Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste, die nach Artikel 2 des Anhangs der Empfehlung 2003/361/EG genannten als mittlere Unternehmen gelten;

d) Einrichtungen der öffentlichen Verwaltung nach Artikel 2 Absatz 2 Buchstabe f Ziffer i;

e) sonstige Einrichtungen der in Anhang I oder II aufgeführten Art, die von einem Mitgliedstaat gemäß Artikel 2 Absatz 2 Buchstaben b bis e als wesentliche Einrichtungen eingestuft werden;

f) Einrichtungen, die gemäß der Richtlinie (EU) 2022/2557 als kritische Einrichtungen eingestuft wurden und die in Artikel 2 Absatz 3 der vorliegenden Richtlinie genannt werden;

g) sofern der Mitgliedstaat dies vorsieht, Einrichtungen, die von den Mitgliedstaaten vor dem 16. Januar 2023 gemäß der Richtlinie (EU) 2016/1148 oder nach nationalem Recht als Betreiber wesentlicher Dienste eingestuft wurden.

(2) Für die Zwecke dieser Richtlinie gelten Einrichtungen der in Anhang I oder II aufgeführten Art, die nicht als wesentliche Einrichtungen im Sinne von Absatz 1 des vorliegenden Artikels gelten, als wichtige Einrichtungen. Dies schließt Einrichtungen ein, die von den Mitgliedstaaten gemäß Artikel 2 Absatz 2 Buchstaben b bis e als wichtige Einrichtungen eingestuft wurden.

(3) Bis zum 17. April 2025 erstellen die Mitgliedstaaten eine Liste von wesentlichen und wichtigen Einrichtungen und von Einrichtungen, die Domänennamen-Registrierungs-

dienste erbringen. Die Mitgliedstaaten überprüfen diese Liste danach regelmäßig, mindestens jedoch alle zwei Jahre, und aktualisieren sie gegebenenfalls.

(4) Für die Zwecke der Erstellung der in Absatz 3 genannten Liste schreiben die Mitgliedstaaten vor, dass die jenem Absatz genannten Einrichtungen den zuständigen Behörden mindestens die folgenden Informationen übermitteln:

a) den Namen der Einrichtung,

b) die Anschrift und aktuellen Kontaktdaten, einschließlich der E-Mail-Adressen, IP-Adressbereiche und Telefonnummern,

c) gegebenenfalls den relevanten Sektor und Teilsektor gemäß Anhang I oder II sowie

d) gegebenenfalls eine Liste der Mitgliedstaaten, in denen sie Dienste erbringen, die in den Anwendungsbereich dieser Richtlinie fallen.

Die in Absatz 3 genannten Einrichtungen teilen alle Änderungen der gemäß Unterabsatz 1 des vorliegenden Absatzes übermittelten Angaben unverzüglich mit, in jedem Fall jedoch innerhalb von zwei Wochen ab dem Zeitpunkt der Änderung.

Die Kommission stellt mit Unterstützung der Agentur der Europäischen Union für Cybersicherheit (ENISA) unverzüglich Leitlinien und Vorlagen für die in diesem Absatz festgelegten Verpflichtungen bereit.

Die Mitgliedstaaten können nationale Mechanismen für die Registrierung von Einrichtungen einrichten.

(5) Bis zum 17. April 2025 und danach alle zwei Jahre teilen die zuständigen Behörden Folgendes mit:

a) der Kommission und der Kooperationsgruppe für jeden Sektor und Teilsektor gemäß Anhang I oder II die Anzahl der wesentlichen und wichtigen Einrichtungen, die gemäß Absatz 3 auf die Liste aufgenommen wurden, und

b) der Kommission sachdienliche Informationen über die Zahl der wesentlichen und wichtigen Einrichtungen, die gemäß Artikel 2 Absatz 2 Buchstaben b bis e ermittelt wurden, über den Sektor und den Teilsektor gemäß Anhang I oder II, zu dem sie gehören, über die Art der von ihnen erbrachten Dienste und über die Bestimmung unter denen in Artikel 2 Absatz 2 Buchstaben b bis e festgelegten Bestimmungen, auf deren Grundlage sie ermittelt wurden.

(6) Bis zum 17. April 2025 können die Mitgliedstaaten der Kommission auf Ersuchen der Kommission die Namen der wesentlichen und wichtigen Einrichtungen gemäß Absatz 5 Buchstabe b mitteilen.

Artikel 4
Sektorspezifische Rechtsakte der Union

(1) Wenn wesentliche oder wichtige Einrichtungen gemäß sektorspezifischen Rechtsakten der Union entweder Maßnahmen zum Cybersicherheitsrisikomanagement ergreifen oder erhebliche Sicherheitsvorfälle melden müssen und wenn die entsprechenden Anforderungen in ihrer Wirkung den in dieser Richtlinie festgelegten Verpflichtungen zumindest gleichwertig sind, finden die einschlägigen Bestimmungen dieser Richtlinie, einschließlich der Be-

stimmungen über Aufsicht und Durchsetzung in Kapitel VII, keine Anwendung auf solche Einrichtungen. Wenn die sektorspezifischen Rechtsakte der Union nicht für alle in den Anwendungsbereich dieser Richtlinie fallenden Einrichtungen eines bestimmten Sektors gelten, kommen die einschlägigen Bestimmungen dieser Richtlinie weiterhin für Einrichtungen zur Anwendung, die nicht unter diese sektorspezifischen Rechtsakte der Union fallen.

(2) Die in Absatz 1 dieses Artikels genannten Anforderungen gelten den in dieser Richtlinie festgelegten Verpflichtungen in ihrer Wirkung als gleichwertig, wenn

a) die Maßnahmen zum Cybersicherheitsrisikomanagement den in Artikel 21 Absätze 1 und 2 festgelegten Maßnahmen in ihrer Wirkung mindestens gleichwertig sind, oder

b) der sektorspezifische Rechtsakt der Union einen unmittelbaren — gegebenenfalls automatischen und direkten — Zugang zu den Meldungen von Sicherheitsvorfällen durch die CSIRTs, die zuständigen Behörden oder die zentralen Anlaufstellen gemäß dieser Richtlinie vorsieht und wenn die Anforderungen an die Meldung erheblicher Sicherheitsvorfälle in ihrer Wirkung mindestens den in Artikel 23 Absätze 1 bis 6 festgelegten gleichwertig sind.

(3) Die Kommission wird bis zum 17. Juli 2023 Leitlinien zur Klarstellung der Anwendung der Absätze 1 und 2 bereitstellen. Die Kommission überprüft diese Leitlinien regelmäßig. Bei der Ausarbeitung der Leitlinien berücksichtigt die Kommission alle Stellungnahmen der Kooperationsgruppe und der ENISA.

Artikel 5
Mindestharmonisierung

Diese Richtlinie hindert die Mitgliedstaaten nicht daran, Bestimmungen zu erlassen oder beizubehalten, die ein höheres Cybersicherheitsniveau gewährleisten, sofern diese Bestimmungen mit den Pflichten der Mitgliedstaaten nach dem Unionsrecht im Einklang stehen.

Artikel 6
Begriffsbestimmungen

Für die Zwecke dieser Richtlinie bezeichnet der Ausdruck

1. „Netz- und Informationssystem“

   a) ein elektronisches Kommunikationsnetz im Sinne des Artikels 2 Nummer 1 der Richtlinie (EU) 2018/1972,

   b) ein Gerät oder eine Gruppe miteinander verbundener oder zusammenhängender Geräte, die einzeln oder zu mehreren auf der Grundlage eines Programms die automatische Verarbeitung digitaler Daten durchführen, oder

   c) digitale Daten, die von den — in den Buchstaben a und b genannten — Elementen zum Zwecke ihres Betriebs, ihrer Nutzung, ihres Schutzes und ihrer Pflege gespeichert, verarbeitet, abgerufen oder übertragen werden;

2. „Sicherheit von Netz- und Informationssystemen“ die Fähigkeit von Netz- und Informationssystemen, auf einem bestimmten Vertrauensniveau alle Ereignisse abzuwehren, die die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter oder übermittelter oder verarbeiteter Daten oder der Dienste, die über

diese Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen können;

3. „Cybersicherheit“ die Cybersicherheit im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) 2019/881;

4. „nationale Cybersicherheitsstrategie“ einen kohärenten Rahmen eines Mitgliedstaats mit strategischen Zielen und Prioritäten im Bereich der Cybersicherheit und der zu ihrer Verwirklichung erforderlichen Governance in diesem Mitgliedstaat;

5. „Beinahe-Vorfall“ ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigt haben könnte, dessen Eintritt jedoch erfolgreich verhindert wurde bzw. das nicht eingetreten ist;

6. „Sicherheitsvorfall“ ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigt;

7. „Cybersicherheitsvorfall großen Ausmaßes“ einen Sicherheitsvorfall, der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit eines Mitgliedstaats übersteigt, oder der beträchtliche Auswirkungen auf mindestens zwei Mitgliedstaaten hat;

8. „Bewältigung von Sicherheitsvorfällen“ alle Maßnahmen und Verfahren zur Verhütung, Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen oder die Reaktion darauf und die Erholung davon;

9. „Risiko“ das Potenzial für Verluste oder Störungen, die durch einen Sicherheitsvorfall verursacht werden, das als eine Kombination des Ausmaßes eines solchen Verlusts oder einer solchen Störung und der Wahrscheinlichkeit des Eintretens des Sicherheitsvorfalls zum Ausdruck gebracht wird;

10. „Cyberbedrohung“ eine Cyberbedrohung im Sinne des Artikel 2 Nummer 8 der Verordnung (EU) 2019/881;

11. „erhebliche Cyberbedrohung“ eine Cyberbedrohung, die das Potenzial besitzt, die Netz- und Informationssysteme einer Einrichtung oder der Nutzer solcher Systeme aufgrund ihrer technischen Merkmale erheblich zu beeinträchtigen, indem sie erheblichen materiellen oder immateriellen Schaden verursacht;

12. „IKT-Produkt“ ein IKT-Produkt im Sinne des Artikels 2 Nummer 12 der Verordnung (EU) 2019/881;

13. „IKT-Dienst“ bezeichnet einen IKT-Dienst im Sinne des Artikels 2 Nummer 13 der Verordnung (EU) 2019/881;

14. „IKT-Prozess“ einen IKT-Prozess im Sinne des Artikels 2 Nummer 14 der Verordnung (EU) 2019/881;

15. „Schwachstelle“ eine Schwäche, Anfälligkeit oder Fehlfunktion von IKT-Produkten oder IKT-Diensten, die bei einer Cyberbedrohung ausgenutzt werden kann;

16. „Norm“ eine Norm im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates (3);

17. „technische Spezifikation“ eine technische Spezifikation im Sinne des Artikels 2 Nummer 4 der Verordnung (EU) Nr. 1025/2012;

18. „Internet-Knoten“ eine Netzeinrichtung, die die Zusammenschaltung von mehr als zwei unabhängigen Netzen (autonomen Systemen) ermöglicht, in erster Linie zur Erleichterung des Austauschs von Internet-Datenverkehr, der nur der Zusammenschaltung autonomer Systeme dient und weder voraussetzt, dass der Internet-Datenverkehr zwischen zwei beliebigen teilnehmenden autonomen Systemen über ein drittes autonomes System läuft; noch den betreffenden Datenverkehr verändert oder anderweitig beeinträchtigt;

19. „Domänennamensystem“ oder „DNS“ ein verteiltes hierarchisches Verzeichnissystem, das die Identifizierung von Diensten und Ressourcen im Internet ermöglicht und es Endnutzergeräten erlaubt, Internet-Routing- und Konnektivitätsdienste zu nutzen, um diese Dienste und Ressourcen zu erreichen;

20. „DNS-Diensteanbieter“ eine Einrichtung, die

    a) für Internet-Endnutzer öffentlich verfügbare rekursive Dienste zur Auflösung von Domänennamen anbietet oder

    b) autoritative Dienste zur Auflösung von Domänennamen zur Nutzung durch Dritte, mit Ausnahme von Root-Namenservern, anbietet;

21. „Namenregister der Domäne oberster Stufe“ oder „TLD-Namenregister“ eine Einrichtung, der eine bestimmte Domäne oberster Stufe (Top Level Domain — TLD) übertragen wurde und die für die Verwaltung der TLD, einschließlich der Registrierung von Domänennamen unterhalb der TLD, sowie für den technischen Betrieb der TLD, einschließlich des Betriebs ihrer Namenserver, der Pflege ihrer Datenbanken und der Verteilung von TLD-Zonendateien über die Namenserver, zuständig ist, unabhängig davon, ob der Betrieb durch die Einrichtung selbst erfolgt oder ausgelagert wird, jedoch mit Ausnahme von Situationen, in denen TLD-Namen von einem Register nur für seine eigenen Zwecke verwendet werden;

22. „Einrichtung, die Domänennamen-Registrierungsdienste erbringt“ ein Registrar oder eine Stelle, die im Namen von Registraren tätig ist, wie etwa ein Anbieter oder Wiederverkäufer von Datenschutz- oder Proxy-Registrierungsdiensten;

23. „digitaler Dienst“ einen Dienst im Sinne des Artikels 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates (4);

24. „Vertrauensdienst“ einen Vertrauensdienst im Sinne des Artikels 3 Nummer 16 der Verordnung (EU) Nr. 910/2014;

25. „Vertrauensdiensteanbieter“ einen Vertrauensdiensteanbieter im Sinne des Artikels 3 Nummer 19 der Verordnung (EU) Nr. 910/2014;

26. „qualifizierter Vertrauensdienst“ einen qualifizierten Vertrauensdienst im Sinne des Artikels 3 Nummer 17 der Verordnung (EU) Nr. 910/2014;

27. „qualifizierter Vertrauensdiensteanbieter“ einen qualifizierten Vertrauensdiensteanbieter im Sinne des Artikels 3 Nummer 20 der Verordnung (EU) Nr. 910/2014;

28. „Online-Marktplatz“ einen digitalen Dienst im Sinne des Artikels 2 Buchstabe n der Richtlinie 2005/29/EG des Europäischen Parlaments und des Rates (5);

29. „Online-Suchmaschine“ eine Online-Suchmaschine im Sinne des Artikels 2 Nummer 5 der Verordnung (EU) 2019/1150 des Europäischen Parlaments und des Rates (6);

30. „Cloud-Computing-Dienst“ einen digitalen Dienst, der auf Abruf die Verwaltung und den umfassenden Fernzugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglicht, auch wenn diese Ressourcen auf mehrere Standorte verteilt sind;

31. „Rechenzentrumsdienst“ einen Dienst, mit dem spezielle Strukturen oder Gruppen von Strukturen für die zentrale Unterbringung, die Verbindung und den Betrieb von IT- und Netzausrüstungen zur Erbringung von Datenspeicher-, Datenverarbeitungs- und Datentransportdiensten sowie alle Anlagen und Infrastrukturen für die Leistungsverteilung und die Umgebungskontrolle bereitgestellt werden;

32. „Inhaltszustellnetz“ bezeichnet ein Netz dezentraler Server zur Gewährleistung einer hohen Verfügbarkeit, Zugänglichkeit oder schnellen Zustellung digitaler Inhalte und Dienste für Internetnutzer im Auftrag von Inhalte- und Diensteanbietern;

33. „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;

34. „Vertreter“ eine in der Union niedergelassene natürliche oder juristische Person, die ausdrücklich benannt wurde, um im Auftrag eines DNS-Diensteanbieters, einer Einrichtung, die Domänennamen-Registrierungsdienste erbringt, eines TLD-Namenregisters, eines Anbieters von Cloud-Computing-Diensten, eines Anbieters von Rechenzentrumsdiensten, eines Betreibers von Inhaltszustellnetzen, eines Anbieters verwalteter Dienste, eines Anbieters verwalteter Sicherheitsdienste oder eines Anbieters von einem Online-Marktplatz, von einer Online-Suchmaschine oder von einer Plattform für Dienste sozialer Netzwerke, der bzw. die nicht in der Union niedergelassen ist, zu handeln, und an die sich eine nationale zuständige Behörde oder ein CSIRT — statt an die Einrichtung — hinsichtlich der Pflichten dieser Einrichtung gemäß dieser Richtlinie wenden kann;

35. „Einrichtung der öffentlichen Verwaltung“ eine als solche in einem Mitgliedstaat nach nationalem Recht anerkannte Einrichtung, ausgenommen Justiz, Parlamente und Zentralbanken, die die folgenden Kriterien erfüllt:

    a) sie wurde zu dem Zweck gegründet, im allgemeinen Interesse liegende Aufgaben zu erfüllen, und hat keinen gewerblichen oder kommerziellen Charakter,

    b) sie besitzt Rechtspersönlichkeit oder ist gesetzlich dazu befugt, im Namen einer anderen Einrichtung mit eigener Rechtspersönlichkeit zu handeln,

c) sie wird überwiegend vom Staat, Gebietskörperschaften oder von anderen Körperschaften des öffentlichen Rechts finanziert, untersteht hinsichtlich ihrer Leitung der Aufsicht dieser Körperschaften oder verfügt über ein Verwaltungs-, Leitungs- bzw. Aufsichtsorgan, das mehrheitlich aus Mitgliedern besteht, die vom Staat, von Gebietskörperschaften oder von anderen Körperschaften des öffentlichen Rechts eingesetzt worden sind,

d) sie ist befugt, an natürliche oder juristische Personen Verwaltungs- oder Regulierungsentscheidungen zu richten, die deren Rechte im grenzüberschreitenden Personen-, Waren-, Dienstleistungs- oder Kapitalverkehr berühren;

36. „öffentliches elektronisches Kommunikationsnetz“ ein öffentliches elektronisches Kommunikationsnetz im Sinne von Artikel 2 Nummer 8 der Richtlinie (EU) 2018/1972;

37. „elektronischer Kommunikationsdienst“ einen elektronischen Kommunikationsdienst im Sinne des Artikels 2 Nummer 4 der Richtlinie (EU) 2018/1972;

38. „Einrichtung“ eine natürliche Person oder nach dem an ihrem Sitz geltenden nationalen Recht geschaffene und anerkannte juristische Person, die in eigenem Namen Rechte ausüben und Pflichten unterliegen kann;

39. „Anbieter verwalteter Dienste“ eine Einrichtung, die Dienste im Zusammenhang mit der Installation, der Verwaltung, dem Betrieb oder der Wartung von IKT-Produkten, Netzen, Infrastruktur, Anwendungen oder jeglicher anderer Netz- und Informationssysteme durch Unterstützung oder aktive Verwaltung erbringt, die entweder in den Räumlichkeiten der Kunden oder aus der Ferne erbringt;

40. „Anbieter verwalteter Sicherheitsdienste“ einen Anbieter verwalteter Dienste, der Unterstützung für Tätigkeiten im Zusammenhang mit dem Risikomanagement im Bereich der Cybersicherheit durchführt oder erbringt;

41. „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, die jedoch Bildungseinrichtungen nicht einschließt.

KAPITEL II
KOORDINIERTE RAHMEN FÜR DIE CYBERSICHERHEIT

Artikel 7
Nationale Cybersicherheitsstrategie

(1) Jeder Mitgliedstaat erlässt eine nationale Cybersicherheitsstrategie, die die strategischen Ziele, die zur Erreichung dieser Ziele erforderlichen Ressourcen sowie angemessene politische und regulatorische Maßnahmen zur Erreichung und Aufrechterhaltung eines hohen Cybersicherheitsniveaus enthält. Die nationale Cybersicherheitsstrategie muss Folgendes umfassen:

a) Ziele und Prioritäten der Cybersicherheitsstrategie des Mitgliedstaats, die insbesondere die in den Anhängen I und II aufgeführten Sektoren abdecken;

b) einen Steuerungsrahmen zur Verwirklichung der unter Buchstabe a dieses Absatzes genannten Ziele und Prioritäten, der die in Absatz 2 genannten Konzepte umfasst;

c) einen Steuerungsrahmen, in dem die Aufgaben und Zuständigkeiten der jeweiligen Interessenträger auf nationaler Ebene klargestellt, die Zusammenarbeit und Koordinierung auf nationaler Ebene zwischen den nach dieser Richtlinie zuständigen Behörden, zentralen Anlaufstellen und CSIRTs sowie die Koordinierung und Zusammenarbeit zwischen diesen Stellen und nach sektorspezifischen Rechtsakten der Union zuständigen Behörden untermauert werden;

d) einen Mechanismus zur Ermittlung von relevanten Anlagen und eine Bewertung der Cybersicherheitsrisiken in diesem Mitgliedstaat;

e) die Bestimmung von Maßnahmen zur Gewährleistung der Vorsorge, Reaktionsfähigkeit und Wiederherstellung bei Sicherheitsvorfällen, einschließlich der Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor;

f) eine Liste der verschiedenen Behörden und Interessenträger, die an der Umsetzung der nationalen Cybersicherheitsstrategie beteiligt sind;

g) einen politischen Rahmen für eine verstärkte Koordinierung zwischen den nach dieser Richtlinie zuständigen Behörden und den nach der Richtlinie (EU) 2022/2557 zuständigen Behörden zum Zweck des Informationsaustauschs über Risiken, Bedrohungen und Sicherheitsvorfälle sowie über nicht cyberbezogene Risiken, Bedrohungen und Sicherheitsvorfälle und für die Wahrnehmung von Aufsichtsaufgaben, soweit zutreffend;

h) einen Plan, einschließlich erforderlicher Maßnahmen, zur Steigerung des allgemeinen Grads der Sensibilisierung für Cybersicherheit bei den Bürgerinnen und Bürgern.

(2) Im Rahmen der nationalen Cybersicherheitsstrategie nehmen die Mitgliedstaaten insbesondere Konzepte an

a) für die Cybersicherheit in der Lieferkette für IKT-Produkte und IKT-Dienste, die von Einrichtungen für die Erbringung ihrer Dienste genutzt werden;

b) für die Aufnahme und Spezifikation cybersicherheitsbezogener Anforderungen an IKT-Produkte und IKT-Dienste bei der Vergabe öffentlicher Aufträge, einschließlich hinsichtlich der Zertifizierung der Cybersicherheit, der Verschlüsselung und der Nutzung quelloffener Cybersicherheitsprodukte;

c) für das Vorgehen bei Schwachstellen, das die Förderung und Erleichterung der koordinierten Offenlegung von Schwachstellen nach Artikel 12 Absatz 1 umfasst;

d) im Zusammenhang mit der Aufrechterhaltung der allgemeinen Verfügbarkeit, Integrität und Vertraulichkeit des öffentlichen Kerns des offenen Internets, erforderlichenfalls einschließlich der Cybersicherheit von Unterseekommunikationskabeln;

e) zur Förderung der Entwicklung und Integration einschlägiger fortgeschrittener Technologien, damit Risikomanagementmaßnahmen im Bereich der Cybersicherheit auf dem neuesten Stand zur Anwendung gelangen;

f) zur Förderung und Entwicklung der allgemeinen und beruflichen Bildung im Bereich der Cybersicherheit, von Kompetenzen, Sensibilisierungsmaßnahmen und Forschungs- und Entwicklungsinitiativen im Bereich der Cybersicherheit sowie der Anleitung zu guten Vorgehensweisen und Kontrollen im Bereich der Cyberhygiene für Bürgerinnen und Bürger, Interessenträger und Einrichtungen;

g) zur Unterstützung von Hochschul- und Forschungseinrichtungen bei der Entwicklung, der Verbesserung des Einsatzes von Cybersicherheitsinstrumenten und sicherer Netzinfrastruktur;

h) mit einschlägigen Verfahren und geeigneten Instrumenten für den Informationsaustausch, um den freiwilligen Austausch von Cybersicherheits-Informationen zwischen Einrichtungen im Einklang mit dem Unionsrecht zu unterstützen;

i) zur Stärkung des Grundniveaus für Cyberresilienz und Cyberhygiene kleiner und mittlerer Unternehmen, insbesondere vom Anwendungsbereich dieser Richtlinie ausgenommener KMU, durch Bereitstellung leicht zugänglicher Orientierungshilfen und Unterstützung für ihre spezifischen Bedürfnisse;

j) zur Förderung eines aktiven Cyberschutzes.

(3) Die Mitgliedstaaten notifizieren der Kommission ihre nationalen Cybersicherheitsstrategien innerhalb von drei Monaten nach ihrem Erlass. Die Mitgliedstaaten können auf ihre nationale Sicherheit bezogene Informationen von diesen Notifizierungen ausnehmen.

(4) Die Mitgliedstaaten bewerten ihre nationalen Cybersicherheitsstrategien regelmäßig, mindestens aber alle fünf Jahre auf der Grundlage wesentlicher Leistungsindikatoren und aktualisieren diese erforderlichenfalls. Die ENISA unterstützt die Mitgliedstaaten auf deren Wunsch bei der Entwicklung oder Aktualisierung einer nationalen Cybersicherheitsstrategie und wesentlicher Leistungsindikatoren für die Bewertung dieser Strategie, um sie mit den in dieser Richtlinie festgelegten Anforderungen und Verpflichtungen in Einklang zu bringen.

Artikel 8
Zuständige Behörden und zentrale Anlaufstellen

(1) Jeder Mitgliedstaat benennt eine oder mehrere für die Cybersicherheit und die in Kapitel VII genannten Aufsichtsaufgaben zuständige Behörden (zuständige Behörden) oder richtet sie ein.

(2) Die zuständigen Behörden gemäß Absatz 1 überwachen die Anwendung dieser Richtlinie auf nationaler Ebene.

(3) Jeder Mitgliedstaat benennt eine zentrale Anlaufstelle oder richtet sie ein. Benennt ein Mitgliedstaat nur eine zuständige Behörde nach Absatz 1 oder richtet er nur eine solche zuständige Behörde ein, so ist diese zuständige Behörde auch die zentrale Anlaufstelle dieses Mitgliedstaats.

(4) Jede zentrale Anlaufstelle fungiert als Verbindungsstelle, um die grenzüberschreitende Zusammenarbeit der Behörden des Mitgliedstaats mit den entsprechenden Behörden anderer Mitgliedstaaten und gegebenenfalls mit der Kommission und der ENISA sowie die sektorübergreifende Zusammenarbeit mit anderen zuständigen Behörden innerhalb ihres Mitgliedstaats zu gewährleisten.

(5) Die Mitgliedstaaten gewährleisten, dass ihre zuständigen Behörden und zentralen Anlaufstellen mit angemessenen Ressourcen ausgestattet sind, damit sie die ihnen übertragenen Aufgaben wirksam und effizient wahrnehmen können und die Ziele dieser Richtlinie somit erreicht werden.

(6) Die Mitgliedstaaten notifizieren der Kommission unverzüglich die Identität der zuständigen Behörde gemäß Absatz 1 und der zentralen Anlaufstelle gemäß Absatz 3, die Aufgaben dieser Behörden sowie etwaige spätere Änderungen dieser Angaben. Jeder Mitgliedstaat veröffentlicht die Identität seiner zuständigen Behörde. Die Kommission erstellt eine öffentlich verfügbare Liste der zentralen Anlaufstellen.

Artikel 9
Nationale Rahmen für das Cyberkrisenmanagement

(1) Jeder Mitgliedstaat benennt eine oder mehrere für das Management von Cybersicherheitsvorfällen großen Ausmaßes und Krisen zuständige Behörden (Behörden für das Cyberkrisenmanagement) oder richtet sie ein. Die Mitgliedstaaten stellen sicher, dass diese Behörden über angemessene Ressourcen verfügen, um die ihnen übertragenen Aufgaben wirksam und effizient ausführen zu können. Sie gewährleisten die Kohärenz mit den geltenden Rahmen für das allgemeine nationale Krisenmanagement.

(2) Benennt ein Mitgliedstaat mehr als eine Behörde für das Cyberkrisenmanagement im Sinne von Absatz 1 oder richtet mehr als eine solche zuständige Behörde ein, so gibt er eindeutig an, welche dieser zuständigen Behörden als Koordinator für das Management von Cybersicherheitsvorfällen großen Ausmaßes und Krisen fungiert.

(3) Jeder Mitgliedstaat ermittelt die Kapazitäten, Mittel und Verfahren, die im Fall einer Krise für die Zwecke dieser Richtlinie eingesetzt werden können.

(4) Jeder Mitgliedstaat verabschiedet einen nationalen Plan für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes und Krisen, in dem die Ziele und Modalitäten für das Management von Cybersicherheitsvorfällen großen Ausmaßes und Krisen festgelegt sind. In diesem Plan wird insbesondere Folgendes festgelegt:

a) die Ziele der nationalen Vorsorgenmaßnahmen und -tätigkeiten;

b) die Aufgaben und Zuständigkeiten der Behörden für das Cyberkrisenmanagement;

c) die Verfahren für das Cyberkrisenmanagement, einschließlich deren Integration in den nationalen Rahmen für das allgemeine Krisenmanagement, und die Kanäle für den Informationsaustausch;

d) die nationalen Vorsorgemaßnahmen, einschließlich Übungen und Ausbildungsmaßnahmen;

e) die einschlägigen öffentlichen und privaten Interessenträger und die betroffene Infrastruktur,

f) die zwischen den einschlägigen nationalen Behörden und Stellen vereinbarten nationalen Verfahren und Regelungen, die gewährleisten sollen, dass sich der Mitgliedstaat wirksam am koordinierten Management von Cybersicherheitsvorfällen großen Ausmaßes und Krisen auf Unionsebene beteiligen und dieses unterstützen kann.

(5) Spätestens drei Monate nach der Benennung oder Einrichtung der in Absatz 1 genannten Behörde für das Cyberkrisenmanagement meldet jeder Mitgliedstaat der Kommission die Identität seiner Behörde und eventueller späterer Änderungen daran. Die Mitgliedstaaten übermitteln der Kommission und dem Europäischen Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe) einschlägige die Anforderungen nach Absatz 4 betreffende Informationen über ihre nationalen Pläne für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes und Krisen innerhalb von drei Monaten nach dem Erlass dieser Pläne. Die Mitgliedstaaten können Informationen ausnehmen, wenn und soweit dies für ihre nationale Sicherheit erforderlich ist.

Artikel 10
Computer-Notfallteams (CSIRTs)

(1) Jeder Mitgliedstaat benennt ein oder mehrere CSIRTs oder richtet sie ein. Die CSIRTs können innerhalb einer zuständigen Behörde benannt oder eingerichtet werden. Die CSIRTs erfüllen die in Artikel 11 Absatz 1 festgelegten Anforderungen, decken mindestens die in den Anhängen I und II genannten Sektoren, Teilsektoren und Arten von Einrichtungen ab und sind für die Bewältigung von Sicherheitsvorfällen nach einem genau festgelegten Ablauf zuständig.

(2) Die Mitgliedstaaten gewährleisten, dass jedes CSIRT mit angemessenen Ressourcen ausgestattet ist, damit es seine in Artikel 11 Absatz 3 aufgeführten Aufgaben wirksam erfüllen kann.

(3) Die Mitgliedstaaten stellen sicher, dass jedes CSIRT über eine geeignete, sichere und belastbare Kommunikations- und Informationsinfrastruktur verfügt, über die es Informationen mit wesentlichen und wichtigen Einrichtungen und anderen einschlägigen Interessenträgern austauscht. Zu diesem Zweck stellen die Mitgliedstaaten sicher, dass jedes CSIRT zur Einführung sicherer Instrumente für den Informationsaustausch beiträgt.

(4) Die CSIRTs arbeiten mit sektorspezifischen oder sektorübergreifenden Gruppierungen wesentlicher und wichtiger Einrichtungen zusammen und tauschen mit diesen gemäß Artikel 29 gegebenenfalls einschlägige Informationen aus.

(5) Die CSIRTs nehmen an gemäß Artikel 19 organisierten Peer Reviews teil.

(6) Die Mitgliedstaaten stellen sicher, dass ihre CSIRTs in dem CSIRTs-Netzwerk wirksam, effizient und sicher zusammenarbeiten.

(7) Die CSIRTs können Kooperationsbeziehungen mit nationalen Computer-Notfallteams von Drittländern aufnehmen. Als Teil solcher Kooperationsbeziehungen erleichtern die Mitgliedstaaten den wirksamen, effizienten und sicheren Informationsaustausch mit diesen nationalen Computer-Notfallteams von Drittländern, wobei sie einschlägige Protokolle für den Informationsaustausch, einschließlich des Traffic Light Protocol, verwendet. Die CSIRTs können mit nationalen Computer-Notfallteams von Drittländern einschlägige Informationen, einschließlich personenbezogener Daten im Einklang mit dem Datenschutzrecht der Union, austauschen.

(8) Die CSIRTS können mit nationalen Computer-Notfallteams von Drittländern oder gleichwertigen Stellen von Drittländern kooperieren, insbesondere um Unterstützung im Bereich der Cybersicherheit zu leisten.

(9) Jeder Mitgliedstaat notifiziert der Kommission unverzüglich die Identität des CSIRT gemäß Absatz 1 und des als Koordinator gemäß Absatz 12 Absatz 1 benannten CSIRT, ihre jeweiligen Aufgaben in Bezug auf wesentliche und wichtige Einrichtungen sowie etwaige spätere Änderungen dieser Angaben.

(10) Die Mitgliedstaaten können die ENISA um Unterstützung bei der Einsetzung ihrer CSIRTs ersuchen.

Artikel 11
Anforderungen an die CSIRTs sowie technische Kapazitäten und Aufgaben der CSIRTs

(1) Die CSIRTs müssen den folgenden Anforderungen genügen:

a) Die CSIRTs sorgen für einen hohen Grad der Verfügbarkeit ihrer Kommunikationskanäle, indem sie punktuellen Ausfällen vorbeugen und mehrere Kanäle bereitstellen, damit sie jederzeit erreichbar bleiben und selbst mit anderen Kontakt aufnehmen können; sie legen die Kommunikationskanäle genau fest und machen sie den CSIRT-Nutzern und Kooperationspartnern bekannt;

b) die Räumlichkeiten der CSIRTs und die unterstützenden Informationssysteme werden an sicheren Standorten eingerichtet;

c) die CSIRTs müssen über ein geeignetes System zur Verwaltung und Weiterleitung von Anfragen verfügen, insbesondere um wirksame und effiziente Übergaben zu erleichtern;

d) die CSIRTs stellen die Vertraulichkeit und Vertrauenswürdigkeit ihrer Tätigkeiten sicher;

e) die CSIRTs müssen personell so ausgestattet sein, dass sie eine ständige Bereitschaft ihrer Dienste gewährleisten können, und sie müssen sicherstellen, dass ihr Personal entsprechend geschult ist;

f) die CSIRTs müssen über Redundanzsysteme und Ausweicharbeitsräume verfügen, um die Kontinuität ihrer Dienste sicherzustellen.

Die CSIRTs können sich an internationalen Kooperationsnetzen beteiligen.

(2) Die Mitgliedstaaten gewährleisten, dass ihre CSIRTs gemeinsam über die notwendigen technischen Fähigkeiten verfügen, damit sie ihre in Absatz 3 aufgeführten Aufgaben erfüllen können. Die Mitgliedstaaten stellen sicher, dass ihre CSIRTs mit ausreichenden Ressourcen ausgestattet sind, um für angemessene Personalausstattungen zu sorgen, damit die CSIRTs ihre technischen Fähigkeiten entwickeln können.

(3) Die CSIRTs haben folgende Aufgaben:

a) Überwachung und Analyse von Cyberbedrohungen, Schwachstellen und Sicherheitsvorfällen auf nationaler Ebene und auf Anfrage Bereitstellung von Unterstützung für betreffende wesentliche und wichtige Einrichtungen hinsichtlich der Überwachung ihrer Netz- und Informationssysteme in Echtzeit oder nahezu in Echtzeit;

b) Ausgabe von Frühwarnungen und Alarmmeldungen sowie Bekanntmachung und Weitergabe von Informationen über Cyberbedrohungen, Schwachstellen und Sicherheitsvorfälle an die wesentlichen und wichtigen Einrichtungen sowie an die

zuständigen Behörden und andere einschlägige Interessenträger, möglichst echtzeitnah;

c) Reaktion auf Sicherheitsvorfälle und gegebenenfalls Unterstützung der betreffenden wesentlichen und wichtigen Einrichtungen;

d) Erhebung und Analyse forensischer Daten sowie dynamische Analyse von Risiken und Sicherheitsvorfällen sowie Lagebeurteilung im Hinblick auf die Cybersicherheit;

e) auf Ersuchen einer wesentlichen oder wichtigen Einrichtung eine proaktive Überprüfung der Netz- und Informationssysteme der betreffenden Einrichtung auf Schwachstellen mit potenziell signifikanten Auswirkungen (Schwachstellenscan);

f) Beteiligung am CSIRTs-Netzwerk und — im Rahmen ihrer Kapazitäten und Kompetenzen — auf Gegenseitigkeit beruhende Unterstützung anderer Mitglieder des CSIRTs-Netzwerks auf deren Ersuchen.

g) gegebenenfalls die Wahrnehmung der Aufgabe eines Koordinators für die Zwecke einer koordinierten Offenlegung von Schwachstellen nach Artikel 12 Absatz 1;

h) Beitrag zum Einsatz sicherer Instrumente für den Informationsaustausch gemäß Artikel 10 Absatz 3.

CSIRTs können eine proaktive nicht intrusive Überprüfung öffentlich zugänglicher Netz- und Informationssysteme wesentlicher und wichtiger Einrichtungen durchführen. Eine solche Überprüfung wird durchgeführt, um anfällige oder unsicher konfigurierte Netz- und Informationssysteme zu ermitteln und die betreffenden Einrichtungen zu unterrichten. Eine solche Überprüfung darf keinerlei nachteilige Auswirkung auf das Funktionieren der Dienste der Einrichtung haben.

Bei der Durchführung der in Unterabsatz 1 genannten Aufgaben können die CSIRTs auf der Grundlage eines risikobasierten Ansatzes bestimmten Aufgaben Vorrang einräumen.

(4) Die CSIRTs bauen Kooperationsbeziehungen mit einschlägigen Interessenträgern des Privatsektors auf, um die Ziele dieser Richtlinie erreichen zu können.

(5) Zur Erleichterung der Zusammenarbeit nach Absatz 4 fördern die CSIRTs die Annahme und Anwendung gemeinsamer oder standardisierter Vorgehensweisen, Klassifizierungssysteme und Taxonomien für

a) Verfahren zur Bewältigung von Sicherheitsvorfällen,

b) das Krisenmanagement und

c) die koordinierte Offenlegung von Schwachstellen nach Artikel 12 Absatz 1.

Artikel 12
Koordinierte Offenlegung von Schwachstellen und eine europäische Schwachstellendatenbank

(1) Jeder Mitgliedstaat benennt eines seiner CSIRTs als Koordinator für die Zwecke einer koordinierten Offenlegung von Schwachstellen. Das als Koordinator benannte CSIRT fungiert als vertrauenswürdiger Vermittler und erleichtert erforderlichenfalls die Interaktion zwischen der eine Schwachstelle meldenden natürlichen oder juristischen Person und dem

Hersteller oder Anbieter der potenziell gefährdeten IKT-Produkte oder IKT-Dienste auf Ersuchen einer der beiden Seiten. Zu den Aufgaben des als Koordinator benannten CSIRT gehört insbesondere

a) betreffende Einrichtungen zu ermitteln und zu kontaktieren,

b) die natürlichen oder juristischen Personen, die eine Schwachstelle melden, zu unterstützen, und

c) Zeitpläne für die Offenlegung auszuhandeln und das Vorgehen bei Schwachstellen zu koordinieren, die mehrere Einrichtungen betreffen.

Die Mitgliedstaaten stellen sicher, dass natürliche oder juristische Personen dem als Koordinator benannten CSIRT eine Schwachstelle, auf Wunsch anonym, melden können. Das als Koordinator benannte CSIRT stellt sicher, dass in Bezug auf die gemeldete Schwachstelle sorgfältige Folgemaßnahmen durchgeführt werden, und sorgen für die Anonymität der die Schwachstelle meldenden natürlichen oder juristischen Person. Wenn die gemeldete Schwachstelle erhebliche Auswirkungen auf Einrichtungen in mehreren Mitgliedstaaten haben könnte, arbeitet das als Koordinator benannte CSIRT jedes betreffenden Mitgliedstaats gegebenenfalls mit den anderen als Koordinatoren benannten CSIRTs innerhalb des CSIRTs-Netzwerks zusammen.

(2) Die ENISA entwickelt und pflegt nach Absprache mit der Kooperationsgruppe eine europäische Schwachstellendatenbank. Zu diesem Zweck führt die ENISA geeignete Informationssysteme, Konzepte und Verfahren ein, pflegt diese und trifft die erforderlichen technischen und organisatorischen Maßnahmen, um die Sicherheit und Integrität der europäischen Schwachstellendatenbank zu gewährleisten, damit insbesondere Einrichtungen, unabhängig davon, ob sie in den Anwendungsbereich dieser Richtlinie fallen, und deren Anbieter von Netz- und Informationssystemen auf freiwilliger Basis öffentlich bekannte Schwachstellen in IKT-Produkten oder -Diensten offenlegen und registrieren können. Allen Interessenträgern wird Zugang zu den Informationen über die Schwachstellen gewährt, die in der europäischen Schwachstellendatenbank enthalten sind. Diese Datenbank umfasst Folgendes:

a) Informationen zur Beschreibung der Schwachstelle,

b) die betroffenen IKT-Produkte oder IKT-Dienste und das Ausmaß der Schwachstelle im Hinblick auf die Umstände, unter denen sie ausgenutzt werden kann,

c) die Verfügbarkeit entsprechender Patches und bei Nichtverfügbarkeit von Patches von den zuständigen Behörden oder den CSIRTs bereitgestellte Orientierungshilfen für die Nutzer gefährdeter IKT-Produkte und IKT-Dienste, wie die von offengelegten Schwachstellen ausgehenden Risiken gemindert werden können.

Artikel 13
Zusammenarbeit auf nationaler Ebene

(1) Handelt es sich bei den zuständigen Behörden, der zentralen Anlaufstelle und den CSIRTs eines Mitgliedstaats um getrennte Einrichtungen, so arbeiten sie bei der Erfüllung der in dieser Richtlinie festgelegten Pflichten zusammen.

(2) Die Mitgliedstaaten stellen sicher, dass Meldungen von erheblichen Sicherheitsvorfällen gemäß Artikel 23 und Sicherheitsvorfällen, Cyberbedrohungen und Beinahe-Vorfällen ge-

mäß Artikel 30 ihren CSIRTs oder gegebenenfalls ihren zuständigen Behörden übermittelt werden.

(3) Die Mitgliedstaaten stellen sicher, dass ihre CSIRTs oder gegebenenfalls zuständigen Behörden ihre zentralen Anlaufstellen über gemäß dieser Richtlinie vorgenommene Meldungen von Sicherheitsvorfällen, Cyberbedrohungen und Beinahe-Vorfällen unterrichten.

(4) Damit die Aufgaben und Pflichten der zuständigen Behörden, zentralen Anlaufstellen und CSIRTs wirksam erfüllt werden, sorgen die Mitgliedstaaten so weit wie möglich für eine angemessene Zusammenarbeit zwischen diesen Stellen und den Strafverfolgungsbehörden, den Datenschutzbehörden, den nationalen Behörden gemäß den Verordnungen (EG) Nr. 300/2008 und (EU) 2018/1139, den Aufsichtsstellen gemäß der Verordnung (EU) Nr. 910/2014, den gemäß der Verordnung (EU) 2022/2554 zuständigen Behörden, den nationalen Regulierungsbehörden gemäß der Richtlinie (EU) 2018/1972, den gemäß der Richtlinie (EU) 2022/2557 zuständigen Behörden sowie im Rahmen anderer sektorspezifischer Rechtsakte der Union innerhalb des jeweiligen Mitgliedstaats zuständiger Behörden.

(5) Die Mitgliedstaaten stellen sicher, dass ihre im Rahmen dieser Richtlinie zuständigen Behörden und ihre nach der Richtlinie (EU) 2022/2557 zuständigen Behörden regelmäßig hinsichtlich der Identifizierung kritischer Einrichtungen zu Risiken, Cyberbedrohungen und Sicherheitsvorfällen sowie zu nicht cyberbezogenen Risiken, Bedrohungen und Sicherheitsvorfällen, die als kritische Einrichtungen im Sinne der Richtlinie (EU) 2022/2557 ermittelte wesentliche Einrichtungen betreffen, und zu den als Reaktion auf diese Risiken, Bedrohungen und Sicherheitsvorfälle ergriffenen Maßnahmen zusammenarbeiten und darüber Informationen austauschen. Die Mitgliedstaaten stellen ferner sicher, dass ihre im Rahmen dieser Richtlinie zuständigen Behörden und ihre nach der Verordnung (EU) Nr. 910/2014, der Verordnung (EU) 2022/2554 und der Richtlinie (EU) 2018/1972 zuständigen Behörden regelmäßig einschlägige Informationen austauschen, auch in Bezug auf einschlägige Sicherheitsvorfälle und Cyberbedrohungen.

(6) Die Mitgliedstaaten vereinfachen die Berichterstattung über die in den Artikeln 23 und 30 genannten technischen Mittel für Notifizierungen.

KAPITEL III
ZUSAMMENARBEIT AUF UNIONS- UND INTERNATIONALER EBENE

Artikel 14
Kooperationsgruppe

(1) Zur Unterstützung und Erleichterung der strategischen Zusammenarbeit und des Informationsaustauschs zwischen den Mitgliedstaaten und zur Stärkung des Vertrauens wird eine Kooperationsgruppe eingesetzt.

(2) Die Kooperationsgruppe nimmt ihre Aufgaben auf der Grundlage von zweijährlichen Arbeitsprogrammen gemäß Absatz 7 wahr.

(3) Die Kooperationsgruppe setzt sich aus Vertretern der Mitgliedstaaten, der Kommission und der ENISA zusammen. Der Europäische Auswärtige Dienst nimmt an den Tätigkeiten der Kooperationsgruppe als Beobachter teil. Die Europäischen Aufsichtsbehörden (ESAs) und die nach der Verordnung (EU) 2022/2554 zuständigen Behörden können sich gemäß

Artikel 47 Absatz 1 jener Verordnung an den Tätigkeiten der Kooperationsgruppe beteiligen.

Gegebenenfalls kann die Kooperationsgruppe das Europäische Parlament und Vertreter der maßgeblichen Interessenträger einladen, an ihren Arbeiten teilzunehmen.

Die Sekretariatsgeschäfte werden von der Kommission geführt.

(4) Die Kooperationsgruppe hat folgende Aufgaben:

a) Bereitstellung von Orientierungshilfen für die zuständigen Behörden in Bezug auf die Umsetzung und Durchführung dieser Richtlinie;

b) Bereitstellung von Orientierungshilfen für die zuständigen Behörden in Bezug auf die Ausarbeitung und Durchführung von Maßnahmen zur koordinierten Offenlegung von Schwachstellen gemäß Artikel 7 Absatz 2 Buchstabe c;

c) Austausch bewährter Verfahren und Informationsaustausch im Zusammenhang mit der Durchführung dieser Richtlinie, auch in Bezug auf Cyberbedrohungen, Sicherheitsvorfälle, Schwachstellen, Beinahe-Vorfälle, Sensibilisierungsinitiativen, Schulungen, Übungen und Kompetenzen, Kapazitätsaufbau, Normen und technische Spezifikationen sowie Bestimmung wesentlicher und wichtiger Einrichtungen gemäß Artikel 2 Absatz 2 Buchstaben b bis e;

d) beratender Austausch und Zusammenarbeit mit der Kommission in Bezug auf neue politische Initiativen im Bereich der Cybersicherheit und die allgemeine Kohärenz der sektorspezifischen Anforderungen an die Cybersicherheit;

e) beratender Austausch und Zusammenarbeit mit der Kommission bei Entwürfen von delegierten Rechtsakten oder Durchführungsrechtsakten, die gemäß dieser Richtlinie erlassen werden;

f) Austausch bewährter Verfahren und Informationsaustausch mit den einschlägigen Organen, Einrichtungen und sonstigen Stellen der Union;

g) Meinungsaustausch über die Durchführung sektorspezifischer Rechtsakte der Union, die Vorschriften über Cybersicherheit enthalten;

h) gegebenenfalls Erörterung von Berichten über die in Artikel 19 Absatz 9 genannten Peer-Reviews und Ausarbeitung von Schlussfolgerungen und Empfehlungen;

i) Durchführung koordinierter Risikobewertungen kritischer Lieferketten gemäß Artikel 22 Absatz 1;

j) Erörterung von Fällen von Amtshilfe, einschließlich Erfahrungen und Ergebnisse gemeinsamer Aufsichtstätigkeiten in grenzübergreifenden Fällen gemäß Artikel 37;

k) auf Ersuchen eines oder mehrerer betreffender Mitgliedstaaten Erörterung spezifischer Amtshilfeersuchen gemäß Artikel 37;

l) Bereitstellung strategischer Orientierungshilfen für das CSIRTs-Netzwerk und das EU-CyCLONe zu spezifischen neu auftretenden Fragen;

m) Meinungsaustausch über das Konzept von Folgemaßnahmen im Anschluss an Cybersicherheitsvorfälle großen Ausmaßes und Krisen auf der Grundlage von im CSIRTs-Netzwerk und im EU-CyCLONe gewonnenen Erkenntnissen;

n) Beitrag zu den Cybersicherheitsfähigkeiten in der gesamten Union durch Erleichterung des Austauschs nationaler Bediensteter im Rahmen eines Programms zum Kapazitätsaufbau, an dem sich Mitarbeiter der zuständigen Behörden oder der CSIRTs beteiligen;

o) Organisation regelmäßiger gemeinsamer Sitzungen mit einschlägigen privaten Interessenträgern aus der gesamten Union, um die Tätigkeiten der Kooperationsgruppe zu erörtern und Beiträge zu neuen politischen Herausforderungen einzuholen;

p) Erörterung der Arbeiten im Zusammenhang mit Cybersicherheitsübungen, einschließlich der Arbeit der ENISA;

q) Festlegung der Methode und der organisatorischen Aspekte der Peer Reviews gemäß Artikel 19 Absatz 1 sowie Festlegung der Selbstbewertungsmethode für die Mitgliedstaaten gemäß Artikel 19 Absatz 5 mit der Unterstützung der Kommission und der ENISA und Entwicklung von Verhaltenskodizes zur Untermauerung der Arbeitsmethoden benannter Sachverständiger für Cybersicherheit gemäß Artikel 19 Absatz 6 in Zusammenarbeit mit der Kommission und der ENISA;

r) Ausarbeitung von Berichten über die auf strategischer Ebene und in den Peer Reviews gewonnenen Erfahrungen zum Zwecke der Überprüfung gemäß Artikel 40;

s) Erörterung und regelmäßige Bewertung des aktuellen Stands in Bezug auf Cyberbedrohungen oder Sicherheitsvorfälle wie Ransomware.

Die Kooperationsgruppe unterbreitet die in Unterabsatz 1 Buchstabe r genannten Berichte der Kommission, dem Europäischen Parlament und dem Rat.

(5) Die Mitgliedstaaten stellen eine wirksame, effiziente und sichere Zusammenarbeit ihrer Vertreter in der Kooperationsgruppe sicher.

(6) Die Kooperationsgruppe kann das CSIRTs-Netzwerk um einen technischen Bericht zu ausgewählten Themen ersuchen.

(7) Bis spätestens 1. Februar 2024 und danach alle zwei Jahre erstellt die Kooperationsgruppe ein Arbeitsprogramm bezüglich der Maßnahmen, die zur Umsetzung ihrer Ziele und Aufgaben zu ergreifen sind.

(8) Die Kommission kann Durchführungsrechtsakte zur Festlegung der Verfahrensmodalitäten erlassen, die für das Funktionieren der Kooperationsgruppe erforderlich sind.

Diese Durchführungsrechtsakte werden gemäß dem in Artikel 39 Absatz 2 genannten Prüfverfahren erlassen.

Die Kommission tauscht sich mit der Kooperationsgruppe gemäß Absatz 4 Buchstabe e über die in den Unterabsatz 1 dieses Absatzes genannten Entwürfe von Durchführungsrechtsakten aus und arbeitet mit ihr zusammen.

(9) Die Kooperationsgruppe tagt regelmäßig und in jedem Fall mindestens einmal jährlich gemeinsam mit der mit der Richtlinie (EU) 2022/2557 eingerichteten Gruppe für die Resilienz kritischer Einrichtungen, um die strategische Zusammenarbeit und den Informationsaustausch zu fördern und zu erleichtern.

Artikel 15
CSIRTs-Netzwerk

(1) Um zum Aufbau von Vertrauen zwischen den Mitgliedstaaten beizutragen und eine rasche und wirksame operative Zusammenarbeit zwischen ihnen zu fördern, wird ein Netzwerk nationaler CSIRTs errichtet.

(2) Das CSIRTs-Netzwerk setzt sich aus Vertretern der gemäß Artikel 10 benannten oder eingerichteten CSIRTs der Mitgliedstaaten und des IT-Notfallteams für die Organe, Einrichtungen und sonstigen Stellen der Union (CERT-EU) zusammen. Die Kommission nimmt als Beobachterin am CSIRTs-Netzwerk teil. Die ENISA führt die Sekretariatsgeschäfte und leistet aktive Unterstützung für die Zusammenarbeit zwischen den CSIRTs.

(3) Das CSIRTs-Netzwerk hat folgende Aufgaben:

a) Informationsaustausch zu den Kapazitäten der CSIRTs;

b) Erleichterung der gemeinsamen Nutzung, des Transfers und des Austauschs von Technologie sowie relevanten Maßnahmen, Strategien, Instrumenten, Abläufen, bewährten Verfahren und Rahmenbedingungen zwischen den CSIRTs;

c) Austausch relevanter Informationen über Sicherheitsvorfälle, Beinahe-Vorfälle, Cyberbedrohungen, Risiken und Schwachstellen;

d) Austausch von Informationen über Veröffentlichungen und Empfehlungen im Bereich Cybersicherheit;

e) Sicherstellung der Interoperabilität in Bezug auf Spezifikationen und Protokolle für den Informationsaustausch;

f) auf Antrag eines potenziell von einem Sicherheitsvorfall betroffenen Mitglieds des CSIRTs-Netzwerks Austausch und Erörterung von Informationen über diesen Sicherheitsvorfall und die damit verbundenen Cyberbedrohungen, Risiken und Schwachstellen;

g) auf Antrag eines Mitglieds des CSIRTs-Netzwerks Erörterung und, sofern möglich, Umsetzung einer koordinierten Reaktion auf einen Sicherheitsvorfall, der im Gebiet seines Mitgliedstaats festgestellt wurde;

h) Unterstützung der Mitgliedstaaten bei der Bewältigung grenzübergreifender Sicherheitsvorfälle gemäß dieser Richtlinie;

i) Zusammenarbeit, Austausch bewährter Verfahren und Unterstützung der gemäß Artikel 12 Absatz 1 als Koordinatoren benannten CSIRTs im Hinblick auf die Steuerung der koordinierten Offenlegung von Schwachstellen, die erhebliche Auswirkungen auf Einrichtungen in mehreren Mitgliedstaaten nach sich ziehen könnten;

j) Erörterung und Bestimmung weiterer Formen der operativen Zusammenarbeit, unter anderem im Zusammenhang mit

   i) Kategorien von Cyberbedrohungen und Sicherheitsvorfällen,

   ii) Frühwarnungen,

   iii) gegenseitiger Unterstützung,

iv) Grundsätzen und Modalitäten der Koordinierung bei der Reaktion auf grenzüberschreitende Risiken und Sicherheitsvorfälle,

v) dem auf Ersuchen eines Mitgliedstaats erfolgenden Beitrag zum nationalen Plan für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes und Krisen gemäß Artikel 9 Absatz 4;

k) Unterrichtung der Kooperationsgruppe über seine Tätigkeiten und über die gemäß Buchstabe j erörterten weiteren Formen der operativen Zusammenarbeit und gegebenenfalls Ersuchen um Orientierungshilfen dafür;

l) Berücksichtigung von Erkenntnissen aus Cybersicherheitsübungen, einschließlich der von der ENISA organisierten Übungen;

m) auf Antrag eines einzelnen CSIRT Erörterung der Kapazitäten und der Vorsorge dieses CSIRT;

n) Zusammenarbeit und Informationsaustausch mit regionalen und unionsweiten Sicherheitsbetriebszentren (Security Operations Centres), um die gemeinsame Lageerfassung bei Sicherheitsvorfällen und Cyberbedrohungen in der gesamten Union zu verbessern;

o) gegebenenfalls Erörterung der in Artikel 19 Absatz 9 genannten Peer Reviews;

p) Bereitstellung von Leitlinien zur Erleichterung der Konvergenz der operativen Verfahrensweisen in Bezug auf die Anwendung der die operative Zusammenarbeit betreffenden Bestimmungen dieses Artikels.

(4) Bis zum 17. Januar 2025 und danach alle zwei Jahre bewertet das CSIRTs-Netzwerk zum Zwecke der in Artikel 40 genannten Überprüfung den bei der operativen Zusammenarbeit erzielten Fortschritt und nimmt einen Bericht an. Der Bericht enthält insbesondere Schlussfolgerungen und Empfehlungen auf der Grundlage der Peer Reviews gemäß Artikel 19, die in Bezug auf nationale CSIRTs durchgeführt werden. Dieser Bericht wird der Kooperationsgruppe übermittelt.

(5) Das CSIRTs-Netzwerk gibt sich eine Geschäftsordnung.

(6) Das CSIRTs-Netzwerk und das EU-CyCLONe einigen sich auf Verfahrensregeln und arbeiten auf deren Grundlage zusammen.

Artikel 16
Das Europäische Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe)

(1) Zur Unterstützung des koordinierten Managements von Cybersicherheitsvorfällen großen Ausmaßes und Krisen auf operativer Ebene und zur Gewährleistung eines regelmäßigen Austauschs relevanter Informationen zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der Union wird das Europäische Netzwerk der Verbindungsorganisationen für Cyberkrisen (European Cyber Crises Liaison Organisation Network, EU-CyCLONe) eingerichtet.

(2) EU-CyCLONe setzt sich aus den Vertretern der Behörden der Mitgliedstaaten für das Cyberkrisenmanagement sowie in Fällen, in denen ein potenzieller oder andauernder Cybersicherheitsvorfall großen Ausmaßes erhebliche Auswirkungen auf unter den Anwen-

dungsbereich dieser Richtlinie fallende Dienste und Tätigkeiten hat oder wahrscheinlich haben wird, der Kommission zusammen. In anderen Fällen nimmt die Kommission als Beobachterin an den Tätigkeiten des EU-CyCLONe teil.

Die ENISA führt die Sekretariatsgeschäfte des EU-CyCLONe, unterstützt den sicheren Informationsaustausch und stellt die Instrumente bereit, die für die Förderung der Zusammenarbeit zwischen den Mitgliedstaaten zur Gewährleistung eines sicheren Informationsaustauschs erforderlich sind.

Gegebenenfalls kann das EU-CyCLONe Vertreter der maßgeblichen Interessenträger einladen, an seinen Arbeiten als Beobachter teilzunehmen.

(3) Das EU-CyCLONe hat folgende Aufgaben:

a) Verbesserung der Vorsorge im Hinblick auf das Management von Cybersicherheitsvorfällen großen Ausmaßes und Krisen;

b) Entwicklung einer gemeinsamen Lageerfassung für Cybersicherheitsvorfälle großen Ausmaßes und Krisen;

c) Bewertung der Folgen und Auswirkungen relevanter Cybersicherheitsvorfälle großen Ausmaßes und Krisen und Vorschläge für mögliche Abhilfemaßnahmen;

d) Koordinierung des Managements von Cybersicherheitsvorfällen großen Ausmaßes und Krisen sowie Unterstützung der Entscheidungsfindung auf politischer Ebene in Bezug auf solche Sicherheitsvorfälle und Krisen;

e) auf Ersuchen eines betreffenden Mitgliedstaats die Erörterung nationaler Pläne für die Reaktion auf Cybersicherheitsvorfälle großen Ausmaßes und Krisen gemäß Artikel 9 Absatz 4.

f) (4) Das EU-CyCLONe gibt sich eine Geschäftsordnung.

(5) Das EU-CyCLONe erstattet der Kooperationsgruppe regelmäßig Bericht über das Management von Cybersicherheitsvorfällen großen Ausmaßes und Krisen sowie Trends, wobei der Schwerpunkt insbesondere auf deren Auswirkungen auf wesentliche und wichtige Einrichtungen liegt.

(6) Das EU-CyCLONe arbeitet auf der Grundlage vereinbarter Verfahrensmodalitäten gemäß Artikel 15 Absatz 6 mit dem CSIRTs-Netzwerk zusammen.

(7) Bis zum 17. Juli 2024 und danach alle 18 Monate unterbreitet das EU-CyCLONe dem Europäischen Parlament und dem Rat einen Bericht, in dem es seine Arbeit bewertet.

Artikel 17
Internationale Zusammenarbeit

Die Union kann gegebenenfalls internationale Übereinkünfte mit Drittländern oder internationalen Organisationen im Einklang mit Artikel 218 AEUV schließen, in denen deren Beteiligung an bestimmten Tätigkeiten der Kooperationsgruppe, dem CSIRTs-Netzwerk und dem EU-CyCLONe ermöglicht und geregelt wird. Solche Übereinkünfte müssen mit dem Datenschutzrecht der Union im Einklang stehen.

Artikel 18
Bericht über den Stand der Cybersicherheit in der Union

(1) Die ENISA nimmt in Zusammenarbeit mit der Kommission und der Kooperationsgruppe einen zweijährlichen Bericht über den Stand der Cybersicherheit in der Union an und legt diesen Bericht dem Europäischen Parlament vor. Dieser Bericht wird unter anderem in maschinenlesbaren Daten zur Verfügung gestellt und muss Folgendes enthalten:

a) eine Bewertung der Cybersicherheitsrisiken auf Unionsebene unter Berücksichtigung der Cyberbedrohungslandschaft;

b) eine Bewertung der Entwicklung von Cybersicherheitskapazitäten im öffentlichen und im privaten Sektor in der gesamten Union;

c) eine Bewertung des allgemeinen Grads der Sensibilisierung für Cybersicherheit und der Cyberhygiene bei Bürgerinnen und Bürgern und Einrichtungen, einschließlich kleiner und mittlerer Unternehmen;

d) eine aggregierte Bewertung der Ergebnisse der Peer Reviews gemäß Artikel 19;

e) eine aggregierte Bewertung des Entwicklungsstands der Cybersicherheitskapazitäten und -ressourcen in der gesamten Union, einschließlich derjenigen auf Sektorenebene, sowie des Ausmaßes, in dem die nationalen Cybersicherheitsstrategien der Mitgliedstaaten aufeinander abgestimmt sind.

(2) Der Bericht muss insbesondere politische Empfehlungen zur Behebung von Mängeln und Erhöhung des Cybersicherheitsniveaus in der gesamten Union und eine Zusammenfassung der Ergebnisse der von der ENISA gemäß Artikel 7 Absatz 6 der Verordnung (EU) 2019/881 für den entsprechenden Zeitraum erstellten technischen EU-Cybersicherheitslageberichte über Sicherheitsvorfälle und Cyberbedrohungen umfassen.

(3) Die ENISA entwickelt in Zusammenarbeit mit der Kommission, der Kooperationsgruppe und dem CSIRTs-Netzwerk die Methodik, einschließlich der einschlägigen Variablen wie quantitativer und qualitativer Indikatoren, für die in Absatz 1 Buchstabe e genannte aggregierte Bewertung.

Artikel 19
Peer Reviews

(1) Die Kooperationsgruppe wird bis zum 17. Januar 2025 mit Unterstützung der Kommission und der ENISA und gegebenenfalls des CSIRTs-Netzwerks die Methode und die organisatorischen Aspekte der Peer Reviews festlegen, um aus gemeinsamen Erfahrungen zu lernen, das gegenseitige Vertrauen zu stärken, ein hohes gemeinsames Cybersicherheitsniveau zu erreichen und die für die Umsetzung dieser Richtlinie erforderlichen Cybersicherheitsfähigkeiten und -konzepte der Mitgliedstaaten zu verbessern. Die Teilnahme an Peer Reviews ist freiwillig. Die Peer Reviews werden von Sachverständigen für Cybersicherheit durchgeführt. Die Sachverständigen für Cybersicherheit werden von mindestens zwei Mitgliedstaaten benannt, die sich von dem überprüften Mitgliedstaat unterscheiden.

Die Peer Reviews erstrecken sich mindestens auf einen der folgenden Punkte:

a) den Stand der Umsetzung der Maßnahmen bezüglich Cybersicherheitsrisikomanagement und der Berichtspflichten gemäß den Artikeln 21 und 23;

b) das Niveau der Kapazitäten, einschließlich der verfügbaren finanziellen, technischen und personellen Ressourcen, und die Wirksamkeit bei der Durchführung der Aufgaben der zuständigen Behörden;

c) die operativen Kapazitäten der CSIRTs;

d) den Stand der Umsetzung der Amtshilfe gemäß Artikel 37;

e) den Stand der Umsetzung der Vereinbarungen über den Austausch von Informationen im Bereich der Cybersicherheit gemäß Artikel 29;

f) spezifische Fragen mit grenz- oder sektorenübergreifendem Charakter.

(2) Die Methode muss gemäß Absatz 1 objektive, nichtdiskriminierende, faire und transparente Kriterien umfassen, anhand deren die Mitgliedstaaten Sachverständige für Cybersicherheit benennen, die für die Durchführung der Peer Reviews infrage kommen. Die ENISA und die Kommission nehmen als Beobachter an den Peer Reviews teil.

(3) Die Mitgliedstaaten können spezifische, in Absatz 1 Buchstabe f genannte Probleme für eine Peer Review ermitteln.

(4) Vor Beginn der Peer Review nach Absatz 1 teilen Mitgliedstaaten den teilnehmenden Mitgliedstaaten ihren Umfang, einschließlich der gemäß Absatz 3 ermittelten Probleme, mit.

(5) Vor Beginn der Peer Review können die Mitgliedstaaten eine Selbstbewertung der überprüften Aspekte vornehmen und diese Selbstbewertung den benannten Sachverständigen für Cybersicherheit vorlegen. Die Kooperationsgruppe legt mit Unterstützung der Kommission und der ENISA die Methode für die Selbstbewertung der Mitgliedstaaten fest.

(6) Die Peer Reviews umfassen physische oder virtuelle Besuche am Standort sowie abseits des Standorts den Austausch von Informationen. Im Einklang mit dem Grundsatz der guten Zusammenarbeit stellt der Mitgliedstaat, der Gegenstand der Peer Review ist, den benannten Sachverständigen für Cybersicherheit die für die Bewertung erforderlichen Informationen zur Verfügung, vorbehaltlich der Rechtsvorschriften der Union oder der Mitgliedstaaten über den Schutz vertraulicher oder als Verschlusssache eingestufter Informationen und der Wahrung grundlegender Funktionen des Staates wie der nationalen Sicherheit. Die Kooperationsgruppe entwickelt in Zusammenarbeit mit der Kommission und der ENISA geeignete Verhaltenskodizes zur Untermauerung der Arbeitsmethoden der benannten Sachverständigen für Cybersicherheit. Sämtliche durch die Peer Review erlangten Informationen dürfen nur zu diesem Zweck verwendet werden. Die an der Peer Review beteiligten Sachverständigen für Cybersicherheit geben keine sensiblen oder vertraulichen Informationen, die im Laufe der Peer Review erlangt wurden, an Dritte weiter.

(7) Nachdem sie einer Peer Review unterzogen wurden, dürfen innerhalb von zwei Jahren nach Abschluss der Peer Review in diesem Mitgliedstaat keine weiteren Peer Reviews zu denselben Aspekten, die in einem Mitgliedstaat überprüft wurden, durchgeführt werden, es sei denn, der Mitgliedstaat beantragt etwas anderes oder es wird auf Vorschlag der Kooperationsgruppe etwas anderes vereinbart.

(8) Die Mitgliedstaaten stellen sicher, dass jegliches Risiko eines Interessenkonflikts im Zusammenhang mit den benannten Sachverständigen für Cybersicherheit den anderen Mitgliedstaaten, der Kooperationsgruppe, der Kommission und der ENISA vor Beginn der Peer Review offengelegt wird. Der Mitgliedstaat, der Gegenstand der Peer Review ist, kann Ein-

wände gegen die Benennung bestimmter Sachverständiger für Cybersicherheit erheben, wenn er dem benennenden Mitgliedstaat stichhaltige Gründe mitteilt.

(9) Die an Peer Reviews beteiligten Sachverständigen für Cybersicherheit erstellen Berichte über die Ergebnisse und Schlussfolgerungen der Peer Reviews. Die einer Peer Review unterliegenden Mitgliedstaaten können zu den sie betreffenden Berichtsentwürfen Stellung nehmen; diese Stellungnahmen werden den Berichten beigefügt. Die Berichte enthalten Empfehlungen zur Verbesserung der im Rahmen der Peer Review behandelten Aspekte. Die Berichte werden gegebenenfalls der Kooperationsgruppe und dem CSIRTs-Netzwerk vorgelegt. Ein einer Peer Review unterliegender Mitgliedstaat kann beschließen, seinen Bericht oder eine redigierte Fassung davon öffentlich zugänglich zu machen.

KAPITEL IV
RISIKOMANAGEMENTMAßNAHMEN UND BERICHTSPFLICHTEN IM BEREICH DER CYBERSICHERHEIT

Artikel 20
Governance

(1) Die Mitgliedstaaten stellen sicher, dass die Leitungsorgane wesentlicher und wichtiger Einrichtungen die von diesen Einrichtungen zur Einhaltung von Artikel 21 ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit billigen, ihre Umsetzung überwachen und für Verstöße gegen diesen Artikel durch die betreffenden Einrichtungen verantwortlich gemacht werden können.

Die Anwendung dieses Absatzes lässt die nationalen Rechtsvorschriften in Bezug auf die für die öffentlichen Einrichtungen geltenden Haftungsregelungen sowie die Haftung von öffentlichen Bediensteten und gewählten oder ernannten Amtsträgern unberührt.

(2) Die Mitgliedstaaten stellen sicher, dass die Mitglieder der Leitungsorgane wesentlicher und wichtiger Einrichtungen an Schulungen teilnehmen müssen, und fordern wesentliche und wichtige Einrichtungen auf, allen Mitarbeitern regelmäßig entsprechende Schulungen anzubieten, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.

Artikel 21
Risikomanagementmaßnahmen im Bereich der Cybersicherheit

(1) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die Risiken für die Sicherheit der Netz- und Informationssysteme, die diese Einrichtungen für ihren Betrieb oder für die Erbringung ihrer Dienste nutzen, zu beherrschen und die Auswirkungen von Sicherheitsvorfällen auf die Empfänger ihrer Dienste und auf andere Dienste zu verhindern oder möglichst gering zu halten.

Die in Unterabsatz 1 genannten Maßnahmen müssen unter Berücksichtigung des Stands der Technik und gegebenenfalls der einschlägigen europäischen und internationalen Normen sowie der Kosten der Umsetzung ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist. Bei der Bewertung der Verhältnismäßigkeit dieser Maßnahmen sind das Ausmaß der Risikoexposition der Einrichtung,

die Größe der Einrichtung und die Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen, gebührend zu berücksichtigen.

(2) Die in Absatz 1 genannten Maßnahmen müssen auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen, und zumindest Folgendes umfassen:

a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;

b) Bewältigung von Sicherheitsvorfällen;

c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;

d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;

e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;

f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;

g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;

h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;

i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;

j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

(3) Die Mitgliedstaaten stellen sicher, dass die Einrichtungen bei der Erwägung geeigneter Maßnahmen nach Absatz 2 Buchstabe d des vorliegenden Artikels die spezifischen Schwachstellen der einzelnen unmittelbaren Anbieter und Diensteanbieter sowie die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse, berücksichtigen. Die Mitgliedstaaten stellen ferner sicher, dass die Einrichtungen bei der Erwägung geeigneter Maßnahmen nach jenem Buchstaben die Ergebnisse der gemäß Artikel 22 Absatz 1 durchgeführten koordinierten Risikobewertungen in Bezug auf die Sicherheit kritischer Lieferketten berücksichtigen müssen.

(4) Die Mitgliedstaaten stellen sicher, dass eine Einrichtung, die feststellt, dass sie den in Absatz 2 genannten Maßnahmen nicht nachkommt, unverzüglich alle erforderlichen, angemessenen und verhältnismäßigen Korrekturmaßnahmen ergreift.

(5) Bis zum 17. Oktober 2024 erlässt die Kommission Durchführungsrechtsakte zur Festlegung der technischen und methodischen Anforderungen an die in Absatz 2 genannten Maßnahmen in Bezug auf DNS-Diensteanbieter, TLD-Namenregister, Cloud-Computing-Dienstleister, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter.

Die Kommission kann Durchführungsrechtsakte erlassen, in denen die technischen und methodischen Anforderungen sowie erforderlichenfalls die sektoralen Anforderungen der in Absatz 2 genannten Maßnahmen in Bezug auf andere als die in Unterabsatz 1 des vorliegenden Absatzes genannten wesentlichen und wichtigen Einrichtungen festgelegt werden.

Bei der Ausarbeitung der in den Unterabsätzen 1 und 2 des vorliegenden Absatzes genannten Durchführungsrechtsakte orientiert sich die Kommission so weit wie möglich an europäischen und internationalen Normen sowie einschlägigen technischen Spezifikationen. Die Kommission tauscht sich mit der Kooperationsgruppe und der ENISA über die Entwürfe von Durchführungsrechtsakten gemäß Artikel 14 Absatz 4 Buchstabe e aus und arbeitet mit ihnen zusammen.

Diese Durchführungsrechtsakte werden gemäß dem in Artikel 39 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 22
Koordinierte Risikobewertungen in Bezug auf die Sicherheit kritischer Lieferketten auf Ebene der Union

(1) Die Kooperationsgruppe kann in Zusammenarbeit mit der Kommission und der ENISA koordinierte Risikobewertungen in Bezug auf die Sicherheit der Lieferketten bestimmter kritischer IKT-Dienste, -Systeme oder -Produkte unter Berücksichtigung technischer und erforderlichenfalls nichttechnischer Risikofaktoren durchführen.

(2) Die Kommission legt nach Konsultation der Kooperationsgruppe und der ENISA sowie gegebenenfalls einschlägiger Interessenträger fest, welche spezifischen kritischen IKT-Dienste, -Systeme oder -Produkte der koordinierten Risikobewertung in Bezug auf die Sicherheit nach Absatz 1 unterzogen werden können

Artikel 23
Berichtspflichten

(1) Jeder Mitgliedstaat stellt sicher, dass wesentliche und wichtige Einrichtungen ihrem CSIRT oder gegebenenfalls ihrer zuständigen Behörde gemäß Absatz 4 unverzüglich über jeden Sicherheitsvorfall unterrichten, der erhebliche Auswirkungen auf die Erbringung ihrer Dienste gemäß Absatz 3 (erheblicher Sicherheitsvorfall) hat. Gegebenenfalls unterrichten die betreffenden Einrichtungen die Empfänger ihrer Dienste unverzüglich über diese erheblichen Sicherheitsvorfälle, die die Erbringung des jeweiligen Dienstes beeinträchtigen könnten. Jeder Mitgliedstaat stellt sicher, dass diese Einrichtungen unter anderem alle Informationen übermitteln, die es dem CSIRT oder gegebenenfalls der zuständigen Behörde ermöglichen zu ermitteln, ob der Sicherheitsvorfall grenzübergreifende Auswirkungen hat. Mit der bloßen Meldung wird keine höhere Haftung der meldenden Einrichtung begründet.

Melden die betreffenden Einrichtungen der zuständigen Behörde einen erheblichen Sicherheitsvorfall gemäß Unterabsatz 1, so stellt der Mitgliedstaat sicher, dass diese zuständige Behörde die Meldung nach Eingang an das CSIRT weiterleitet.

Im Falle eines grenz- oder sektorenübergreifenden erheblichen Sicherheitsvorfalls stellen die Mitgliedstaaten sicher, dass ihre zentralen Anlaufstellen rechtzeitig einschlägige Informationen erhalten, die gemäß Absatz 4 gemeldet wurden.

(2) Gegebenenfalls stellen die Mitgliedstaaten sicher, dass wesentliche und wichtige Einrichtungen den potenziell von einer erheblichen Cyberbedrohung betroffenen Empfängern ihrer Dienste unverzüglich alle Maßnahmen oder Abhilfemaßnahmen mitteilen, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können. Die Einrichtungen informieren diese Empfänger gegebenenfalls auch über die erhebliche Cyberbedrohung selbst.

(3) Ein Sicherheitsvorfall gilt als erheblich, wenn

a) er schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann;

b) er andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.

(4) Die Mitgliedstaaten stellen sicher, dass die betreffenden Einrichtungen dem CSIRT oder gegebenenfalls der zuständigen Behörde für die Zwecke der Meldung nach Absatz 1 Folgendes übermitteln:

a) unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls, eine Frühwarnung, in der gegebenenfalls angegeben wird, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist oder grenzüberschreitende Auswirkungen haben könnte;

b) unverzüglich, in jedem Fall aber innerhalb von 72 Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls, eine Meldung über den Sicherheitsvorfall, in der gegebenenfalls die unter Buchstabe a genannten Informationen aktualisiert werden und eine erste Bewertung des erheblichen Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, sowie gegebenenfalls die Kompromittierungsindikatoren angegeben werden;

c) auf Ersuchen eines CSIRT oder gegebenenfalls der zuständigen Behörde einen Zwischenbericht über relevante Statusaktualisierungen;

d) spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls gemäß Buchstabe b einen Abschlussbericht, der Folgendes enthält:

   i) eine ausführliche Beschreibung des Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen;

   ii) Angaben zur Art der Bedrohung bzw. zugrunde liegenden Ursache, die wahrscheinlich den Sicherheitsvorfall ausgelöst hat;

   iii) Angaben zu den getroffenen und laufenden Abhilfemaßnahmen;

   iv) gegebenenfalls die grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls;

e) im Falle eines andauernden Sicherheitsvorfalls zum Zeitpunkt der Vorlage des Abschlussberichts gemäß Buchstabe d stellen die Mitgliedstaaten sicher, dass die betreffenden Einrichtungen zu diesem Zeitpunkt einen Fortschrittsbericht und einen Abschlussbericht innerhalb eines Monats nach Behandlung des Sicherheitsvorfalls vorlegen.

Abweichend von Unterabsatz 1 Buchstabe b unterrichtet ein Vertrauensdiensteanbieter das CSIRT oder gegebenenfalls die zuständige Behörde in Bezug auf erhebliche Sicherheitsvorfälle, die sich auf die Erbringung seiner Vertrauensdienste auswirken, unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls.

(5) Das CSIRT oder die zuständige Behörde übermitteln der meldenden Einrichtung unverzüglich und nach Möglichkeit innerhalb von 24 Stunden nach Eingang der Frühwarnung gemäß Absatz 4 Buchstabe a eine Antwort, einschließlich einer ersten Rückmeldung zu dem erheblichen Sicherheitsvorfall und, auf Ersuchen der Einrichtung, Orientierungshilfen oder operativer Beratung für die Durchführung möglicher Abhilfemaßnahmen. Ist das CSIRT nicht der ursprüngliche Empfänger der in Absatz 1 genannten Meldung, werden die Orientierungshilfen von der zuständigen Behörde in Zusammenarbeit mit dem CSIRT bereitgestellt. Das CSIRT leistet auf Ersuchen der betreffenden Einrichtung zusätzliche technische Unterstützung. Wird bei dem erheblichen Sicherheitsvorfall ein krimineller Hintergrund vermutet, gibt das CSIRT oder die zuständige Behörde ferner Orientierungshilfen für die Meldung des Sicherheitsvorfalls an die Strafverfolgungsbehörden.

(6) Gegebenenfalls und insbesondere, wenn der erhebliche Sicherheitsvorfall zwei oder mehr Mitgliedstaaten betrifft, unterrichtet das CSIRT, die zuständige Behörde oder die zentrale Anlaufstelle unverzüglich die anderen betroffenen Mitgliedstaaten und die ENISA über den erheblichen Sicherheitsvorfall. Diese Informationen umfassen die Art der gemäß Absatz 4 erhaltenen Informationen. Dabei wahren das CSIRT, die zuständige Behörde oder die zentrale Anlaufstelle im Einklang mit dem Unionsrecht oder dem einzelstaatlichen Recht die Sicherheit und das wirtschaftliche Interesse der Einrichtung sowie die Vertraulichkeit der bereitgestellten Informationen.

(7) Ist eine Sensibilisierung der Öffentlichkeit erforderlich, um einen erheblichen Sicherheitsvorfall zu verhindern oder einen laufenden erheblichen Sicherheitsvorfall zu bewältigen oder liegt die Offenlegung des erheblichen Sicherheitsvorfalls anderweitig im öffentlichen Interesse, so kann das CSIRT eines Mitgliedstaats oder gegebenenfalls seine zuständige Behörde sowie gegebenenfalls die CSIRTs oder die zuständigen Behörden anderer betreffender Mitgliedstaaten nach Konsultation der betreffenden Einrichtung die Öffentlichkeit über den erheblichen Sicherheitsvorfall informieren oder die Einrichtung auffordern, dies zu tun.

(8) Auf Ersuchen des CSIRT oder der zuständigen Behörde leitet die zentrale Anlaufstelle die nach Absatz 1 eingegangenen Meldungen an die zentralen Anlaufstellen der anderen betroffenen Mitgliedstaaten weiter.

(9) Die zentrale Anlaufstelle legt der ENISA alle drei Monate einen zusammenfassenden Bericht vor, der anonymisierte und aggregierte Daten zu erheblichen Sicherheitsvorfällen, erheblichen Cyberbedrohungen und Beinahe-Vorfällen enthält, die gemäß Absatz 1 des vorliegenden Artikels und Artikel 30 gemeldet wurden. Um zur Bereitstellung vergleichbarer Informationen beizutragen, kann die ENISA technische Leitlinien zu den Parametern der in den zusammenfassenden Bericht aufzunehmenden Angaben verabschieden. Die ENISA un-

terrichtet die Kooperationsgruppe und das CSIRTs-Netzwerk alle sechs Monate über ihre Erkenntnisse zu den eingegangenen Meldungen.

(10) Die CSIRTs oder gegebenenfalls die zuständigen Behörden stellen den gemäß der Richtlinie (EU) 2022/2557 zuständigen Behörden Informationen über erhebliche Sicherheitsvorfälle, erhebliche Cyberbedrohungen und Beinahe-Vorfälle zur Verfügung, die nach Absatz 1 des vorliegenden Artikels und Artikel 30 von Einrichtungen, die im Sinne der Richtlinie (EU) 2022/2557 als kritische Einrichtungen gelten, gemeldet wurden.

(11) Die Kommission kann Durchführungsrechtsakte erlassen, in denen die Art der Angaben, das Format und das Verfahren für Meldungen gemäß Absatz 1 dieses Artikels und Artikel 30 sowie einer gemäß Absatz 2 dieses Artikels übermittelten Mitteilung näher bestimmt werden.

Bis zum 17. Oktober 2024 erlässt die Kommission in Bezug auf DNS-Diensteanbieter, TLD-Namenregister, Cloud-Computing-Dienstleister, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten sowie Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke Durchführungsrechtsakte, in denen näher bestimmt wird, in welchen Fällen ein Sicherheitsvorfall als erheblich im Sinne von Absatz 3 anzusehen ist. Die Kommission kann solche Durchführungsrechtsakte in Bezug auf andere wesentliche und wichtige Einrichtungen erlassen.

Die Kommission tauscht sich mit der Kooperationsgruppe gemäß Artikel 14 Absatz 4 Buchstabe e über die in den Unterabsätzen 1 und 2 dieses Absatzes genannten Entwürfe von Durchführungsrechtsakten aus und arbeitet mit ihr zusammen.

Diese Durchführungsrechtsakte werden gemäß dem in Artikel 39 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 24
Nutzung der europäischen Schemata für die Cybersicherheitszertifizierung

(1) Die Mitgliedstaaten können wesentliche und wichtige Einrichtungen dazu verpflichten, spezielle IKT-Produkte, -Dienste und -Prozesse zu verwenden, die von der wesentlichen oder wichtigen Einrichtung entwickelt oder von Dritten beschafft werden und die im Rahmen europäischer Schemata für die Cybersicherheitszertifizierung, die gemäß Artikel 49 der Verordnung (EU) 2019/881 angenommen wurden, zertifiziert sind, um die Erfüllung bestimmter in Artikel 21 genannter Anforderungen nachzuweisen. Darüber hinaus fördern die Mitgliedstaaten, dass wesentliche und wichtige Einrichtungen qualifizierte Vertrauensdienste nutzen.

(2) Die Kommission ist befugt, gemäß Artikel 38 delegierte Rechtsakte zu erlassen, um diese Richtlinie dadurch zu ergänzen, dass ausgeführt wird, welche Kategorien wesentlicher und wichtiger Einrichtungen verpflichtet sind, bestimmte zertifizierte IKT-Produkte, -Dienste und -Prozesse zu nutzen oder ein Zertifikat im Rahmen eines gemäß Artikel 49 der Verordnung (EU) 2019/881 erlassenen europäischen Schemas für die Cybersicherheitszertifizierung zu erlangen. Diese delegierten Rechtsakte werden erlassen, wenn ein unzureichendes Niveau der Cybersicherheit festgestellt wurde, und umfassen eine Umsetzungsfrist.

Vor dem Erlass solcher delegierten Rechtsakte nimmt die Kommission eine Folgenabschätzung vor und führt Konsultationen gemäß Artikel 56 der Verordnung (EU) 2019/881 durch.

(3) Steht kein geeignetes europäisches Schema für die Cybersicherheitszertifizierung für die Zwecke des Absatzes 2 dieses Artikels zur Verfügung, kann die Kommission nach Anhörung der Kooperationsgruppe und der Europäischen Gruppe für die Cybersicherheitszertifizierung die ENISA auffordern, ein mögliches Schema gemäß Artikel 48 Absatz 2 der Verordnung (EU) 2019/881 auszuarbeiten.

Artikel 25
Normung

(1) Um die einheitliche Anwendung des Artikels 21 Absätze 1 und 2 zu gewährleisten, fördern die Mitgliedstaaten ohne Auferlegung oder willkürliche Bevorzugung der Verwendung einer bestimmten Technologieart die Anwendung europäischer und internationaler Normen und technischer Spezifikationen für die Sicherheit von Netz- und Informationssystemen.

(2) In Zusammenarbeit mit den Mitgliedstaaten und gegebenenfalls nach Konsultation einschlägiger Interessenträger bietet die ENISA Beratung und erlässt Leitlinien zu den technischen Bereichen, die in Bezug auf Absatz 1 in Betracht zu ziehen sind, sowie zu den bereits bestehenden Normen — einschließlich der nationalen Normen —, mit denen diese Bereiche abgedeckt werden könnten.

KAPITEL V
ZUSTÄNDIGKEIT UND REGISTRIERUNG

Artikel 26
Zuständigkeit und Territorialität

(1) Einrichtungen, die in den Anwendungsbereich dieser Richtlinie fallen, gelten als der Zuständigkeit des Mitgliedstaats unterliegend, in dem sie niedergelassen sind, außer in folgenden Fällen:

a) Anbieter öffentlicher elektronischer Kommunikationsnetze oder Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste, die als der Zuständigkeit des Mitgliedstaats unterliegend betrachtet werden, in dem sie ihre Dienste erbringen;

b) DNS-Diensteanbieter, TLD-Namenregister, Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten sowie Anbieter von Online-Marktplätzen, Online-Suchmaschinen oder Plattformen für Dienste sozialer Netzwerke, die als der Zuständigkeit des Mitgliedstaats unterliegend betrachtet werden, in dem sie gemäß Absatz 2 ihre Hauptniederlassung in der Union haben;

c) Einrichtungen der öffentlichen Verwaltung, die als der Zuständigkeit des Mitgliedstaats unterliegend betrachtet werden, der sie gegründet hat.

(2) Für die Zwecke dieser Richtlinie wird davon ausgegangen, dass als Hauptniederlassung in der Union einer in Absatz 1 Buchstabe b genannten Einrichtung jeweils die Niederlassung in demjenigen Mitgliedstaat betrachtet wird, in dem die Entscheidungen im Zusammen-

hang mit den Maßnahmen zum Cybersicherheitsrisikomanagement vorwiegend getroffen werden. Kann ein solcher Mitgliedstaat nicht bestimmt werden oder werden solche Entscheidungen nicht in der 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 Union hat.

(3) Hat eine in Absatz 1 Buchstabe b genannte Einrichtung keine Niederlassung in der Union, bietet aber Dienste innerhalb der Union an, muss sie einen Vertreter in der Union benennen. Der Vertreter muss in einem der Mitgliedstaaten niedergelassen sein, in denen die Dienste angeboten werden. Es wird davon ausgegangen, dass eine solche Einrichtung der Zuständigkeit des Mitgliedstaats unterliegt, in dem der Vertreter niedergelassen ist. Wurde in der Union kein Vertreter im Sinne dieses Absatzes benannt, kann jeder Mitgliedstaat, in dem die Einrichtung Dienste erbringt, gegen die Einrichtung rechtliche Schritte wegen des Verstoßes gegen diese Richtlinie einleiten.

(4) Die Benennung eines Vertreters durch eine in Absatz 1 Buchstabe b genannte Einrichtung lässt rechtliche Schritte, die gegen die Einrichtung selbst eingeleitet werden könnten, unberührt.

(5) Mitgliedstaaten, die ein Rechtshilfeersuchen zu einer in Absatz 1 Buchstabe b genannten Einrichtung erhalten haben, können innerhalb der Grenzen dieses Ersuchens geeignete Aufsichts- und Durchsetzungsmaßnahmen in Bezug auf die betreffende Einrichtung ergreifen, die in ihrem Hoheitsgebiet Dienste anbietet oder ein Netz- und Informationssystem betreibt.

Artikel 27
Register der Einrichtungen

(1) Die ENISA erstellt und pflegt ein Register der DNS-Diensteanbieter, TLD-Namenregister, Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten sowie Anbieter von Online-Marktplätzen, Online-Suchmaschinen oder Plattformen für Dienste sozialer Netzwerke auf der Grundlage der Informationen, die sie von den zentralen Anlaufstellen im Einklang mit Artikel 4 erhalten hat. Auf Ersuchen ermöglicht die ENISA den zuständigen Behörden den Zugang zu diesem Register, wobei sie gegebenenfalls für den Schutz der Vertraulichkeit der Informationen sorgt.

(2) Die Mitgliedstaaten verlangen von den in Absatz 1 genannten Einrichtungen, dass sie bis zum 17. Januar 2025 den zuständigen Behörden folgende Angaben übermitteln:

a) Name der Einrichtung,

b) gegebenenfalls, einschlägiger Sektor, Teilsektor und Art der Einrichtung gemäß Anhang I oder II,

c) Anschrift der Hauptniederlassung der Einrichtung und ihrer sonstigen Niederlassungen in der Union oder, falls sie nicht in der Union niedergelassen ist, Anschrift ihres nach Artikel 26 Absatz 3 benannten Vertreters,

d) aktuelle Kontaktdaten, einschließlich E-Mail-Adressen und Telefonnummern der Einrichtung und gegebenenfalls ihres gemäß Artikel 26 Absatz 3 benannten Vertreters,

e) die Mitgliedstaaten, in denen die Einrichtung Dienste erbringt, und

f) die IP-Adressbereiche der Einrichtung.

(3) Die Mitgliedstaaten stellen sicher, dass im Falle einer Änderung der gemäß Absatz 2 übermittelten Angaben die in Absatz 1 genannten Einrichtungen die zuständige Behörde unverzüglich über diese Änderung, in jedem Fall aber innerhalb von drei Monaten ab dem Tag der Änderung, unterrichten.

(4) Nach Erhalt der in Absatz 2 und 3 genannten Angaben, mit Ausnahme der in Absatz 2 Buchstabe f genannten Angaben, leitet die zentrale Anlaufstelle des betreffenden Mitgliedstaats diese unverzüglich an die ENISA weiter.

(5) Gegebenenfalls werden die in den Absätzen 2 und 3 des vorliegenden Artikels genannten Angaben über den in Artikel 3 Absatz 4 Unterabsatz 4 genannten nationalen Mechanismus übermittelt.

Artikel 28
Datenbank der Domänennamen-Registrierungsdaten

(1) Um einen Beitrag zur Sicherheit, Stabilität und Resilienz des Domänennamensystems zu leisten, verpflichten die Mitgliedstaaten, dass die TLD-Namenregister und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, genaue und vollständige Domänennamen-Registrierungsdaten in einer eigenen Datenbank im Einklang mit dem Datenschutzrecht der Union in Bezug auf personenbezogene Daten mit der gebotenen Sorgfalt sammeln und pflegen.

(2) Für die Zwecke des Absatzes 1 schreiben die Mitgliedstaaten vor, dass die Datenbank der Domänennamen-Registrierungsdaten die erforderlichen Angaben enthält, anhand derer die Inhaber der Domänennamen und die Kontaktstellen, die die Domänennamen im Rahmen der TLD verwalten, identifiziert und kontaktiert werden können. Diese Informationen müssen Folgendes umfassen:

a) den Domänennamen;

b) das Datum der Registrierung;

c) den Namen des Domäneninhabers, seine E-Mail-Adresse und Telefonnummer;

d) die Kontakt-E-Mail-Adresse und die Telefonnummer der Anlaufstelle, die den Domänennamen verwaltet, falls diese sich von denen des Domäneninhabers unterscheiden.

(3) Die Mitgliedstaaten schreiben vor, dass die TLD-Namenregister und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, über Vorgaben und Verfahren, einschließlich Überprüfungsverfahren, verfügen, mit denen sichergestellt wird, dass die in Absatz 1 genannten Datenbanken genaue und vollständige Angaben enthalten. Die Mitgliedstaaten schreiben vor, dass diese Vorgaben und Verfahren öffentlich zugänglich gemacht werden.

(4) Die Mitgliedstaaten schreiben vor, dass die TLD-Namenregister und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, unverzüglich nach der Registrierung eines Domänennamens die nicht personenbezogenen Domänennamen-Registrierungsdaten öffentlich zugänglich machen.

(5) Die Mitgliedstaaten schreiben vor, dass die TLD-Namenregister und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, auf rechtmäßige und hinreichend begründete Anträge berechtigten Zugangsnachfragern im Einklang mit dem Datenschutzrecht der Union Zugang zu bestimmten Domänennamen-Registrierungsdaten gewähren. Die Mitgliedstaaten schreiben vor, dass die TLD-Namenregister und Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, alle Anträge auf Zugang unverzüglich und in jedem Fall innerhalb von 72 Stunden nach Eingang eines Antrags auf Zugang beantworten. Die Mitgliedstaaten schreiben vor, dass diese Vorgaben und Verfahren im Hinblick auf die Offenlegung solcher Daten öffentlich zugänglich gemacht werden.

(6) Die Einhaltung der in den Absätzen 1 bis 5 festgelegten Verpflichtungen darf nicht zu einer doppelten Erhebung von Domänennamen-Registrierungsdaten führen. Zu diesem Zweck schreiben die Mitgliedstaaten vor, dass die TLD-Namenregister und die Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, miteinander zusammenarbeiten.

KAPITEL VI
INFORMATIONSAUSTAUSCH

Artikel 29
Vereinbarungen über den Austausch von Informationen zur Cybersicherheit

(1) Die Mitgliedstaaten stellen sicher, dass in den Anwendungsbereich dieser Richtlinie fallende Einrichtungen und gegebenenfalls andere Einrichtungen, die nicht in den Anwendungsbereich dieser Richtlinie fallen, auf freiwilliger Basis relevante Cybersicherheitsinformationen untereinander austauschen können, einschließlich Informationen über Cyberbedrohungen, Beinahe-Vorfälle, Schwachstellen, Techniken und Verfahren, Kompromittierungsindikatoren, gegnerische Taktiken, bedrohungsspezifische Informationen, Cybersicherheitswarnungen und Empfehlungen für die Konfiguration von Cybersicherheitsinstrumenten zur Aufdeckung von Cyberangriffen, sofern

a) dieser Informationsaustausch darauf abzielt, Sicherheitsvorfälle zu verhindern, aufzudecken, darauf zu reagieren oder sich von ihnen zu erholen oder ihre Folgen einzudämmen;

b) durch diesen Informationsaustausch das Cybersicherheitsniveau erhöht wird, insbesondere indem Aufklärungsarbeit über Cyberbedrohungen geleistet wird, die Fähigkeit solcher Bedrohungen, sich zu verbreiten eingedämmt bzw. verhindert wird und eine Reihe von Abwehrkapazitäten, die Beseitigung und Offenlegung von Schwachstellen, Techniken zur Erkennung, Eindämmung und Verhütung von Bedrohungen, Eindämmungsstrategien, Reaktions- und Wiederherstellungsphasen unterstützt werden oder indem die gemeinsame Forschung im Bereich Cyberbedrohung zwischen öffentlichen und privaten Einrichtungen gefördert wird.

(2) Die Mitgliedstaaten stellen sicher, dass der Informationsaustausch innerhalb Gemeinschaften wesentlicher und wichtiger Einrichtungen und gegebenenfalls ihrer Lieferanten oder Dienstleister stattfindet. Dieser Austausch muss im Wege von Vereinbarungen über

den Informationsaustausch im Bereich der Cybersicherheit unter Beachtung des potenziell sensiblen Charakters der ausgetauschten Informationen erfolgen.

(3) Die Mitgliedstaaten erleichtern die Festlegung von Vereinbarungen über den Austausch von Informationen im Bereich der Cybersicherheit gemäß Absatz 2 dieses Artikels. In solchen Vereinbarungen können operative Elemente, einschließlich der Nutzung spezieller IKT-Plattformen und Automatisierungsinstrumente, der Inhalt und die Bedingungen der Vereinbarungen über den Informationsaustausch bestimmt werden. Bei der Festlegung der Einzelheiten der Beteiligung von Behörden an solchen Vereinbarungen können die Mitgliedstaaten Bedingungen für die von den zuständigen Behörden oder CSIRTs bereitgestellten Informationen festlegen. Die Mitgliedstaaten bieten Unterstützung bei der Anwendung solcher Vereinbarungen im Einklang mit ihren in Artikel 7 Absatz 2 Buchstabe h genannten Konzepten.

(4) Die Mitgliedstaaten stellen sicher, dass wesentliche und wichtige Einrichtungen die zuständigen Behörden beim Abschluss von in Absatz 2 genannten Vereinbarungen über den Informationsaustausch im Bereich der Cybersicherheit oder gegebenenfalls über ihren Rücktritt von solchen Vereinbarungen unterrichten, sobald dieser wirksam wird.

(5) Die ENISA unterstützt den Abschluss von Vereinbarungen über den Austausch von Informationen im Bereich der Cybersicherheit gemäß Absatz 2, indem sie bewährte Verfahren austauscht und Orientierungshilfen zur Verfügung stellt.

Artikel 30
Freiwillige Meldung relevanter Informationen

(1) Die Mitgliedstaaten stellen sicher, dass zusätzlich zu der Berichtspflicht nach Artikel 23 Meldungen den CSIRTs oder gegebenenfalls den zuständigen Behörden auf freiwilliger Basis übermittelt werden können, und zwar durch:

a) wesentliche und wichtige Einrichtungen in Bezug auf Sicherheitsvorfälle, Cyberbedrohungen und Beinahe-Vorfälle;

b) andere als die in Buchstabe a genannten Einrichtungen, unabhängig davon, ob sie in den Anwendungsbereich dieser Richtlinie fallen, in Bezug auf erhebliche Sicherheitsvorfälle, Cyberbedrohungen und Beinahe-Vorfälle.

(2) Die Mitgliedstaaten bearbeiten die in Absatz 1 des vorliegenden Artikels genannten Meldungen nach dem in Artikel 23 vorgesehenen Verfahren. Die Mitgliedstaaten können Pflichtmeldungen vorrangig vor freiwilligen Meldungen bearbeiten.

Erforderlichenfalls übermitteln die CSIRTs und gegebenenfalls die zuständigen Behörden den zentralen Anlaufstellen die Informationen über die gemäß diesem Artikel eingegangenen Meldungen, wobei sie die Vertraulichkeit und den angemessenen Schutz der von der meldenden Einrichtung übermittelten Informationen sicherstellen. Unbeschadet der Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten dürfen die freiwilligen Meldungen nicht dazu führen, dass der meldenden Einrichtung zusätzliche Verpflichtungen auferlegt werden, die nicht für sie gegolten hätten, wenn sie die Meldung nicht übermittelt hätte.

KAPITEL VII
AUFSICHT UND DURCHSETZUNG

Artikel 31
Allgemeine Aspekte der Aufsicht und Durchsetzung

(1) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden die Einhaltung der Verpflichtungen aus dieser Richtlinie wirksam beaufsichtigen und die erforderlichen Maßnahmen treffen.

(2) Die Mitgliedstaaten können ihren zuständigen Behörden gestatten, Aufsichtsaufgaben zu priorisieren. Diese Priorisierung beruht auf einem risikobasierten Ansatz. Zu diesem Zweck können die zuständigen Behörden bei der Wahrnehmung ihrer in den Artikeln 32 und 33 aufgeführten Aufsichtsaufgaben Aufsichtsmethoden festlegen, die eine Priorisierung dieser Aufgaben auf der Grundlage eines risikobasierten Ansatzes ermöglichen.

(3) Unbeschadet der Zuständigkeiten und Aufgaben der Aufsichtsbehörden gemäß der Verordnung (EU) 2016/679 arbeiten die zuständigen Behörden bei der Bearbeitung von Sicherheitsvorfällen, die zur Verletzung des Schutzes personenbezogener Daten führen, eng mit den Aufsichtsbehörden gemäß jener Verordnung zusammen.

(4) Unbeschadet der nationalen rechtlichen und institutionellen Rahmenbedingungen stellen die Mitgliedstaaten sicher, dass die zuständigen Behörden bei der Überwachung der Einhaltung dieser Richtlinie durch Einrichtungen der öffentlichen Verwaltung und bei der Verhängung von Durchsetzungsmaßnahmenbei Verstößen gegen diese Richtlinie über die geeigneten Befugnisse verfügen, um diese Aufgaben in operativer Unabhängigkeit von den beaufsichtigten Einrichtungen der öffentlichen Verwaltung wahrzunehmen. Die Mitgliedstaaten können entscheiden, ob diesen Einrichtungen im Einklang mit den nationalen rechtlichen und institutionellen Rahmenbedingungen geeignete, verhältnismäßige und wirksame Aufsichts- und Durchsetzungsmaßnahmen auferlegt werden.

Artikel 32
Aufsichts- und Durchsetzungsmaßnahmen in Bezug auf wesentliche Einrichtungen

(1) Die Mitgliedstaaten stellen sicher, dass die Aufsichts- bzw. Durchsetzungsmaßnahmen, die wesentlichen Einrichtungen in Bezug auf die in dieser Richtlinie festgelegten Verpflichtungen auferlegt werden, unter Berücksichtigung der Umstände des Einzelfalls wirksam, verhältnismäßig und abschreckend sind.

(2) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden bei der Wahrnehmung ihrer Aufsichtsaufgaben in Bezug auf wesentliche Einrichtungen befugt sind, in Bezug auf diese Einrichtungen mindestens folgende Maßnahmen vorzunehmen:

a) Vor-Ort-Kontrollen und externe Aufsichtsmaßnahmen, einschließlich von geschulten Fachleuten durchgeführten Stichprobenkontrollen;

b) regelmäßige und gezielte Sicherheitsprüfungen, die von einer unabhängigen Stelle oder einer zuständigen Behörde durchgeführt werden;

c) Ad-hoc-Prüfungen, einschließlich solcher, die aufgrund eines erheblichen Sicherheitsvorfalls oder Verstoßes gegen diese Richtlinie der wesentlichen Einrichtung gerechtfertigt sind;

d) Sicherheitsscans auf der Grundlage objektiver, nichtdiskriminierender, fairer und transparenter Risikobewertungskriterien, erforderlichenfalls in Zusammenarbeit mit der betreffenden Einrichtung;

e) Anforderung von Informationen, die für die Bewertung der von der betreffenden Einrichtung ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit erforderlich sind, einschließlich dokumentierter Cybersicherheitskonzepte, sowie der Einhaltung der Verpflichtungen zur Übermittlung von Informationen an die zuständigen Behörden nach Artikel 27;

f) Anforderung des Zugangs zu Daten, Dokumenten und sonstigen Informationen, die zur Erfüllung der Aufsichtsaufgaben erforderlich sind;

g) Anforderung von Nachweisen für die Umsetzung der Cybersicherheitskonzepte, z. B. der Ergebnisse von Sicherheitsprüfungen, die von einem qualifizierten Prüfer durchgeführt wurden, und der entsprechenden zugrunde liegenden Nachweise.

Die in Unterabsatz 1 Buchstabe b genannten gezielten Sicherheitsprüfungen stützen sich auf Risikobewertungen, die von der zuständigen Behörde oder der geprüften Einrichtung durchgeführt werden, oder auf sonstige verfügbare risikobezogene Informationen.

Die Ergebnisse einer gezielten Sicherheitsprüfung sind der zuständigen Behörde zur Verfügung zu stellen. Die Kosten einer solchen gezielten Sicherheitsprüfung, die von einer unabhängigen Stelle durchgeführt wird, sind von der geprüften Einrichtung zu tragen, es sei denn, die zuständige Behörde trifft in hinreichend begründeten Fällen eine anderslautende Entscheidung.

(3) Bei der Ausübung ihrer Befugnisse nach Absatz 2 Buchstaben e, f oder g geben die zuständigen Behörden den Zweck der Anfrage und die erbetenen Informationen an.

(4) Die Mitgliedstaaten stellen sicher, dass ihre zuständigen Behörden bei der Wahrnehmung ihrer Durchsetzungsbefugnisse in Bezug auf wesentliche Einrichtungen mindestens befugt sind,

a) Warnungen über Verstöße gegen diese Richtlinie durch die betreffenden Einrichtungen herauszugeben;

b) verbindliche Anweisungen zu erlassen, auch in Bezug auf Maßnahmen, die zur Verhütung oder Behebung eines Sicherheitsvorfalls erforderlich sind, sowie Fristen für die Durchführung dieser Maßnahmen und für die Berichterstattung über ihre Durchführung zu setzen, oder Anordnungen zu erlassen, um diese Einrichtungen aufzufordern, die festgestellten Mängel oder die Verstöße gegen diese Richtlinie zu beheben;

c) die betreffenden Einrichtungen anzuweisen, das gegen diese Richtlinie verstoßende Verhalten einzustellen und von Wiederholungen abzusehen;

d) die betreffenden Einrichtungen anzuweisen, entsprechend bestimmten Vorgaben und innerhalb einer bestimmten Frist sicherzustellen, dass ihre Risikomanagementmaßnahmen im Bereich der Cybersicherheit mit Artikel 21 im Einklang stehen, bzw. die in Artikel 23 festgelegten Berichtspflichten zu erfüllen;

e) die betreffenden Einrichtungen anzuweisen, 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 Bedro-

hung und mögliche Abwehr- oder Abhilfemaßnahmen zu unterrichten, die von diesen natürlichen oder juristischen Personen als Reaktion auf diese Bedrohung ergriffen werden können;

f) die betreffenden Einrichtungen anzuweisen, die im Rahmen einer Sicherheitsprüfung formulierten Empfehlungen innerhalb einer angemessenen Frist umzusetzen;

g) für einen bestimmten Zeitraum einen mit genau festgelegten Aufgaben betrauten Überwachungsbeauftragten zu benennen, der die Einhaltung der Artikel 21 und 23 durch die betreffenden Einrichtungen überwacht;

h) die betreffenden Einrichtungen anzuweisen, Aspekte der Verstöße gegen diese Richtlinie entsprechend bestimmten Vorgaben öffentlich bekannt zu machen;

i) gemäß einzelstaatlichem Recht zusätzlich zu jeglichen der unter den Buchstaben a bis h dieses Absatzes genannten Maßnahmen eine Geldbuße gemäß Artikel 34 zu verhängen oder die zuständigen Stellen oder Gerichte um die Verhängung einer solchen Geldbuße zu ersuchen.

(5) Erweisen sich die gemäß Absatz 4 Buchstaben a bis d und f ergriffenen Durchsetzungsmaßnahmen als unwirksam, so stellen die Mitgliedstaaten sicher, dass ihre zuständigen Behörden befugt sind, eine Frist festzusetzen, innerhalb derer die wesentliche Einrichtung die erforderlichen Maßnahmen ergreifen muss, um die Mängel zu beheben oder die Anforderungen dieser Behörden zu erfüllen. Für den Fall, dass die geforderten Maßnahmen nicht innerhalb der gesetzten Frist ergriffen werden, stellen die Mitgliedstaaten sicher, dass ihre zuständigen Behörden befugt sind,

die Zertifizierung oder Genehmigung für einen Teil oder alle von der wesentlichen Einrichtung erbrachten einschlägigen Dienste oder Tätigkeiten vorübergehend auszusetzen oder eine Zertifizierungs- oder Genehmigungsstelle oder ein Gericht im Einklang mit dem nationalen Recht aufzufordern, die Zertifizierung oder Genehmigung vorübergehend auszusetzen;

zu verlangen, dass die zuständigen Stellen oder Gerichte im Einklang mit dem nationalen Recht natürlichen Personen, die auf Geschäftsführungs- bzw. Vorstandsebene oder Ebene des rechtlichen Vertreters für Leitungsaufgaben in dieser wesentlichen Einrichtung zuständig sind, vorübergehend untersagen, Leitungsaufgaben in dieser Einrichtung wahrzunehmen.

Die gemäß diesem Absatz verhängten vorübergehenden Aussetzungen oder Verbote werden nur so lange angewandt, bis die betreffende Einrichtung die erforderlichen Maßnahmen ergreift, um die Mängel zu beheben oder die Anforderungen der zuständigen Behörde, wegen deren Nichterfüllung die Durchsetzungsmaßnahmenverhängt wurden, zu erfüllen. Für die Verhängung solcher vorübergehenden Aussetzungen oder Verbote muss es angemessene Verfahrensgarantien geben, die den allgemeinen Grundsätzen des Unionsrechts und der Charta, einschließlich des Rechts auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht, der Unschuldsvermutung und der Verteidigungsrechte, entsprechen.

Die in diesem Absatz vorgesehenen Durchsetzungsmaßnahmen finden keine Anwendung auf Einrichtungen der öffentlichen Verwaltung, die dieser Richtlinie unterliegen.

(6) Die Mitgliedstaaten stellen sicher, dass jede natürliche Person, die für eine wesentliche Einrichtung verantwortlich ist oder auf der Grundlage ihrer Vertretungsbefugnis, der Befugnis, im Namen der Einrichtung Entscheidungen zu treffen, oder ihrer Kontrollbefugnis über die Einrichtung als Vertreterin der wesentlichen Einrichtung handelt, befugt ist zu ge-

währleisten, dass die Einrichtung diese Richtlinie erfüllt. Die Mitgliedstaaten stellen sicher, dass diese natürlichen Personen für Verstöße gegen ihre Pflichten zur Gewährleistung der Einhaltung dieser Richtlinie haftbar gemacht werden können.

Für Einrichtungen der öffentlichen Verwaltung gilt dieser Absatz unbeschadet der nationalen Rechtsvorschriften über die Haftung von öffentlichen Bediensteten und von gewählten oder ernannten Amtsträgern.

(7) Bei der Ergreifung von Durchsetzungsmaßnahmen gemäß Absatz 4 oder 5 müssen die zuständigen Behörden die Verteidigungsrechte einhalten und den Umständen des Einzelfalls Rechnung tragen und dabei zumindest Folgendes gebührend berücksichtigen:

a) die Schwere des Verstoßes und die Wichtigkeit der Bestimmungen, gegen die verstoßen wurde, wobei u. a. Folgendes immer als schwerer Verstoß anzusehen ist:

   i) wiederholte Verstöße,

   ii) eine unterlassene Meldung oder Behebung von erheblichen Sicherheitsvorfällen,

   iii) eine Nichtbehebung von Mängeln nach verbindlicher Anweisung der zuständigen Behörden,

   iv) die Behinderung von Prüfungen oder Überwachungstätigkeiten, die nach der Feststellung eines Verstoßes von der zuständigen Behörde angeordnet wurden, sowie

   v) Übermittlung falscher oder grob verfälschender Informationen in Bezug auf Risikomanagementmaßnahmen im Bereich der Cybersicherheit oder Berichtspflichten gemäß den Artikeln 21 und 23.

b) die Dauer des Verstoßes;

c) einschlägige frühere Verstöße der betreffenden Einrichtung;

d) der verursachte materielle oder immaterielle Schaden, darunter finanzieller oder wirtschaftlicher Verlust, Auswirkungen auf andere Dienste und die Zahl der betroffenen Nutzer;

e) etwaiger Vorsatz oder etwaige Fahrlässigkeit des Urhebers des Verstoßes;

f) von der Einrichtung ergriffene Maßnahmen zur Verhinderung oder Minderung des materiellen oder immateriellen Schadens;

g) Einhaltung genehmigter Verhaltensregeln oder genehmigter Zertifizierungsverfahren;

h) Umfang der Zusammenarbeit der verantwortlichen natürlichen oder juristischen Personen mit den zuständigen Behörden.

(8) Die zuständigen Behörden müssen ihre Durchsetzungsmaßnahmen ausführlich begründen. Bevor sie solche Maßnahmen ergreifen, teilen die zuständigen Behörden den betreffenden Einrichtungen ihre vorläufigen Erkenntnisse mit. Sie räumen diesen Einrichtungen ferner eine angemessene Frist zur Stellungnahme ein, außer in hinreichend begründeten Fällen, in denen sofortige Maßnahmen zur Verhütung von Sicherheitsvorfällen oder zur Reaktion auf Sicherheitsvorfälle andernfalls beeinträchtigt würden.

(9) Die Mitgliedstaaten stellen sicher, dass ihre gemäß der vorliegenden Richtlinie zuständigen Behörden bei der Ausübung ihrer Aufsichts- und Durchsetzungsbefugnisse — mit denen sichergestellt werden soll, dass Einrichtungen, die gemäß der Richtlinie (EU) 2022/2557 als kritische Einrichtungen eingestuft wurden, diese Richtlinie erfüllen — die gemäß der Richtlinie (EU) 2022/2557 zuständigen Behörden innerhalb desselben Mitgliedstaats unterrichten. Gegebenenfalls können die gemäß der Richtlinie (EU) 2022/2557 zuständigen Behörden die gemäß der vorliegenden Richtlinie zuständigen Behörden ersuchen, ihre Aufsichts- und Durchsetzungsbefugnisse in Bezug auf eine Einrichtung, die gemäß der Richtlinie (EU) 2022/2557 als kritische Einrichtung eingestuft wird, auszuüben.

(10) Die Mitgliedstaaten stellen sicher, dass ihre gemäß der vorliegenden Richtlinie zuständigen Behörden mit den gemäß der Verordnung (EU) 2022/2554 jeweils zuständigen Behörden des betreffenden Mitgliedstaats zusammenarbeiten. Insbesondere stellen die Mitgliedstaaten sicher, dass ihre gemäß dieser Richtlinie zuständigen Behörden bei der Ausübung ihrer Aufsichts- und Durchsetzungsbefugnisse — mit denen sichergestellt werden soll, dass wesentliche Einrichtungen, die als IKT-Drittanbieter gemäß Artikel 31 der Verordnung (EU) 2022/2554 benannt wurden, diese Richtlinie erfüllen — das gemäß Artikel 32 Absatz 1 der Verordnung (EU) 2022/2554 eingerichtete Überwachungsforum unterrichten.

Artikel 33
Aufsichts- und Durchsetzungsmaßnahmen in Bezug auf wichtige Einrichtungen

(1) Werden Nachweise, Hinweise oder Informationen vorgelegt, wonach eine wichtige Einrichtung mutmaßlich dieser Richtlinie, insbesondere deren Artikeln 21 und 23, nicht nachkommt, so stellen die Mitgliedstaaten sicher, dass die zuständigen Behörden erforderlichenfalls im Wege von nachträglichen Aufsichtsmaßnahmen tätig werden. Die Mitgliedstaaten stellen sicher, dass diese Maßnahmen wirksam, verhältnismäßig und abschreckend sind, wobei die Umstände des Einzelfalls jeweils zu berücksichtigen sind.

(2) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden bei der Wahrnehmung ihrer Aufsichtsaufgaben in Bezug auf wichtige Einrichtungen befugt sind, in Bezug auf diese Einrichtungen mindestens folgende Maßnahmen vorzunehmen:

a) Vor-Ort-Kontrollen und externe nachträgliche Aufsichtsmaßnahmen, die von geschulten Fachkräften durchgeführt werden;

b) gezielte Sicherheitsprüfungen, die von einer unabhängigen Stelle oder einer zuständigen Behörde durchgeführt werden;

c) Sicherheitsscans auf der Grundlage objektiver, nichtdiskriminierender, fairer und transparenter Risikobewertungskriterien, erforderlichenfalls auch in Zusammenarbeit mit der betreffenden Einrichtung;

d) Anforderung von Informationen, die für die nachträgliche Bewertung der von der betreffenden Einrichtung ergriffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit erforderlich sind, einschließlich dokumentierter Cybersicherheitskonzepte, sowie der Einhaltung der Verpflichtungen zur Übermittlung von Informationen an die zuständigen Behörden nach Artikel 27;

e) Anforderung des Zugangs zu Daten, Dokumenten und sonstigen Informationen, die zur Erfüllung ihrer Aufsichtsaufgaben erforderlich sind;

f) Anforderung von Nachweisen für die Umsetzung der Cybersicherheitskonzepte, z. B. der Ergebnisse von von einem qualifizierten Prüfer durchgeführten Sicherheitsprüfungen und der entsprechenden zugrunde liegenden Nachweise.

Die in Unterabsatz 1 Buchstabe b genannten gezielten Sicherheitsprüfungen stützen sich auf Risikobewertungen, die von der zuständigen Behörde oder der geprüften Einrichtung durchgeführt werden, oder auf sonstige verfügbare risikobezogene Informationen.

Die Ergebnisse gezielter Sicherheitsprüfungen sind der zuständigen Behörde zur Verfügung zu stellen. Die Kosten einer solchen gezielten Sicherheitsprüfung, die von einer unabhängigen Stelle durchgeführt wird, sind von der geprüften Einrichtung zu tragen, es sei denn, die zuständige Behörde trifft in hinreichend begründeten Fällen eine anderslautende Entscheidung.

(3) Bei der Ausübung ihrer Befugnisse nach Absatz 2 Buchstabe d, e oder f geben die zuständigen Behörden den Zweck der Anfrage und die erbetenen Informationen an.

(4) Die Mitgliedstaaten stellen sicher, dass die zuständigen Behörden bei der Wahrnehmung ihrer Durchsetzungsbefugnisse in Bezug auf wichtige Einrichtungen mindestens dazu befugt sind,

a) Warnungen über Verstöße gegen diese Richtlinie durch die betreffenden Einrichtungen herauszugeben;

b) verbindliche Anweisungen oder Anordnungen zu erlassen, um die betreffenden Einrichtungen aufzufordern, die festgestellten Mängel oder den Verstoß gegen diese Richtlinie zu beheben;

c) die betreffenden Einrichtungen anzuweisen, das gegen diese Richtlinie verstoßende Verhalten einzustellen und von Wiederholungen abzusehen;

d) die betreffenden Einrichtungen anzuweisen, entsprechend bestimmten Vorgaben und innerhalb einer bestimmten Frist sicherzustellen, dass ihre Risikomanagementmaßnahmen im Bereich der Cybersicherheit mit Artikel 21 im Einklang stehen, bzw. die in Artikel 23 festgelegten Berichtspflichten zu erfüllen;

e) die betreffenden Einrichtungen anzuweisen, die natürlichen oder juristischen Personen, für die sie Dienste erbringen oder Tätigkeiten ausüben und die potenziell von einer erheblichen Cyberbedrohung betroffen sind, über die Art der Bedrohung und mögliche Abwehr- oder Abhilfemaßnahmen zu unterrichten, die von diesen natürlichen oder juristischen Personen als Reaktion auf diese Bedrohung ergriffen werden können;

f) die betreffenden Einrichtungen anzuweisen, die im Rahmen einer Sicherheitsprüfung formulierten Empfehlungen innerhalb einer angemessenen Frist umzusetzen;

g) die betreffenden Einrichtungen anzuweisen, Aspekte der Verstöße gegen diese Richtlinie entsprechend bestimmten Vorgaben öffentlich bekannt zu machen;

h) gemäß einzelstaatlichem Recht zusätzlich zu jeglichen der unter den Buchstaben a bis g dieses Absatzes genannten Maßnahmen eine Geldbuße gemäß Artikel 34 zu verhängen oder die zuständigen Stellen oder Gerichte um die Verhängung einer solchen Geldbuße zu ersuchen.

(5) Artikel 32 Absätze 6, 7 und 8 gelten entsprechend für die Aufsichts- und Durchsetzungsmaßnahmen, die in diesem Artikel für wichtige Einrichtungen vorgesehen sind.

(6) Die Mitgliedstaaten stellen sicher, dass ihre gemäß der vorliegenden Richtlinie zuständigen Behörden mit den gemäß der Verordnung (EU) 2022/2554 jeweils zuständigen Behörden des betreffenden Mitgliedstaats zusammenarbeiten. Insbesondere stellen die Mitgliedstaaten sicher, dass ihre gemäß dieser Richtlinie zuständigen Behörden bei der Ausübung ihrer Aufsichts- und Durchsetzungsbefugnisse — mit denen sichergestellt werden soll, dass wichtige Einrichtungen, die als IKT-Drittanbieter gemäß Artikel 31 der Verordnung (EU) 2022/2554 benannt wurden, diese Richtlinie erfüllen — das gemäß Artikel 32 Absatz 1 der Verordnung (EU) 2022/2554 eingerichtete Überwachungsforum unterrichten.

Artikel 34
Allgemeine Bedingungen für die Verhängung von Geldbußen gegen wesentliche und wichtige Einrichtungen

(1) Die Mitgliedstaaten stellen sicher, dass die Geldbußen, die gemäß dem vorliegenden Artikel gegen wesentliche und wichtige Einrichtungen in Bezug auf Verstöße gegen diese Richtlinie verhängt werden, unter Berücksichtigung der Umstände des Einzelfalls wirksam, verhältnismäßig und abschreckend sind.

(2) Geldbußen werden zusätzlich zu jeglichen der Maßnahmen nach Artikel 32 Absatz 4 Buchstaben a bis h, Artikel 32 Absatz 5 und Artikel 33 Absatz 4 Buchstaben a bis g verhängt.

(3) Bei der Entscheidung über die Verhängung einer Geldbuße und deren Höhe sind in jedem Einzelfall zumindest die in Artikel 32 Absatz 7 genannten Elemente gebührend zu berücksichtigen.

(4) Die Mitgliedstaaten stellen sicher, dass gegen wesentliche Einrichtungen, die gegen Artikel 21 oder 23 verstoßen, im Einklang mit den Absätzen 2 und 3 des vorliegenden Artikels Geldbußen mit einem Höchstbetrag von mindestens 10 000 000 EUR oder mit einem Höchstbetrag von mindestens 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem die wesentliche Einrichtung angehört, verhängt werden, je nachdem, welcher Betrag höher ist.

(5) Die Mitgliedstaaten stellen sicher, dass gegen wichtige Einrichtungen, die gegen Artikel 21 oder 23 verstoßen, im Einklang mit den Absätzen 2 und 3 des vorliegenden Artikels Geldbußen mit einem Höchstbetrag von mindestens 7 000 000 EUR oder mit einem Höchstbetrag von mindestens 1,4 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens, dem die wichtige Einrichtung angehört, verhängt werden, je nachdem, welcher Betrag höher ist.

(6) Die Mitgliedstaaten können die Befugnis vorsehen, Zwangsgelder zu verhängen, um eine wesentliche oder wichtige Einrichtung zu zwingen, einen Verstoß gegen diese Richtlinie gemäß einer vorherigen Entscheidung der zuständigen Behörde einzustellen.

(7) Unbeschadet der Befugnisse der zuständigen Behörden gemäß den Artikeln 32 und 33 kann jeder Mitgliedstaat Vorschriften dafür festlegen, ob und in welchem Umfang gegen Einrichtungen der öffentlichen Verwaltung Geldbußen verhängt werden können.

(8) Sieht die Rechtsordnung eines Mitgliedstaats keine Geldbußen vor, so stellt dieser Mitgliedstaat sicher, dass dieser Artikel so angewandt wird, dass die Geldbuße von der zuständigen Behörde in die Wege geleitet und von den zuständigen nationalen Gerichten verhängt

wird, wobei sicherzustellen ist, dass diese Rechtsbehelfe wirksam sind und die gleiche Wirkung wie die von den zuständigen Behörden verhängten Geldbußen haben. In jedem Fall müssen die verhängten Geldbußen wirksam, verhältnismäßig und abschreckend sein. Der betreffende Mitgliedstaat teilt der Kommission bis zum 17. Oktober 2024 die Rechtsvorschriften, die er aufgrund dieses Absatzes erlässt, sowie unverzüglich alle nachfolgenden Änderungsgesetze oder Änderungen dieser Vorschriften mit.

Artikel 35
Verstöße mit Verletzungen des Schutzes personenbezogener Daten

(1) Stellen die zuständigen Behörden im Zuge der Beaufsichtigung oder Durchsetzung fest, dass der Verstoß einer wesentlichen oder wichtigen Einrichtung gegen die in den Artikeln 21 und 23 der vorliegenden Richtlinie festgelegten Verpflichtungen eine Verletzung des Schutzes personenbezogener Daten im Sinne von Artikel 4 Nummer 12 der Verordnung (EU) 2016/679 zur Folge haben kann, die gemäß Artikel 33 der genannten Verordnung zu melden ist, unterrichten sie unverzüglich die in Artikel 55 oder 56 jener Verordnung genannten Aufsichtsbehörden.

(2) Verhängen die in Artikel 55 oder 56 der Verordnung (EU) 2016/679 genannten Aufsichtsbehörden gemäß Artikel 58 Absatz 2 Buchstabe i der genannten Verordnung eine Geldbuße, so dürfen die zuständigen Behörden für einen Verstoß im Sinne von Absatz 1 des vorliegenden Artikels, 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, keine Geldbuße nach Artikel 34 der vorliegenden Richtlinie verhängen. Die zuständigen Behörden können jedoch die Durchsetzungsmaßnahmen gemäß Artikel 32 Absatz 4 Buchstaben a bis h, Artikel 32 Absatz 5 und Artikel 33 Absatz 4 Buchstaben a bis g dieser Richtlinie anwenden bzw. verhängen.

(3) Ist die gemäß der Verordnung (EU) 2016/679 zuständige Aufsichtsbehörde in einem anderen Mitgliedstaat angesiedelt als die zuständige Behörde, so setzt die zuständige Behörde die in ihrem eigenen Mitgliedstaat angesiedelte Aufsichtsbehörde über die mögliche Verletzung des Schutzes personenbezogener Daten nach Absatz 1 in Kenntnis.

Artikel 36
Sanktionen

Die Mitgliedstaaten erlassen Vorschriften über Sanktionen, die bei Verstößen gegen die gemäß dieser Richtlinie erlassenen nationalen Maßnahmen zu verhängen sind, und treffen alle für die Anwendung der Sanktionen erforderlichen Maßnahmen. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. Die Mitgliedstaaten teilen der Kommission diese Vorschriften und Maßnahmen bis zum 17. Januar 2025 mit und melden ihr unverzüglich alle diesbezüglichen Änderungen.

Artikel 37
Amtshilfe

(1) Wenn eine Einrichtung ihre Dienste in mehr als einem Mitgliedstaat erbringt oder wenn sie ihre Dienste in einem oder mehreren Mitgliedstaaten erbringt und sich ihre Netz- und Informationssysteme in einem oder mehreren anderen Mitgliedstaaten befinden, so arbeiten die zuständigen Behörden der betreffenden Mitgliedstaaten zusammen und unterstützen einander. Diese Zusammenarbeit umfasst mindestens Folgendes:

a) über die zentralen Anlaufstellen unterrichten die zuständigen Behörden, die in einem Mitgliedstaat Aufsichts- oder Durchsetzungsmaßnahmen ergreifen, die zuständigen Behörden in den anderen betreffenden Mitgliedstaaten über die Aufsichts- und Durchsetzungsmaßnahmen und konsultieren sie zu diesen;

b) eine zuständige Behörde kann eine andere zuständige Behörde ersuchen, Aufsichts- oder Durchsetzungsmaßnahmen zu ergreifen;

c) auf begründetes Ersuchen einer anderen zuständigen Behörde leistet eine zuständige Behörde der ersuchenden Behörde in einem ihren zur Verfügung stehenden Ressourcen angemessenen Umfang Amtshilfe, damit die Aufsichts- oder Durchsetzungsmaßnahmen wirksam, effizient und kohärent durchgeführt werden können.

Die in Unterabsatz 1 Buchstabe c genannte Amtshilfe kann Auskunftsersuchen und Aufsichtsmaßnahmen umfassen, einschließlich Ersuchen um Durchführung von Vor-Ort-Kontrollen und externen Aufsichtsmaßnahmen oder gezielten Sicherheitsprüfungen. Die ersuchte zuständige Behörde darf das Amtshilfeersuchen nur ablehnen, wenn festgestellt wird, dass sie für die erbetene Amtshilfe nicht zuständig ist, dass die ersuchte Amtshilfe in keinem angemessenen Verhältnis zu den Aufsichtsaufgaben der zuständigen Behörde steht oder dass das Ersuchen Informationen betrifft oder Tätigkeiten umfasst, deren Offenlegung bzw. Ausführung den wesentlichen Interessen der Mitgliedstaaten im Bereich der nationalen Sicherheit, der öffentlichen Sicherheit oder der Landesverteidigung des betreffenden Mitgliedstaats zuwiderlaufen würde. Bevor die zuständige Behörde einen solchen Antrag ablehnt, konsultiert sie die anderen betreffenden zuständigen Behörden sowie — auf Ersuchen eines der betreffenden Mitgliedstaaten — die Kommission und die ENISA.

(2) Die zuständigen Behörden verschiedener Mitgliedstaaten können, wenn angezeigt und im gegenseitigen Einvernehmen, gemeinsame Aufsichtsmaßnahmen durchführen.

KAPITEL VIII
DELEGIERTE RECHTSAKTE UND DURCHFÜHRUNGSRECHTSAKTE

Artikel 38
Ausübung der Befugnisübertragung

(1) Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission unter den in diesem Artikel festgelegten Bedingungen übertragen.

(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 24 Absatz 2 wird der Kommission für einen Zeitraum von fünf Jahren ab dem 16. Januar 2023 übertragen.

(3) Die Befugnisübertragung gemäß Artikel 24 Absatz 2 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im Amtsblatt der Europäischen Union oder zu einem im Beschluss über den Widerruf angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.

(4) Vor dem Erlass eines delegierten Rechtsakts konsultiert die Kommission die von den einzelnen Mitgliedstaaten benannten Sachverständigen, im Einklang mit den in der Interinsti-

tutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung enthaltenen Grundsätzen.

(5) Sobald die Kommission einen delegierten Rechtsakt erlässt, übermittelt sie ihn gleichzeitig dem Europäischen Parlament und dem Rat.

(6) Ein delegierter Rechtsakt, der gemäß Artikel 24 Absatz 2 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von zwei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Initiative des Europäischen Parlaments oder des Rates wird diese Frist um zwei Monate verlängert.

Artikel 39
Ausschussverfahren

(1) Die Kommission wird von einem Ausschuss unterstützt. Dieser Ausschuss ist ein Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.

(2) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 5 der Verordnung (EU) Nr. 182/2011.

(3) Wird die Stellungnahme des Ausschusses im schriftlichen Verfahren eingeholt, so wird das Verfahren ohne Ergebnis abgeschlossen, wenn der Vorsitz des Ausschusses dies innerhalb der Frist zur Abgabe der Stellungnahme beschließt oder ein Ausschussmitglied dies verlangt.

KAPITEL IX
SCHLUSSBESTIMMUNGEN

Artikel 40
Überprüfung

Bis zum 17. Oktober 2027 und danach alle 36 Monate überprüft die Kommission die Anwendung dieser Richtlinie und erstattet dem Europäischen Parlament und dem Rat Bericht. In dem Bericht wird insbesondere die Relevanz der Größe der betreffenden Einrichtungen, und der Sektoren, der Teilsektoren und der Arten der in den Anhängen I und II genannten Einrichtung für das Funktionieren der Wirtschaft und Gesellschaft in Bezug auf die Cybersicherheit bewertet. Zu diesem Zweck berücksichtigt die Kommission im Hinblick auf die weitere Förderung der strategischen und operativen Zusammenarbeit die Berichte der Kooperationsgruppe und des CSIRTs-Netzwerks über die auf strategischer und operativer Ebene gemachten Erfahrungen. Dem Bericht ist erforderlichenfalls ein Gesetzgebungsvorschlag beizufügen.

Artikel 41
Umsetzung

(1) Bis zum 17. Oktober 2024 erlassen und veröffentlichen die Mitgliedstaaten die erforderlichen Vorschriften, um dieser Richtlinie nachzukommen. Sie setzen die Kommission unverzüglich davon in Kenntnis.

Sie wenden diese Vorschriften ab dem 18. Oktober 2024 an.

(2) Bei Erlass der in Absatz 1 genannten Vorschriften nehmen die Mitgliedstaaten in den Vorschriften selbst oder durch einen Hinweis bei der amtlichen Veröffentlichung auf diese Richtlinie Bezug. Die Mitgliedstaaten regeln die Einzelheiten dieser Bezugnahme.

Artikel 42 & 43

[Vom Abdruck wurde abgesehen]

Artikel 44
Aufhebung

Die Richtlinie (EU) 2016/1148 wird mit Wirkung vom 18. Oktober 2024 aufgehoben.

Bezugnahmen auf die durch die vorliegende Richtlinie aufgehobene Richtlinie gelten als Bezugnahmen auf die vorliegende Richtlinie und sind nach Maßgabe der Entsprechungstabelle in Anhang III zu lesen.

Artikel 45
Inkrafttreten

Diese Richtlinie tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.

Artikel 46
Adressaten

Diese Richtlinie ist an die Mitgliedstaaten gerichtet.

ANHANG I
SEKTOREN MIT HOHER KRITIKALITÄT

Sektor	Teilsektor	Art der Einrichtung
1. Energie	a) Elektrizität	— Elektrizitätsunternehmen im Sinne des Artikels 2 Nummer 57 der Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates, die die Funktion „Versorgung“ im Sinne des Artikels 2 Nummer 12 jener Richtlinie wahrnehmen
		— Verteilernetzbetreiber im Sinne von Artikel 2 Nummer 29 der Richtlinie (EU) 2019/944
		— Übertragungsnetzbetreiber im Sinne des Artikels 2 Nummer 35 der Richtlinie (EU) 2019/944
		— Erzeuger im Sinne des Artikels 2 Nummer 38 der Richtlinie (EU) 2019/944
		— nominierte Strommarktbetreiber im Sinne des Artikels 2 Nummer 8 der Verordnung (EU) 2019/943 des Europäischen Parlaments und des Rates — Marktteilnehmer im Sinne des Artikels 2 Nummer 25 der Verordnung (EU) 2019/943, die Aggregierungs-, Laststeuerungs- oder Energiespeicherungsdienste im Sinne des Artikels 2

		Nummern 18, 20 und 59 der Richtlinie (EU) 2019/944 anbieten — Betreiber von Ladepunkten, die für die Verwaltung und den Betrieb eines Ladepunkts zuständig sind und Endnutzern einen Aufladedienst erbringen, auch im Namen und Auftrag eines Mobilitätsdienstleisters
	b) Fernwärme und -kälte	— Betreiber von Fernwärme oder Fernkälte im Sinne des Artikels 2 Nummer 19 der Richtlinie (EU) 2018/2001 des Europäischen Parlaments und des Rates
	c) Erdöl	— Betreiber von Erdöl-Fernleitungen
		— Betreiber von Anlagen zur Produktion, Raffination und Aufbereitung von Erdöl sowie Betreiber von Erdöllagern und Erdöl-Fernleitungen
		— zentrale Bevorratungsstellen im Sinne des Artikels 2 Buchstabe f der Richtlinie 2009/119/EG des Rates
	d) Erdgas	— Versorgungsunternehmen im Sinne des Artikels 2 Nummer 8 der Richtlinie 2009/73/EG des Europäischen Parlaments und des Rates
		— Verteilernetzbetreiber im Sinne des Artikels 2 Nummer 6 der Richtlinie 2009/73/EG
		— Fernleitungsnetzbetreiber im Sinne des Artikels 2 Nummer 4 der Richtlinie 2009/73/EG
		— Betreiber einer Speicheranlage im Sinne des Artikels 2 Nummer 10 der Richtlinie 2009/73/EG
		— Betreiber einer LNG-Anlage im Sinne des Artikels 2 Nummer 12 der Richtlinie 2009/73/EG
		— Erdgasunternehmen im Sinne des Artikels 2 Nummer 1 der Richtlinie 2009/73/EG
		— Betreiber von Anlagen zur Raffination und Aufbereitung von Erdgas
	e) Wasserstoff	— Betreiber im Bereich Wasserstofferzeugung, -speicherung und -fernleitung
2. Verkehr	a) Luftverkehr	— Luftfahrtunternehmen im Sinne des Artikels 3 Nummer 4 der Verordnung (EG) Nr. 300/2008, die für gewerbliche Zwecke genutzt werden
		— Flughafenleitungsorgane im Sinne des Artikels 2 Nummer 2 der Richtlinie 2009/12/EG des Europäischen Parlaments und des Rates, Flughäfen im Sinne des Artikels 2 Nummer 1 jener Richtlinie, einschließlich der in Anhang II Abschnitt 2 der Verordnung (EU) Nr. 1315/2013 des Europäischen Parlaments und des Rates aufgeführten Flughäfen des Kernnetzes, und Einrichtungen, die innerhalb von Flughäfen befindliche zugehörige Einrichtungen betreiben
		— Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen, die Flugverkehrskontrolldienste im Sinne des Artikels 2 Nummer 1 der Verordnung (EG)

		Nr. 549/2004 des Europäischen Parlaments und des Rates bereitstellen
	b) Schienenverkehr	— Infrastrukturbetreiber im Sinne des Artikels 3 Nummer 2 der Richtlinie 2012/34/EU des Europäischen Parlaments und des Rates
		— Eisenbahnunternehmen im Sinne des Artikels 3 Nummer 1 der Richtlinie 2012/34/EU, einschließlich Betreiber einer Serviceeinrichtung im Sinne des Artikels 3 Nummer 12 jener Richtlinie
	c) Schifffahrt	— Passagier- und Frachtbeförderungsunternehmen der Binnen-, See- und Küstenschifffahrt, wie sie in Anhang I der Verordnung (EG) Nr. 725/2004 des Europäischen Parlaments und des Rates für die Schifffahrt definiert sind, ausschließlich der einzelnen von diesen Unternehmen betriebenen Schiffe
		— Leitungsorgane von Häfen im Sinne des Artikels 3 Nummer 1 der Richtlinie 2005/65/EG des Europäischen Parlaments und des Rates, einschließlich ihrer Hafenanlagen im Sinne des Artikels 2 Nummer 11 der Verordnung (EG) Nr. 725/2004, sowie Einrichtungen, die innerhalb von Häfen befindliche Anlagen und Ausrüstung betreiben
		— Betreiber von Schiffsverkehrsdiensten im Sinne des Artikels 3 Buchstabe o der Richtlinie 2002/59/EG des Europäischen Parlaments und des Rates
	d) Straßenverkehr	— Straßenverkehrsbehörden im Sinne des Artikels 2 Nummer 12 der Delegierten Verordnung (EU) 2015/962 der Kommission, die für Verkehrsmanagement und Verkehrssteuerung verantwortlich sind, ausgenommen öffentliche Einrichtungen, für die das Verkehrsmanagement oder der Betrieb intelligenter Verkehrssysteme ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit ist
		— Betreiber intelligenter Verkehrssysteme im Sinne des Artikels 4 Nummer 1 der Richtlinie 2010/40/EU des Europäischen Parlaments und des Rates
3. Bankwesen		Kreditinstitute im Sinne von Artikel 4 Nummer 1 der Verordnung (EU) Nr. 575/2013 des Europäischen Parlaments und des Rates
4. Finanzmarktinfrastrukturen		— Betreiber von Handelsplätzen im Sinne des Artikels 4 Nummer 24 der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates
		— zentrale Gegenparteien im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) Nr. 648/2012 des Europäischen Parlaments und des Rates
5. Gesundheitswesen		— Gesundheitsdienstleister im Sinne des Artikels 3 Buchstabe g der Richtlinie 2011/24/EU des Europäischen Parlaments und des Rates
		— EU-Referenzlaboratorien im Sinne des Artikels 15 der Verordnung (EU) 2022/2371 des Europäischen Parlaments und des Rates

		— Einrichtungen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel im Sinne des Artikels 1 Nummer 2 der Richtlinie 2001/83/EG des Europäischen Parlaments und des Rates ausüben — Einrichtungen, die pharmazeutische Erzeugnisse im Sinne des Abschnitts C Abteilung 21 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) herstellen — Einrichtungen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch im Sinne des Artikels 22 der Verordnung (EU) 2022/123 des Europäischen Parlaments und des Rates („Liste kritischer Medizinprodukte für Notlagen im Bereich der öffentlichen Gesundheit“) eingestuft werden
6. Trinkwasser		Lieferanten von und Unternehmen der Versorgung mit „Wasser für den menschlichen Gebrauch“ im Sinne des Artikels 2 Nummer 1 Buchstabe a der Richtlinie (EU) 2020/2184 des Europäischen Parlaments und des Rates, 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
7. Abwasser		Unternehmen, die kommunales Abwasser, häusliches Abwasser oder industrielles Abwasser im Sinne des Artikels 2 Nummern 1, 2 und 3 der Richtlinie 91/271/EWG des Rates 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
8. Digitale Infrastruktur		— Betreiber von Internet-Knoten — DNS-Diensteanbieter, ausgenommen Betreiber von Root-Namenservern — TLD-Namenregister — Anbieter von Cloud-Computing-Diensten — Anbieter von Rechenzentrumsdiensten — Betreiber von Inhaltszustellnetzen — Vertrauensdiensteanbieter — Anbieter öffentlicher elektronischer Kommunikationsnetze oder — Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste
9. Verwaltung von IKT-Diensten (Business-to-Business)		— Anbieter verwalteter Dienste — Anbieter verwalteter Sicherheitsdienste
10. öffentliche		— Einrichtungen der öffentlichen Verwaltung von Zentralregierungen entsprechend der Definition eines

Verwaltung		Mitgliedstaats gemäß nationalem Recht
		— Einrichtungen der öffentlichen Verwaltung auf regionaler Ebene entsprechend der Definition eines Mitgliedstaats gemäß nationalem Recht
11. Weltraum		Betreiber von Bodeninfrastrukturen, die sich im Eigentum von Mitgliedstaaten oder privaten Parteien befinden und von diesen verwaltet und betrieben werden und die Erbringung von weltraumgestützten Diensten unterstützen, ausgenommen Anbieter öffentlicher elektronischer Kommunikationsnetze

ANHANG II
SONSTIGE KRITISCHE SEKTOREN

Sektor	Teilsektor	Art der Einrichtung
1. Post- und Kurierdienste		Anbieter von Postdiensten im Sinne des Artikels 2 Nummer 1a der Richtlinie 97/67/EG, einschließlich Anbieter von Kurierdiensten
2. Abfallbewirtschaftung		Unternehmen der Abfallbewirtschaftung im Sinne des Artikels 3 Nummer 9 der Richtlinie 2008/98/EG des Europäischen Parlaments und des Rates, ausgenommen Unternehmen, für die Abfallbewirtschaftung nicht ihre Hauptwirtschaftstätigkeit ist
3. Produktion, Herstellung und Handel mit chemischen Stoffen		Unternehmen im Sinne des Artikels 3 Nummern 9 und 14 der Verordnung (EG) Nr. 1907/2006 des Europäischen Parlaments und des Rates, die Stoffe herstellen und mit Stoffen oder Gemischen handeln, und Unternehmen, die Erzeugnisse im Sinne des Artikels 3 Nummer 3 der genannten Verordnung aus Stoffen oder Gemischen produzieren
4. Produktion, Verarbeitung und Vertrieb von Lebensmitteln		Lebensmittelunternehmen im Sinne des Artikels 3 Nummer 2 der Verordnung (EG) Nr. 178/2002 des Europäischen Parlaments und des Rates, die im Großhandel sowie in der industriellen Produktion und Verarbeitung tätig sind
5. Verarbeitendes Gewerbe/Herstellung von Waren	a) Herstellung von Medizinprodukten und In-vitro-Diagnostika	Einrichtungen, die Medizinprodukte im Sinne des Artikels 2 Nummer 1 der Verordnung (EU) 2017/745 des Europäischen Parlaments und des Rates herstellen, und Einrichtungen, die In-vitro-Diagnostika im Sinne des Artikels 2 Nummer 2 der Verordnung (EU) 2017/746 des Europäischen

		Parlaments und des Rates herstellen, mit Ausnahme der unter Anhang I Nummer 5 fünfter Gedankenstrich dieser Richtlinie aufgeführten Einrichtungen, die Medizinprodukte herstellen
	b) Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 26 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
	c) Herstellung von elektrischen Ausrüstungen	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
	d) Maschinenbau	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 28 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
	e) Herstellung von Kraftwagen und Kraftwagenteilen	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 29 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
	f) sonstiger Fahrzeugbau	Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 30 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft (NACE Rev. 2) ausüben
6. Anbieter digitaler Dienste		— Anbieter von Online-Marktplätzen
		— Anbieter von Online-Suchmaschinen
		— Anbieter von Plattformen für Dienste sozialer Netzwerke
7. Forschung		Forschungseinrichtungen

ANHANG III
ENTSPRECHUNGSTABELLE

[Vom Abdruck wurde abgesehen.]

Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG)

Inhaltsübersicht

§ 1 Bundesamt für Sicherheit in der Informationstechnik

§ 2 Begriffsbestimmungen

§ 3 Aufgaben des Bundesamtes

§ 3a Verarbeitung personenbezogener Daten

§ 4 Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes

§ 4a Kontrolle der Kommunikationstechnik des Bundes, Betretensrechte

§ 4b Allgemeine Meldestelle für die Sicherheit in der Informationstechnik

§ 5 Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes

§ 5a Verarbeitung behördeninterner Protokollierungsdaten

§ 5b Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen

§ 5c Bestandsdatenauskunft

§ 6 Beschränkungen der Rechte der betroffenen Person

§ 6a Informationspflicht bei Erhebung von personenbezogenen Daten

§ 6b Auskunftsrecht der betroffenen Person

§ 6c Recht auf Berichtigung

§ 6d Recht auf Löschung

§ 6e Recht auf Einschränkung der Verarbeitung

§ 6f Widerspruchsrecht

§ 7 Warnungen

§ 7a Untersuchung der Sicherheit in der Informationstechnik

§ 7b Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden

§ 7c Anordnungen des Bundesamtes gegenüber Diensteanbietern

§ 7d Anordnungen des Bundesamtes gegenüber Anbietern von Telemediendiensten

§ 8 Vorgaben des Bundesamtes

§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen

§ 8b Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen

§ 8c Besondere Anforderungen an Anbieter digitaler Dienste

§ 8d Anwendungsbereich

§ 8e Auskunftsverlangen

§ 8f Sicherheit in der Informationstechnik bei Unternehmen im besonderen öffentlichen Interesse

§ 9 Zertifizierung
§ 9a Nationale Behörde für die Cybersicherheitszertifizierung
§ 9b Untersagung des Einsatzes kritischer Komponenten
§ 9c Freiwilliges IT-Sicherheitskennzeichen
§ 10 Ermächtigung zum Erlass von Rechtsverordnungen
§ 11 Einschränkung von Grundrechten
§ 12 Rat der IT-Beauftragten der Bundesregierung
§ 13 Berichtspflichten
§ 14 Bußgeldvorschriften
§ 14a Institutionen der Sozialen Sicherung
§ 15 Anwendbarkeit der Vorschriften für Anbieter digitaler Dienste

§ 1 Bundesamt für Sicherheit in der Informationstechnik

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

§ 2 Begriffsbestimmungen

(1) Die Informationstechnik im Sinne dieses Gesetzes umfasst alle technischen Mittel zur Verarbeitung von Informationen.

(2) Informationen sowie informationsverarbeitende Systeme, Komponenten und Prozesse sind besonders schützenswert. Der Zugriff auf diese darf ausschließlich durch autorisierte Personen oder Programme erfolgen. Die Sicherheit in der Informationstechnik und der damit verbundene Schutz von Informationen und informationsverarbeitenden Systemen vor Angriffen und unautorisierten Zugriffen im Sinne dieses Gesetzes erfordert die Einhaltung bestimmter Sicherheitsstandards zur Gewährleistung der informationstechnischen Grundwerte und Schutzziele. Sicherheit in der Informationstechnik im Sinne dieses Gesetzes bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen

1. in informationstechnischen Systemen, Komponenten oder Prozessen oder
2. bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen.

(3) Kommunikationstechnik des Bundes im Sinne dieses Gesetzes ist die Informationstechnik, die von einer oder mehreren Bundesbehörden oder im Auftrag einer oder mehrerer Bundesbehörden betrieben wird und der Kommunikation oder dem Datenaustausch innerhalb einer Bundesbehörde, der Bundesbehörden untereinander oder der Bundesbehörden mit Dritten dient. Kommunikationstechnik des Bundesverfassungsgerichts, der Bundesgerichte, soweit sie nicht öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen, des Bundes-

tages, des Bundesrates, des Bundespräsidenten und des Bundesrechnungshofes ist nicht Kommunikationstechnik des Bundes, soweit sie ausschließlich in deren eigener Zuständigkeit betrieben wird.

(4) Schnittstellen der Kommunikationstechnik des Bundes im Sinne dieses Gesetzes sind sicherheitsrelevante Netzwerkübergänge innerhalb der Kommunikationstechnik des Bundes sowie zwischen dieser und der Informationstechnik der einzelnen Bundesbehörden, Gruppen von Bundesbehörden oder Dritter. Dies gilt nicht für die Komponenten an den Netzwerkübergängen, die in eigener Zuständigkeit der in Absatz 3 Satz 2 genannten Gerichte und Verfassungsorgane betrieben werden.

(5) Schadprogramme im Sinne dieses Gesetzes sind Programme und sonstige informationstechnische Routinen und Verfahren, die dem Zweck dienen, unbefugt Daten zu nutzen oder zu löschen oder die dem Zweck dienen, unbefugt auf sonstige informationstechnische Abläufe einzuwirken.

(6) Sicherheitslücken im Sinne dieses Gesetzes sind Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Dritte gegen den Willen des Berechtigten Zugang zu fremden informationstechnischen Systemen verschaffen oder die Funktion der informationstechnischen Systeme beeinflussen können.

(7) Zertifizierung im Sinne dieses Gesetzes ist die Feststellung durch eine Zertifizierungsstelle, dass ein Produkt, ein Prozess, ein System, ein Schutzprofil (Sicherheitszertifizierung), eine Person (Personenzertifizierung) oder ein IT-Sicherheitsdienstleister bestimmte Anforderungen erfüllt.

(8) Protokolldaten im Sinne dieses Gesetzes sind Steuerdaten eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind. Protokolldaten können Verkehrsdaten gemäß § 3 Nummer 70 des Telekommunikationsgesetzes und Nutzungsdaten nach § 2 Absatz 2 Nummer 3 des Telekommunikation-Telemedien-Datenschutz-Gesetzes enthalten.

(8a) Protokollierungsdaten im Sinne dieses Gesetzes sind Aufzeichnungen über technische Ereignisse oder Zustände innerhalb informationstechnischer Systeme.

(9) Datenverkehr im Sinne dieses Gesetzes sind die mittels technischer Protokolle übertragenen Daten. Der Datenverkehr kann Telekommunikationsinhalte nach § 3 Absatz 1 des Telekommunikation-Telemedien-Datenschutz-Gesetzes und Nutzungsdaten nach § 2 Absatz 2 Nummer 3 des Telekommunikation-Telemedien-Datenschutz-Gesetzes enthalten.

(9a) IT-Produkte im Sinne dieses Gesetzes sind Software, Hardware sowie alle einzelnen oder miteinander verbundenen Komponenten, die Informationen informationstechnisch verarbeiten.

(9b) Systeme zur Angriffserkennung im Sinne dieses Gesetzes sind durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme. Die Angriffserkennung erfolgt dabei durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten.

(10) Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die

1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung angehören und
2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmt.

(11) Digitale Dienste im Sinne dieses Gesetzes sind Dienste im Sinne von Artikel 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1), und die

1. es Verbrauchern oder Unternehmern im Sinne des Artikels 4 Absatz 1 Buchstabe a beziehungsweise Buchstabe b der Richtlinie 2013/11/EU des Europäischen Parlaments und des Rates vom 21. Mai 2013 über die alternative Beilegung verbraucherrechtlicher Streitigkeiten und zur Änderung der Verordnung (EG) Nr. 2006/2004 und der Richtlinie 2009/22/EG (Richtlinie über alternative Streitbeilegung in Verbraucherangelegenheiten) (ABl. L 165 vom 18.6.2013, S. 63) ermöglichen, Kaufverträge oder Dienstleistungsverträge mit Unternehmern entweder auf der Webseite dieser Dienste oder auf der Webseite eines Unternehmers, die von diesen Diensten bereitgestellte Rechendienste verwendet, abzuschließen (Online-Marktplätze);
2. es Nutzern ermöglichen, Suchen grundsätzlich auf allen Webseiten oder auf Webseiten in einer bestimmten Sprache anhand einer Abfrage zu einem beliebigen Thema in Form eines Stichworts, einer Wortgruppe oder einer anderen Eingabe vorzunehmen, die daraufhin Links anzeigen, über die der Abfrage entsprechende Inhalte abgerufen werden können (Online-Suchmaschinen);
3. den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglichen (Cloud-Computing-Dienste),

und nicht zum Schutz grundlegender staatlicher Funktionen eingerichtet worden sind oder für diese genutzt werden.

(12) „Anbieter digitaler Dienste“ im Sinne dieses Gesetzes ist eine juristische Person, die einen digitalen Dienst anbietet.

(13) Kritische Komponenten im Sinne dieses Gesetzes sind IT-Produkte,

1. die in Kritischen Infrastrukturen eingesetzt werden,
2. bei denen Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit Kritischer Infrastrukturen oder zu Gefährdungen für die öffentliche Sicherheit führen können und
3. die auf Grund eines Gesetzes unter Verweis auf diese Vorschrift

a) als kritische Komponente bestimmt werden oder

b) eine auf Grund eines Gesetzes als kritisch bestimmte Funktion realisieren.

Werden für einen der in Absatz 10 Satz 1 Nummer 1 genannten Sektoren keine kritischen Komponenten und keine kritischen Funktionen, aus denen kritische Komponenten abgeleitet werden können, auf Grund eines Gesetzes unter Verweis auf diese Vorschrift bestimmt, gibt es in diesem Sektor keine kritischen Komponenten im Sinne dieses Gesetzes.

(14) Unternehmen im besonderen öffentlichen Interesse sind Unternehmen, die nicht Betreiber Kritischer Infrastrukturen nach Absatz 10 sind und

1. die Güter nach § 60 Absatz 1 Nummer 1 und 3 der Außenwirtschaftsverordnung in der jeweils geltenden Fassung herstellen oder entwickeln,
2. die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland sind oder die für solche Unternehmen als Zulieferer wegen ihrer Alleinstellungsmerkmale von wesentlicher Bedeutung sind oder
3. die Betreiber eines Betriebsbereichs der oberen Klasse im Sinne der Störfall-Verordnung in der jeweils geltenden Fassung sind oder nach § 1 Absatz 2 der Störfall-Verordnung diesen gleichgestellt sind.

Die Unternehmen im besonderen öffentlichen Interesse nach Satz 1 Nummer 2 werden durch die Rechtsverordnung nach § 10 Absatz 5 bestimmt, in der festgelegt wird, welche wirtschaftlichen Kennzahlen maßgeblich dafür sind, dass ein Unternehmen zu den größten Unternehmen in Deutschland im Sinne der Nummer 2 gehört und welche Alleinstellungsmerkmale maßgeblich dafür sind, dass Zulieferer für solche Unternehmen von wesentlicher Bedeutung sind.

§ 3 Aufgaben des Bundesamtes

(1) Das Bundesamt fördert die Sicherheit in der Informationstechnik mit dem Ziel, die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen und deren Verarbeitung zu gewährleisten. Hierzu nimmt es folgende wichtige im öffentlichen Interesse liegende Aufgaben wahr:

1. Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes;
2. Sammlung und Auswertung von Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen und Zurverfügungstellung der gewonnenen Erkenntnisse für andere Stellen, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist, sowie für Dritte, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist;
3. Untersuchung von Sicherheitsrisiken bei Anwendung der Informationstechnik sowie Entwicklung von Sicherheitsvorkehrungen, insbesondere von informationstechnischen Verfahren und Geräten für die Sicherheit in der Informationstechnik (IT-Sicherheitsprodukte), soweit dies zur Erfüllung von Aufgaben des Bundes erforderlich ist, einschließlich der Forschung im Rahmen seiner gesetzlichen Aufgaben;
4. Entwicklung von Kriterien, Verfahren und Werkzeugen für die Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen oder Komponen-

ten und für die Prüfung und Bewertung der Konformität im Bereich der IT-Sicherheit;

5. Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen oder Komponenten und Erteilung von Sicherheitszertifikaten;

5a. Wahrnehmung der Aufgaben und Befugnisse nach Artikel 58 Absatz 7 und 8 der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit, ABl. L 151 vom 7.6.2019, S. 15) als nationale Behörde für die Cybersicherheitszertifizierung;

6. Prüfung und Bestätigung der Konformität im Bereich der IT-Sicherheit von informationstechnischen Systemen und Komponenten mit technischen Richtlinien des Bundesamtes;

7. Prüfung, Bewertung und Zulassung von informationstechnischen Systemen oder Komponenten, die für die Verarbeitung amtlich geheim gehaltener Informationen nach § 4 des Sicherheitsüberprüfungsgesetzes im Bereich des Bundes oder bei Unternehmen im Rahmen von Aufträgen des Bundes eingesetzt werden sollen;

8. Herstellung von Schlüsseldaten und Betrieb von Krypto- und Sicherheitsmanagementsystemen für informationssichernde Systeme des Bundes, die im Bereich des staatlichen Geheimschutzes oder auf Anforderung der betroffenen Behörde auch in anderen Bereichen eingesetzt werden;

9. Unterstützung und Beratung bei organisatorischen und technischen Sicherheitsmaßnahmen sowie Durchführung von technischen Prüfungen zum Schutz amtlich geheim gehaltener Informationen nach § 4 des Sicherheitsüberprüfungsgesetzes gegen die Kenntnisnahme durch Unbefugte;

10. Entwicklung von sicherheitstechnischen Anforderungen an die einzusetzende Informationstechnik des Bundes und an die Eignung von Auftragnehmern im Bereich von Informationstechnik mit besonderem Schutzbedarf;

11. Bereitstellung von IT-Sicherheitsprodukten für Stellen des Bundes;

12. Unterstützung der für Sicherheit in der Informationstechnik zuständigen Stellen des Bundes, insbesondere soweit sie Beratungs- oder Kontrollaufgaben wahrnehmen; dies gilt vorrangig für den Bundesbeauftragten für den Datenschutz, dessen Unterstützung im Rahmen der Unabhängigkeit erfolgt, die ihm bei der Erfüllung seiner Aufgaben nach dem Bundesdatenschutzgesetz zusteht;

12a. Beratung und Unterstützung der Stellen des Bundes in Fragen der Sicherheit in der Informationstechnik;

13. Unterstützung

   a) der Polizeien und Strafverfolgungsbehörden bei der Wahrnehmung ihrer gesetzlichen Aufgaben,

   b) der Verfassungsschutzbehörden und des Militärischen Abschirmdienstes bei der Auswertung und Bewertung von Informationen, die bei der Beobachtung

terroristischer Bestrebungen oder nachrichtendienstlicher Tätigkeiten im Rahmen der gesetzlichen Befugnisse nach den Verfassungsschutzgesetzen des Bundes und der Länder beziehungsweise dem MAD-Gesetz anfallen,

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;

13a. auf Ersuchen der zuständigen Stellen der Länder Unterstützung dieser Stellen in Fragen der Abwehr von Gefahren für die Sicherheit in der Informationstechnik;

14. Beratung, Information und Warnung der Stellen des Bundes, der Länder sowie der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik, insbesondere unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen;

14a. Verbraucherschutz und Verbraucherinformation im Bereich der Sicherheit in der Informationstechnik, insbesondere durch Beratung und Warnung von Verbrauchern in Fragen der Sicherheit in der Informationstechnik und unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen;

15. Aufbau geeigneter Kommunikationsstrukturen zur Krisenfrüherkennung, Krisenreaktion und Krisenbewältigung sowie Koordinierung der Zusammenarbeit zum Schutz der Sicherheit in der Informationstechnik Kritischer Infrastrukturen im Verbund mit der Privatwirtschaft;

16. Aufgaben als zentrale Stelle im Bereich der Sicherheit in der Informationstechnik im Hinblick auf die Zusammenarbeit mit den zuständigen Stellen im Ausland, unbeschadet besonderer Zuständigkeiten anderer Stellen;

17. Aufgaben nach den §§ 8a bis 8c und 8f als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen, digitaler Dienste und der Unternehmen im besonderen öffentlichen Interesse;

18. Unterstützung bei der Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen nach § 5a;

19. Empfehlungen für Identifizierungs- und Authentisierungsverfahren und Bewertung dieser Verfahren im Hinblick auf die Informationssicherheit;

20. Beschreibung und Veröffentlichung eines Stands der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte unter Berücksichtigung bestehender Normen und Standards sowie Einbeziehung der betroffenen Wirtschaftsverbände.

(2) Das Bundesamt kann die Länder auf Ersuchen bei der Sicherung ihrer Informationstechnik unterstützen.

(3) Das Bundesamt kann Betreiber Kritischer Infrastrukturen auf deren Ersuchen bei der Sicherung ihrer Informationstechnik beraten und unterstützen oder auf qualifizierte Sicherheitsdienstleister verweisen.

§ 3a 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 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2) in der jeweils geltenden Fassung und von § 23 des Bundesdatenschutzgesetzes zulässig, wenn

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.

§ 4 Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes

(1) Das Bundesamt ist die zentrale Meldestelle für die Zusammenarbeit der Bundesbehörden 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 Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und der dabei beobachteten Vorgehensweise, zu sammeln und auszuwerten,

2. die Bundesbehörden unverzüglich über die sie betreffenden Informationen nach Nummer 1 und die in Erfahrung gebrachten Zusammenhänge zu unterrichten.

(3) Werden anderen Bundesbehörden Informationen nach Absatz 2 Nummer 1 bekannt, die für die Erfüllung von Aufgaben oder die Sicherheit der Informationstechnik anderer Behörden von Bedeutung sind, unterrichten diese ab dem 1. Januar 2010 das Bundesamt hierüber unverzüglich, soweit andere Vorschriften dem nicht entgegenstehen.

(4) Ausgenommen von den Unterrichtungspflichten nach Absatz 2 Nummer 2 und Absatz 3 sind Informationen, die aufgrund von Regelungen zum Geheimschutz oder Vereinbarungen mit Dritten nicht weitergegeben werden dürfen oder deren Weitergabe im Widerspruch zu der verfassungsrechtlichen Stellung eines Abgeordneten des Bundestages oder eines Verfassungsorgans oder der gesetzlich geregelten Unabhängigkeit einzelner Stellen stünde.

(5) Die Vorschriften zum Schutz personenbezogener Daten bleiben unberührt.

(6) Das Bundesministerium des Innern, für Bau und Heimat erlässt nach Zustimmung durch den Rat der IT-Beauftragten der Bundesregierung allgemeine Verwaltungsvorschriften zur Durchführung des Absatzes 3.

§ 4a 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 die Bereitstellung der zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1 und 14 erforderlichen Informationen, insbesondere zu technischen Details, zu Strategien, Planungen und Regelungen mit Bezug zur Kommunikationstechnik des Bundes einschließlich Aufbau- und Ablauforganisation verlangen sowie Unterlagen und Datenträger des Betreibers der jeweiligen Kommunikationstechnik des Bundes oder eines mit Betriebsleistungen beauftragten Dritten einsehen und die unentgeltliche Herausgabe von Kopien dieser Unterlagen und Dokumente, auch in elektronischer Form, verlangen, soweit nicht Geheimschutzinteressen oder überwiegende Sicherheitsinteressen des Betreibers im Sinne des Satzes 2 entgegenstehen.

(2) Dem Bundesamt ist in den Zeiten, zu denen die Räume normalerweise für die jeweilige geschäftliche oder betriebliche Nutzung zur Verfügung stehen, zu den Grundstücken und Betriebsräumen, einschließlich Datenverarbeitungsanlagen und -geräten, die für die Kommunikationstechnik des Bundes verwendet werden, Zugang zu gewähren, soweit dies zur Erfüllung der Zwecke nach Absatz 1 erforderlich ist.

(3) Bei Einrichtungen eines Dritten, bei dem eine Schnittstelle zur Kommunikationstechnik des Bundes besteht, kann das Bundesamt auf der Schnittstellenseite der Einrichtung nur mit Zustimmung des Dritten die Sicherheit der Schnittstelle kontrollieren. Es kann hierzu mit Zustimmung des Dritten die zur Aufgabenerfüllung erforderlichen Informationen, insbesondere zu technischen Details, zu Strategien, Planungen und Regelungen sowie Unterlagen und Datenträger des Betreibers einsehen und unentgeltlich Kopien, auch in elektronischer Form, anfertigen.

(4) Das Bundesamt teilt das Ergebnis seiner Kontrolle nach den Absätzen 1 bis 3 dem jeweiligen überprüften Betreiber sowie im Falle einer öffentlichen Stelle des Bundes der zuständigen Rechts- und Fachaufsicht mit. Mit der Mitteilung soll es Vorschläge zur Verbesserung

der Informationssicherheit, insbesondere zur Beseitigung der festgestellten Mängel, verbinden.

(5) Ausgenommen von den Befugnissen nach den Absätzen 1 bis 3 sind Kontrollen der Auslandsinformations- und -kommunikationstechnik im Sinne des § 9 Absatz 2 des Gesetzes über den Auswärtigen Dienst, soweit sie ausschließlich im Ausland belegen ist oder für das Ausland oder für Anwender im Ausland betrieben wird. Die Bestimmungen für die Schnittstellen der Kommunikationstechnik des Bundes im Inland bleiben davon unberührt. Näheres zu Satz 1 regelt eine Verwaltungsvereinbarung zwischen dem Bundesministerium des Innern, für Bau und Heimat und dem Auswärtigen Amt.

(6) Die Befugnisse nach den Absätzen 1 bis 3 gelten im Geschäftsbereich des Bundesministeriums der Verteidigung nicht für die Kontrolle der Informations- und Kommunikationstechnik, die von den Streitkräften für ihre Zwecke oder dem Militärischen Abschirmdienst genutzt wird. Nicht ausgenommen ist die Informations- und Kommunikationstechnik von Dritten, insbesondere von IT-Dienstleistern, soweit sie nicht ausschließlich für die Zwecke der Streitkräfte betrieben wird. Die Bestimmungen für die Schnittstellen der Kommunikationstechnik des Bundes bleiben von den Sätzen 1 und 2 unberührt. Näheres regelt eine Verwaltungsvereinbarung zwischen dem Bundesministerium des Innern, für Bau und Heimat und dem Bundesministerium der Verteidigung.

§ 4b 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.

(2) Das Bundesamt nimmt zur Wahrnehmung der Aufgaben nach Absatz 1 Informationen zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und der dabei beobachteten Vorgehensweisen entgegen. Das Bundesamt richtet hierzu geeignete Meldemöglichkeiten ein. Die Meldungen können anonym erfolgen. Soweit die Meldung nicht anonym erfolgt, kann der Meldende mit der Meldung oder später verlangen, dass seine personenbezogenen Daten nur anonymisiert weitergegeben werden dürfen. Dies gilt nicht in den Fällen des § 5 Absatz 5 und 6 Satz 1. Eine Übermittlung der personenbezogenen Daten in den Fällen von § 5 Absatz 5 und 6 Satz 1 hat zu unterbleiben, wenn für das Bundesamt erkennbar ist, dass die schutzwürdigen Interessen des Meldenden das Allgemeininteresse an der Übermittlung überwiegen. Zu berücksichtigen ist dabei auch die Art und Weise, mittels derer der Meldende die Erkenntnisse gewonnen hat. Die Entscheidung nach Satz 6 muss dem oder der behördlichen Datenschutzbeauftragten des Bundesamtes sowie einem oder einer weiteren Bediensteten des Bundesamtes, der oder die die Befähigung zum Richteramt hat, zur vorherigen Prüfung vorgelegt werden.

(3) Das Bundesamt soll die gemäß Absatz 2 gemeldeten Informationen nutzen, um

1. Dritte über bekannt gewordene Sicherheitslücken, Schadprogramme, erfolgte oder versuchte Angriffe auf die Sicherheit in der Informationstechnik zu informieren, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist,
2. die Öffentlichkeit oder betroffene Kreise gemäß § 7 zu warnen und zu informieren,
3. Bundesbehörden gemäß § 4 Absatz 2 Nummer 2 über die sie betreffenden Informationen zu unterrichten,

4. Betreiber Kritischer Infrastrukturen und Unternehmen im öffentlichen Interesse gemäß § 8b Absatz 2 Nummer 4 Buchstabe a über die sie betreffenden Informationen zu unterrichten.

(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. auf Grund von Vereinbarungen des Bundesamtes mit Dritten nicht übermittelt werden dürfen.

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

§ 5 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 erforderlich ist.

Sofern nicht die nachfolgenden Absätze eine weitere Verwendung gestatten, muss die automatisierte Auswertung dieser Daten unverzüglich erfolgen und müssen diese nach erfolgtem Abgleich sofort und spurenlos gelöscht werden. Die Verwendungsbeschränkungen gelten nicht für Protokolldaten, sofern diese weder personenbezogene noch dem Fernmeldegeheimnis unterliegende Daten beinhalten. Die Bundesbehörden sind verpflichtet, das Bundesamt bei Maßnahmen nach Satz 1 zu unterstützen und hierbei den Zugang des Bundesamtes zu behördeninternen Protokolldaten nach Satz 1 Nummer 1 sowie Schnittstellendaten nach Satz 1 Nummer 2 sicherzustellen. Protokolldaten der Bundesgerichte dürfen nur in deren Einvernehmen erhoben werden.

(2) Protokolldaten nach Absatz 1 Satz 1 Nummer 1 dürfen über den für die automatisierte Auswertung nach Absatz 1 Satz 1 Nummer 1 erforderlichen Zeitraum hinaus, längstens jedoch für 18 Monate, gespeichert werden, soweit tatsächliche Anhaltspunkte dafür bestehen, dass diese im Falle der Bestätigung eines Verdachts nach Absatz 3 Satz 2 zur Abwehr von Gefahren, die von dem gefundenen Schadprogramm ausgehen oder zur Erkennung und Abwehr anderer Schadprogramme erforderlich sein können. Durch organisatorische und technische Maßnahmen ist sicherzustellen, dass eine Auswertung der nach diesem Absatz gespeicherten Daten nur automatisiert erfolgt und dass ein Zugriff auf Daten, die länger als drei Monate gespeichert sind, nur bei Vorliegen tatsächlicher Erkenntnisse über die Betroffenheit des Bundes mit einem Schadprogramm erfolgt. Die Daten 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.

(2a) Protokolldaten dürfen vor ihrer Pseudonymisierung und Speicherung nach Absatz 2 zur Sicherstellung einer fehlerfreien automatisierten Auswertung manuell verarbeitet werden. Liegen Hinweise vor, dass die fehlerfreie automatisierte Auswertung wegen eines erheblichen Fehlers erschwert wird, darf der Personenbezug von Protokolldaten zur Sicherstellung der fehlerfreien automatisierten Auswertung wiederhergestellt werden, sofern dies im Einzelfall erforderlich ist. Absatz 2 Satz 3 bis 6 gilt entsprechend.

(3) Eine über die Absätze 1 und 2 hinausgehende Verwendung personenbezogener Daten ist nur zulässig, wenn bestimmte Tatsachen den Verdacht begründen, dass

1. diese ein Schadprogramm enthalten,
2. diese durch ein Schadprogramm übermittelt wurden oder
3. sich aus ihnen Hinweise auf ein Schadprogramm ergeben können,

und soweit die Datenverarbeitung erforderlich ist, um den Verdacht zu bestätigen oder zu widerlegen. Im Falle der Bestätigung ist die weitere Verarbeitung personenbezogener Daten zulässig, soweit dies

1. zur Abwehr des Schadprogramms,
2. zur Abwehr von Gefahren, die von dem aufgefundenen Schadprogramm ausgehen, oder
3. zur Erkennung und Abwehr anderer Schadprogramme erforderlich ist.

Ein Schadprogramm kann beseitigt oder in seiner Funktionsweise gehindert werden. Die nicht automatisierte Verwendung der Daten nach den Sätzen 1 und 2 darf nur durch einen Bediensteten des Bundesamtes mit der Befähigung zum Richteramt angeordnet werden.

(4) Die Beteiligten des Kommunikationsvorgangs sind spätestens nach dem Erkennen und der Abwehr eines Schadprogramms oder von Gefahren, die von einem Schadprogramm ausgehen, zu benachrichtigen, wenn sie bekannt sind oder ihre Identifikation ohne unverhältnismäßige weitere Ermittlungen möglich ist und nicht überwiegende schutzwürdige Belange Dritter entgegenstehen. Die Unterrichtung kann unterbleiben, wenn die Person nur unerheblich betroffen wurde, und anzunehmen ist, dass sie an einer Benachrichtigung kein Interesse hat. Das Bundesamt legt Fälle, in denen es von einer Benachrichtigung absieht, dem behördlichen Datenschutzbeauftragten des Bundesamtes sowie einem weiteren Bediensteten des Bundesamtes, der die Befähigung zum Richteramt hat, zur Kontrolle vor. Wenn der behördliche Datenschutzbeauftragte der Entscheidung des Bundesamtes widerspricht, ist die Benachrichtigung nachzuholen. Die Entscheidung über die Nichtbenachrichtigung ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist nach zwölf Monaten zu löschen. In den Fällen der Absätze 5 und 6 erfolgt die Benachrichtigung durch die dort genannten Behörden in entsprechender Anwendung der für diese Behörden geltenden Vorschriften. Enthalten diese keine Bestimmungen zu Benachrichtigungspflichten, sind die Vorschriften der Strafprozessordnung entsprechend anzuwenden.

(5) Das Bundesamt kann die nach Absatz 3 verwendeten personenbezogenen Daten an die Strafverfolgungsbehörden zur Verfolgung einer mittels eines Schadprogramms begangenen Straftat nach den §§ 202a, 202b, 303a oder 303b des Strafgesetzbuches übermitteln. Es kann diese Daten ferner übermitteln

1. zur Abwehr einer Gefahr für die öffentliche Sicherheit, die unmittelbar von einem Schadprogramm ausgeht, an die Polizeien des Bundes und der Länder,
2. zur Unterrichtung über Tatsachen, die sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht erkennen lassen, an das Bundesamt für Verfassungsschutz sowie an den Militärischen Abschirmdienst, wenn sich diese Tätigkeiten gegen Personen, Dienststellen oder Einrichtungen im Geschäftsbereich des Bundesministeriums der Verteidigung richten,
3. zur Unterrichtung über Tatsachen, die einen internationalen kriminellen, terroristischen oder staatlichen Angriff mittels Schadprogrammen oder vergleichbaren schädlich wirkenden informationstechnischen Mitteln auf die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Systemen in Fällen von erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland erkennen lassen, an den Bundesnachrichtendienst.

(6) Für sonstige Zwecke kann das Bundesamt die Daten 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 beziehungsweise § 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 1 Nummer 1 und 2 bedarf der vorherigen gerichtlichen Zustimmung. Für das Verfahren nach Satz 1 Nummer 1 und 2 gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Zuständig ist das Amtsgericht, in dessen Bezirk das Bundesamt seinen Sitz hat. Die Übermittlung nach Satz 1 Nummer 3 und Nummer 4 erfolgt nach Zustimmung des Bundesministeriums des Innern, für Bau und Heimat; die §§ 9 bis 16 des Artikel 10-Gesetzes gelten entsprechend.

(7) Eine über die vorstehenden Absätze hinausgehende inhaltliche Auswertung zu anderen Zwecken und die Weitergabe von personenbezogenen Daten an Dritte sind unzulässig. So-

weit möglich, ist technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Werden aufgrund der Maßnahmen der Absätze 1 bis 3 Erkenntnisse aus dem Kernbereich privater Lebensgestaltung oder Daten im Sinne des Artikels 9 Absatz 1 der Verordnung (EU) 2016/679 erlangt, dürfen diese nicht verwendet werden. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung sind unverzüglich zu löschen. Dies gilt auch in Zweifelsfällen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt. Werden im Rahmen der Absätze 4 oder 5 Inhalte oder Umstände der Kommunikation von in § 53 Absatz 1 Satz 1 der Strafprozessordnung genannten Personen übermittelt, auf die sich das Zeugnisverweigerungsrecht der genannten Personen erstreckt, ist die Verwertung dieser Daten zu Beweiszwecken in einem Strafverfahren nur insoweit zulässig, als Gegenstand dieses Strafverfahrens eine Straftat ist, die im Höchstmaß mit mindestens fünf Jahren Freiheitsstrafe bedroht ist.

(8) Vor Aufnahme der Datenerhebung und -verwendung hat das Bundesamt ein Datenerhebungs- und -verwendungskonzept zu erstellen und für Kontrollen durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit bereitzuhalten. Das Konzept hat dem besonderen Schutzbedürfnis der Regierungskommunikation Rechnung zu tragen. Die für die automatisierte Auswertung verwendeten Kriterien sind zu dokumentieren. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit teilt das Ergebnis seiner Kontrollen nach § 16 des Bundesdatenschutzgesetzes auch dem Rat der IT-Beauftragten der Bundesregierung mit.

(9) Das Bundesamt unterrichtet 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 5 Satz 1, Absatz 5 Satz 2 Nummer 1 oder Absatz 6 Nummer 1 übermittelt wurden, aufgegliedert nach den einzelnen Übermittlungsbefugnissen,
2. die Anzahl der personenbezogenen Auswertungen nach Absatz 3 Satz 1, in denen der Verdacht widerlegt wurde,
3. die Anzahl der Fälle, in denen das Bundesamt nach Absatz 4 Satz 2 oder 3 von einer Benachrichtigung der Betroffenen abgesehen hat.

(10) Das Bundesamt unterrichtet kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres den Innenausschuss des Deutschen Bundestages über die Anwendung dieser Vorschrift.

§ 5a Verarbeitung behördeninterner Protokollierungsdaten

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 Sicher-

heitsinteressen der betroffenen Stellen nicht entgegenstehen. Die Bundesbehörden sind verpflichtet, das Bundesamt bei Maßnahmen nach Satz 1 zu unterstützen und hierbei den Zugang des Bundesamtes zu behördeninternen Protokollierungsdaten nach Satz 1 sicherzustellen. Hierzu dürfen sie dem Bundesamt die entsprechenden Protokollierungsdaten übermitteln. § 5 Absatz 1 Satz 5, Absatz 2 bis 4, 8 und 9 gilt entsprechend. § 4a Absatz 6 gilt für die Verpflichtung nach Satz 2 entsprechend.

§ 5b 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 Stelle des Bundes oder eines Betreibers einer Kritischen Infrastruktur oder eines Unternehmens im besonderen öffentlichen Interesse um einen herausgehobenen Fall, so kann das Bundesamt auf Ersuchen der betroffenen Stelle oder des betroffenen Betreibers die Maßnahmen treffen, die zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich sind. Soweit das Bundesamt erste Maßnahmen zur Schadensbegrenzung und Sicherstellung des 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 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 erheben und verarbeiten, soweit dies zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich und angemessen ist. Die Daten sind unverzüglich zu löschen, sobald sie für die Wiederherstellung der Sicherheit oder Funktionsfähigkeit des informationstechnischen Systems nicht mehr benötigt werden. Wenn die Daten in Fällen des Absatzes 4 an eine andere Behörde zur Erfüllung von deren gesetzlichen Aufgaben weitergegeben worden sind, darf das Bundesamt die Daten abweichend von Satz 2 bis zur Beendigung der Unterstützung dieser Behörden weiterverarbeiten. Eine Nutzung zu anderen Zwecken ist unzulässig. § 5 Absatz 7 ist entsprechend anzuwenden.

(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 § 5 Absatz 5 und 6 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 es darum ersucht wurde und es sich um einen herausgehobenen Fall im Sinne des Absatzes 2 handelt. Ein begründeter Einzelfall liegt in der Regel vor, wenn eine Stelle eines Landes betroffen ist.

(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 § 5b die Vorgaben aufgrund des Atomgesetzes Vorrang.

§ 5c Bestandsdatenauskunft

(1) Das Bundesamt darf zur Erfüllung seiner gesetzlichen Aufgabe nach § 3 Absatz 1 Satz 1 Nummer 1, 2, 14, 17 oder 18 von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, über Bestandsdaten gemäß § 3 Nummer 6 des Telekommunikationsgesetzes und über die nach § 172 des Telekommunikationsgesetzes erhobenen Daten (§ 174 Absatz 1 Satz 1 des Telekommunikationsgesetzes) Auskunft verlangen. Die Auskunft nach Satz 1 darf nur verlangt werden zum Schutz der Versorgung der Bevölkerung in den Bereichen des § 2 Absatz 10 Satz 1 Nummer 1 oder der öffentlichen Sicherheit, um damit eine Beeinträchtigung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme

1. einer Kritischen Infrastruktur oder
2. eines Unternehmens von besonderem öffentlichem Interesse

abzuwenden, wenn Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, das auf die informationstechnischen Systeme bestimmbarer Infrastrukturen oder Unternehmen abzielen wird, und die in die Auskunft aufzunehmenden Daten im Einzelfall erforderlich sind, um die Betroffenen nach Absatz 4 vor dieser Beeinträchtigung zu warnen, über diese zu informieren oder sie bei deren 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 auf Grund eines Auskunftsverlangens Verpflichtete hat die zur Auskunftserteilung erforderlichen Daten unverzüglich und vollständig zu übermitteln.

(4) Nach erfolgter Auskunft weist das Bundesamt den Betreiber der betroffenen Kritischen Infrastruktur oder das betroffene Unternehmen im besonderen öffentlichen Interesse auf die bei ihm drohenden Beeinträchtigungen hin. Nach Möglichkeit weist das Bundesamt den Betreiber der betroffenen Kritischen Infrastruktur oder das betroffene Unternehmen im besonderen öffentlichen Interesse auf technische Mittel hin, mittels derer die festgestellten Be-

einträchtigungen durch den Betreiber der betroffenen Kritischen Infrastruktur oder das betroffene Unternehmen im besonderen öffentlichen Interesse selbst beseitigt werden können.

(5) Das Bundesamt kann personenbezogene Daten, die es im Rahmen dieser Vorschrift verarbeitet, entsprechend § 5 Absatz 5 und 6 übermitteln.

(6) In den Fällen des Absatzes 2 ist die betroffene Person über die Auskunft zu benachrichtigen. Im Falle der Weitergabe der Information nach § 5 Absatz 5 oder wenn Tatsachen die Annahme rechtfertigen, dass die Voraussetzungen einer Weitergabe nach § 5 Absatz 5 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.

§ 6 Beschränkungen der Rechte der betroffenen Person

Für die Rechte der betroffenen Person gegen das Bundesamt gelten ergänzend zu den in der Verordnung (EU) 2016/679 enthaltenen Ausnahmen die nachfolgenden Beschränkungen. Soweit dieses Gesetz keine oder geringere Beschränkungen der Rechte der betroffenen Person enthält, gelten für die Beschränkungen im Übrigen die Regelungen des Bundesdatenschutzgesetzes ergänzend.

§ 6a 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 be-

troffenen 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.

§ 6b 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 Ordnung 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.

§ 6c 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.

§ 6d Recht auf Löschung

(1) Im Fall der nicht automatisierten Verarbeitung besteht die Pflicht des Bundesamtes zur Löschung personenbezogener Daten gemäß Artikel 17 Absatz 1 und 2 der Verordnung (EU) 2016/679 ergänzend zu den in Artikel 17 Absatz 3 genannten Ausnahmen nicht, wenn

1. 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 § 5 Absatz 3 zurückgestellt, dürfen die Daten ohne Einwilligung der betroffenen Person nur zu diesem Zweck verwendet werden; sie sind für andere Zwecke in der Verarbeitung einzuschränken. § 5 Absatz 7 bleibt unberührt.

§ 6e 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

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

§ 6f 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.

§ 7 Warnungen

(1) Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 14 und 14a kann das Bundesamt

1. die folgenden Warnungen und Informationen an die Öffentlichkeit oder an die betroffenen Kreise richten:
   a) Warnungen vor Sicherheitslücken in informationstechnischen Produkten und Diensten,
   b) Warnungen vor Schadprogrammen,
   c) Warnungen bei einem Verlust oder einem unerlaubten Zugriff auf Daten und
   d) Informationen über sicherheitsrelevante IT-Eigenschaften von Produkten.
2. Sicherheitsmaßnahmen sowie den 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.

(1a) 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 wird oder
2. wenn berechtigterweise davon ausgegangen werden kann, dass der Hersteller an einer vorherigen Benachrichtigung kein Interesse hat.

Soweit entdeckte Sicherheitslücken oder Schadprogramme nicht allgemein bekannt werden sollen, um eine Weiterverbreitung oder rechtswidrige Ausnutzung zu verhindern oder weil das Bundesamt gegenüber Dritten zur Vertraulichkeit verpflichtet ist, kann es den Kreis der zu warnenden Personen einschränken. Kriterien für die Auswahl des zu warnenden Personenkreises nach Satz 3 sind insbesondere die besondere Gefährdung bestimmter Einrichtungen oder die besondere Zuverlässigkeit des Empfängers.

(2) Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 14 und 14a kann das Bundesamt die Öffentlichkeit unter Nennung der Bezeichnung und des Herstellers des betroffenen Produkts und Dienstes vor Sicherheitslücken in informationstechnischen Produkten und Diensten und vor Schadprogrammen warnen, wenn hinreichende Anhaltspunkte dafür vorliegen, dass Gefahren für die Sicherheit in der Informationstechnik hiervon ausgehen, oder Sicherheitsmaßnahmen sowie den Einsatz bestimmter informationstechnischer Produkte und Dienste empfehlen. Stellen sich die an die Öffentlichkeit gegebenen Informationen im Nachhinein als falsch oder die zugrunde liegenden Umstände als unzutreffend wiedergegeben heraus, ist dies unverzüglich öffentlich bekannt zu machen.

§ 7a Untersuchung der Sicherheit in der Informationstechnik

(1) Das Bundesamt kann zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 14, 14a, 17 oder 18 auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene informationstechnische Produkte und Systeme untersuchen. Es kann sich hierbei der Unterstützung Dritter bedienen, soweit berechtigte Interessen des Herstellers der betroffenen Produkte und Systeme dem nicht entgegenstehen.

(2) Soweit erforderlich, kann das Bundesamt für Untersuchungen nach Absatz 1 von Herstellern informationstechnischer Produkte und Systeme alle notwendigen Auskünfte, insbesondere auch zu technischen Details, verlangen. In dem Auskunftsverlangen gibt das Bundesamt die Rechtsgrundlage, den Zweck des Auskunftsverlangens und die benötigten Auskünfte an und legt eine angemessene Frist für die Übermittlung der Auskünfte fest. Das Auskunftsverlangen enthält ferner einen Hinweis auf die in § 14 vorgesehenen Sanktionen.

(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, 14, 14a, 17 und 18 genutzt werden. Das Bundesamt darf seine Erkenntnisse weitergeben und veröffentlichen, soweit dies zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 14, 14a, 17 und 18 erforderlich ist. Zuvor ist dem Hersteller der betroffenen Produkte und Systeme mit angemessener Frist Gelegenheit zur Stellungnahme zu geben.

(5) Kommt ein Hersteller der Aufforderung des Bundesamtes nach Absatz 2 Satz 1 nicht oder nur unzureichend nach, kann das Bundesamt hierüber die Öffentlichkeit informieren. Es kann hierbei den Namen des Herstellers sowie die Bezeichnung des betroffenen Produkts oder Systems angeben und darlegen, inwieweit der Hersteller seiner Auskunftspflicht nicht nachgekommen ist. Zuvor ist dem Hersteller mit angemessener Frist Gelegenheit zur Stellungnahme zu gewähren. § 7 Absatz 2 Satz 2 gilt entsprechend.

§ 7b Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden

(1) Das Bundesamt kann im Rahmen seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 2, 14 oder 17 zur Detektion von Sicherheitslücken und anderen Sicherheitsrisiken bei Einrichtungen des Bundes oder der in § 2 Absatz 10, 11 und 14 genannten Unternehmen Maßnahmen an den Schnittstellen öffentlich erreichbarer informationstechnischer Systeme zu öffentlichen Telekommunikationsnetzen (Portscans) durchführen, wenn Tatsachen die Annahme rechtfertigen, dass diese ungeschützt im Sinne des Absatzes 2 sein können und dadurch in ihrer Sicherheit oder Funktionsfähigkeit gefährdet sein können. Die Maßnahmen müssen sich auf einen vorher bestimmten Bereich von Internet-Protokolladressen, die regelmäßig den informationstechnischen Systemen

1. des Bundes oder
2. Kritischer Infrastrukturen, digitaler Dienste und der Unternehmen im besonderen öffentlichen Interesse

zugeordnet sind (Weiße Liste), beschränken. Die Weiße Liste ist stetig durch geeignete Überprüfungen anzupassen, um Änderungen bei der Zuordnung von Internetprotokoll-Adressen zu den in den Nummern 1 und 2 bezeichneten Stellen zu berücksichtigen. Erlangt das Bundesamt dabei Informationen, die durch Artikel 10 des Grundgesetzes geschützt sind, darf es diese nur zum Zwecke der Übermittlung nach § 5 Absatz 5 und 6 verarbeiten. Sofern die Voraussetzungen des § 5 Absatz 5 und 6 nicht vorliegen, sind Informationen, die nach Artikel 10 des Grundgesetzes geschützt sind, unverzüglich zu löschen. Maßnahmen nach Satz 1 dürfen nur durch eine Bedienstete oder einen Bediensteten des Bundesamtes mit der Befähigung zum Richteramt angeordnet werden.

(2) Ein informationstechnisches System ist ungeschützt im Sinne des Absatzes 1, wenn in diesem öffentlich bekannte Sicherheitslücken bestehen oder wenn auf Grund sonstiger offensichtlich unzureichender Sicherheitsvorkehrungen unbefugt von Dritten auf das System zugegriffen werden kann.

(3) Wird durch Maßnahmen gemäß Absatz 1 eine Sicherheitslücke oder ein anderes Sicherheitsrisiko eines informationstechnischen Systems erkannt, sind die für das informationstechnische System Verantwortlichen unverzüglich darüber zu informieren. Das Bundesamt soll dabei auf bestehende Abhilfemöglichkeiten hinweisen. Sind dem Bundesamt die Verantwortlichen nicht bekannt oder ist ihre Identifikation nur mit unverhältnismäßigem Aufwand oder über eine Bestandsdatenabfrage nach § 5c möglich, ist hilfsweise der betreibende Dienstleister des jeweiligen Netzes oder Systems unverzüglich zu benachrichtigen, wenn überwiegende Sicherheitsinteressen nicht entgegenstehen. Das Bundesamt unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit jeweils bis zum 30. Juni des Folgejahres über die Anzahl der gemäß Absatz 1 ergriffenen Maßnahmen. Das Bundesamt legt die Weiße Liste nach Absatz 1 Satz 3 der Bun-

desbeauftragten oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vierteljährlich zur Kontrolle vor.

(4) Das Bundesamt darf zur Erfüllung seiner Aufgaben Systeme und Verfahren einsetzen, welche einem Angreifer einen erfolgreichen Angriff vortäuschen, um den Einsatz von Schadprogrammen oder andere Angriffsmethoden zu erheben und auszuwerten. Das Bundesamt darf dabei die zur Auswertung der Funktionsweise der Schadprogramme und Angriffsmethoden erforderlichen Daten verarbeiten.

§ 7c Anordnungen des Bundesamtes gegenüber Diensteanbietern

(1) Zur Abwehr konkreter erheblicher Gefahren für die in Absatz 2 genannten Schutzziele kann das Bundesamt gegenüber einem Anbieter von Telekommunikationsdiensten im Sinne des Telekommunikationsgesetzes (Diensteanbieter) mit mehr als 100 000 Kunden anordnen, dass er

1. 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 Diensteanbieter dazu technisch in der Lage ist und es ihm wirtschaftlich zumutbar ist. Vor der Anordnung der Maßnahmen nach Satz 1 Nummer 1 oder 2 durch das Bundesamt ist Einvernehmen mit der Bundesnetzagentur herzustellen. Vor der Anordnung der Maßnahme nach Satz 1 Nummer 2 durch das Bundesamt ist zusätzlich Einvernehmen mit der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit herzustellen. Die Daten, auf die mit der Maßnahme nach Satz 1 Nummer 2 zugegriffen werden soll, sind in der Anordnung zu benennen. § 5 Absatz 7 Satz 2 bis 8 gilt entsprechend. Widerspruch und Anfechtungsklage gegen die Anordnungen nach Satz 1 haben keine aufschiebende Wirkung.

(2) Schutzziele gemäß Absatz 1 Satz 1 sind die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit

1. der Kommunikationstechnik des Bundes, eines Betreibers Kritischer Infrastrukturen, eines Unternehmens im besonderen öffentlichen Interesse oder eines Anbieters digitaler Dienste,
2. von Informations- oder Kommunikationsdiensten oder
3. von Informationen, sofern deren Verfügbarkeit, Unversehrtheit oder Vertraulichkeit durch unerlaubte Zugriffe auf eine erhebliche Anzahl von telekommunikations- oder informationstechnischen Systemen von Nutzern eingeschränkt wird.

(3) Ordnet das Bundesamt eine Maßnahme nach Absatz 1 Satz 1 Nummer 1 an, so kann es gegenüber dem Diensteanbieter auch anordnen, den Datenverkehr an eine vom Bundesamt benannte Anschlusskennung umzuleiten.

(4) Das Bundesamt darf Daten, die von einem Diensteanbieter nach Absatz 1 Satz 1 Nummer 1 und Absatz 3 umgeleitet wurden, verarbeiten, um Informationen über Schadprogramme oder andere Sicherheitsrisiken in informationstechnischen Systemen zu erlangen. Die übermittelten Daten dürfen durch das Bundesamt so lange gespeichert werden, wie dies für die Erfüllung des in Satz 1 genannten Zwecks erforderlich ist, längstens jedoch für drei Mo-

nate. § 5 Absatz 7 Satz 2 bis 8 gilt entsprechend. Das Bundesamt unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit jeweils bis zum 30. Juni des Folgejahres über die Gesamtzahl der angeordneten Datenumleitungen.

§ 7d Anordnungen des Bundesamtes gegenüber Anbietern von Telemediendiensten

Das Bundesamt kann in begründeten Einzelfällen zur Abwehr konkreter, erheblicher Gefahren für informationstechnische Systeme einer Vielzahl von Nutzern, die von Telemedienangeboten von Anbietern von Telemedien im Sinne des § 2 Absatz 2 Nummer 1 des Telekommunikation-Telemedien-Datenschutz-Gesetzes ausgehen, die durch ungenügende technische und organisatorische Vorkehrungen im Sinne des § 19 Absatz 4 des Telekommunikation-Telemedien-Datenschutz-Gesetzes unzureichend gesichert sind und dadurch keinen hinreichenden Schutz bieten vor

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

gegenüber dem jeweiligen Anbieter von Telemedien im Sinne des § 2 Absatz 2 Nummer 1 des Telekommunikation-Telemedien-Datenschutz-Gesetzes anordnen, dass dieser die jeweils zur Herstellung des ordnungsgemäßen Zustands seiner Telemedienangebote erforderlichen technischen und organisatorischen Maßnahmen ergreift, um den ordnungsgemäßen Zustand seiner Telemedienangebote herzustellen. Die Zuständigkeit der Aufsichtsbehörden der Länder bleibt im Übrigen unberührt.

§ 8 Vorgaben des Bundesamtes

(1) Das Bundesamt legt im Benehmen mit den Ressorts Mindeststandards für die Sicherheit der Informationstechnik des Bundes fest, die von

1. Stellen des Bundes,
2. Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie ihren Vereinigungen ungeachtet ihrer Rechtsform auf Bundesebene, soweit von der jeweils zuständigen obersten Bundesbehörde angeordnet, sowie
3. öffentlichen Unternehmen, die mehrheitlich im Eigentum des Bundes stehen und die IT-Dienstleistungen für die Bundesverwaltung erbringen,

umzusetzen sind. Abweichungen von den Mindeststandards sind nur in sachlich gerechtfertigten Fällen zulässig und sind zu dokumentieren und zu begründen. Das Bundesamt berät die in Satz 1 genannten Stellen auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards. Für die in § 2 Absatz 3 Satz 2 genannten Gerichte und Verfassungsorgane haben die Vorschriften nach Satz 1 empfehlenden Charakter. Für die Verpflichtung nach Satz 1 gilt die Ausnahme nach § 4a Absatz 6 entsprechend.

(1a) Das Bundesministerium des Innern, für Bau und Heimat kann im Benehmen mit der Konferenz der IT-Beauftragten der Ressorts bei bedeutenden Mindeststandards die Überwachung und Kontrolle ihrer Einhaltung durch das Bundesamt anordnen. Das Bundesamt teilt das Ergebnis seiner Kontrolle der jeweiligen überprüften Stelle, deren zuständiger Aufsichtsbehörde sowie der Konferenz der IT-Beauftragten der Ressorts mit. Für andere öffentlich-rechtlich oder privatrechtlich organisierte Stellen dürfen nur dann Schnittstellen zur

Kommunikationstechnik des Bundes eingerichtet werden, soweit die für die Einrichtung verantwortliche Stelle vertraglich sicherstellt, dass die öffentlich- oder privatrechtlich organisierte Stelle sich zur Einhaltung der Mindeststandards verpflichtet. Das Bundesamt kann im Einvernehmen mit dem Dritten die Einhaltung der Mindeststandards überprüfen und kontrollieren.

(2) Das Bundesamt stellt im Rahmen seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 10 technische Richtlinien bereit, die von den Stellen des Bundes als Rahmen für die Entwicklung sachgerechter Anforderungen an Auftragnehmer (Eignung) und IT-Produkte (Spezifikation) für die Durchführung von Vergabeverfahren berücksichtigt werden. Die Vorschriften des Vergaberechts und des Geheimschutzes bleiben unberührt.

(3) Die Bereitstellung von IT-Sicherheitsprodukten durch das Bundesamt nach § 3 Absatz 1 Satz 2 Nummer 11 erfolgt durch Eigenentwicklung oder nach Durchführung von Vergabeverfahren aufgrund einer entsprechenden Bedarfsfeststellung. IT-Sicherheitsprodukte können nur in begründeten Ausnahmefällen durch eine Eigenentwicklung des Bundesamtes zur Verfügung gestellt werden. Die Vorschriften des Vergaberechts bleiben unberührt. Wenn das Bundesamt IT-Sicherheitsprodukte bereitstellt, können die Stellen des Bundes oder von ihnen beauftragte Dritte diese Produkte beim Bundesamt abrufen. Durch Beschluss des Rats der IT-Beauftragten der Bundesregierung kann festgelegt werden, dass die Bundesbehörden verpflichtet sind, diese Produkte beim Bundesamt abzurufen. Eigenbeschaffungen anderer Bundesbehörden sind in diesem Fall nur zulässig, wenn das spezifische Anforderungsprofil den Einsatz abweichender Produkte erfordert. Die Sätze 5 und 6 gelten nicht für die in § 2 Absatz 3 Satz 2 genannten Gerichte und Verfassungsorgane.

(4) Zur Gewährleistung der Sicherheit in der Informationstechnik bei der Planung und Umsetzung von wesentlichen Digitalisierungsvorhaben des Bundes soll die jeweils verantwortliche Stelle das Bundesamt frühzeitig beteiligen und dem Bundesamt Gelegenheit zur Stellungnahme geben.

§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen

(1) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens bis zum ersten Werktag, der darauf folgt, dass diese erstmalig oder erneut als Betreiber einer Kritischen Infrastruktur nach der Rechtsverordnung nach § 10 Absatz 1 gelten, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.

(1a) Die Verpflichtung nach Absatz 1 Satz 1, angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst ab dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. Absatz 1 Satz 2 und 3 gilt entsprechend.

(2) Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach den Absätzen 1 und 1a vorschlagen. Das Bundesamt stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach den Absätzen 1 und 1a zu gewährleisten. Die Feststellung erfolgt

1. im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe,
2. im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes.

(3) Betreiber Kritischer Infrastrukturen haben die Erfüllung der Anforderungen nach den Absätzen 1 und 1a spätestens zwei Jahre nach dem in Absatz 1 genannten Zeitpunkt und anschließend alle zwei Jahre dem Bundesamt nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt die Ergebnisse der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Das Bundesamt kann die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen. Es kann bei Sicherheitsmängeln im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen.

(4) Das Bundesamt kann beim Betreiber Kritischer Infrastrukturen die Einhaltung der Anforderungen nach den Absätzen 1 und 1a überprüfen; es kann sich bei der Durchführung der Überprüfung eines qualifizierten unabhängigen Dritten bedienen. Der Betreiber Kritischer Infrastrukturen hat dem Bundesamt und den in dessen Auftrag handelnden Personen zum Zweck der Überprüfung das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten und auf Verlangen die in Betracht kommenden Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorzulegen, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren. Für die Überprüfung erhebt das Bundesamt Gebühren und Auslagen bei dem jeweiligen Betreiber Kritischer Infrastrukturen nur, sofern das Bundesamt auf Grund von Anhaltspunkten tätig geworden ist, die berechtigte Zweifel an der Einhaltung der Anforderungen nach den Absätzen 1 und 1a begründeten.

(5) Das Bundesamt kann zur Ausgestaltung des Verfahrens der Sicherheitsaudits, Prüfungen und Zertifizierungen nach Absatz 3 Anforderungen an die Art und Weise der Durchführung, an die hierüber auszustellenden Nachweise sowie fachliche und organisatorische Anforderungen an die prüfende Stelle nach Anhörung von Vertretern der betroffenen Betreiber und der betroffenen Wirtschaftsverbände festlegen.

§ 8b Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen

(1) Das Bundesamt ist die zentrale Meldestelle für Betreiber Kritischer Infrastrukturen in Angelegenheiten der Sicherheit in der Informationstechnik.

(2) Das Bundesamt hat zur Wahrnehmung dieser Aufgabe

1. die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik wesentlichen Informationen zu sammeln und auszuwerten, insbesondere Informationen zu Sicherheitslücken, zu Schadprogrammen, zu erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und zu der dabei beobachteten Vorgehensweise,

2. deren potentielle Auswirkungen auf die Verfügbarkeit der Kritischen Infrastrukturen in Zusammenarbeit mit den zuständigen Aufsichtsbehörden und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe zu analysieren,
3. das Lagebild bezüglich der Sicherheit in der Informationstechnik der Kritischen Infrastrukturen oder der Unternehmen im besonderen öffentlichen Interesse kontinuierlich zu aktualisieren und
4. unverzüglich
   a) die Betreiber Kritischer Infrastrukturen und die Unternehmen im besonderen öffentlichen Interesse über sie betreffende Informationen nach den Nummern 1 bis 3,
   b) die zuständigen Aufsichtsbehörden und die sonst zuständigen Behörden des Bundes über die zur Erfüllung ihrer Aufgaben erforderlichen Informationen nach den Nummern 1 bis 3,
   c) die zuständigen Aufsichtsbehörden der Länder oder die zu diesem Zweck dem Bundesamt von den Ländern als zentrale Kontaktstellen benannten Behörden über die zur Erfüllung ihrer Aufgaben erforderlichen Informationen nach den Nummern 1 bis 3 sowie
   d) die zuständigen Behörden eines anderen Mitgliedstaats der Europäischen Union über nach Absatz 4 oder nach vergleichbaren Regelungen gemeldete erhebliche Störungen, die Auswirkungen in diesem Mitgliedstaat haben,

zu unterrichten.

(3) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens bis zum ersten Werktag, der darauf folgt, dass diese erstmalig oder erneut als Betreiber einer Kritischen Infrastruktur nach der Rechtsverordnung nach § 10 Absatz 1 gelten, die von ihnen betriebenen Kritischen Infrastrukturen beim Bundesamt zu registrieren und eine Kontaktstelle zu benennen. Die Registrierung eines Betreibers einer Kritischen Infrastruktur kann das Bundesamt auch selbst vornehmen, wenn der Betreiber seine Pflicht zur Registrierung nicht erfüllt. Nimmt das Bundesamt eine solche Registrierung selbst vor, informiert es die zuständige Aufsichtsbehörde des Bundes darüber. Die Betreiber haben sicherzustellen, dass sie über die benannte oder durch das Bundesamt festgelegte Kontaktstelle jederzeit erreichbar sind. Die Übermittlung von Informationen durch das Bundesamt nach Absatz 2 Nummer 4 erfolgt an diese Kontaktstelle.

(3a) Rechtfertigen Tatsachen die Annahme, dass ein Betreiber seine Pflicht zur Registrierung nach Absatz 3 nicht erfüllt, so hat der Betreiber dem Bundesamt auf Verlangen die für die Bewertung aus Sicht des Bundesamtes erforderlichen Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorzulegen und Auskunft zu erteilen, soweit nicht Geheimschutzinteressen oder überwiegende Sicherheitsinteressen entgegenstehen.

(4) Betreiber Kritischer Infrastrukturen haben die folgenden Störungen unverzüglich über die Kontaktstelle an das Bundesamt zu melden:

1. Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen geführt haben,

2. erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können.

Die Meldung muss Angaben zu der Störung, zu möglichen grenzübergreifenden Auswirkungen sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik, der Art der betroffenen Einrichtung oder Anlage sowie zur erbrachten kritischen Dienstleistung und zu den Auswirkungen der Störung auf diese Dienstleistung enthalten. Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat.

(4a) Während einer erheblichen Störung gemäß Absatz 4 Satz 1 Nummer 2, § 8f Absatz 7 Satz 1 Nummer 2 oder Absatz 8 Satz 1 Nummer 2 kann das Bundesamt im Einvernehmen mit der jeweils zuständigen Aufsichtsbehörde des Bundes von den betroffenen Betreibern Kritischer Infrastrukturen oder den Unternehmen im besonderen öffentlichen Interesse die Herausgabe der zur Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten verlangen. Betreiber Kritischer Infrastrukturen und Unternehmen im besonderen öffentlichen Interesse sind befugt, dem Bundesamt auf Verlangen die zur Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten zu übermitteln, soweit dies zur Bewältigung einer erheblichen Störung gemäß Absatz 4 Satz 1 Nummer 2, § 8f Absatz 7 Satz 1 Nummer 2 oder Absatz 8 Satz 1 Nummer 2 erforderlich ist.

(5) Zusätzlich zu ihrer Kontaktstelle nach Absatz 3 können Betreiber Kritischer Infrastrukturen, die dem gleichen Sektor angehören, eine gemeinsame übergeordnete Ansprechstelle benennen. Wurde eine solche benannt, erfolgt der Informationsaustausch zwischen den Kontaktstellen und dem Bundesamt in der Regel über die gemeinsame Ansprechstelle.

(6) Soweit erforderlich kann das Bundesamt vom Hersteller der betroffenen informationstechnischen Produkte und Systeme die Mitwirkung an der Beseitigung oder Vermeidung einer Störung nach Absatz 4, oder § 8f Absatz 7 oder 8 verlangen. Satz 1 gilt für Störungen bei Betreibern und Genehmigungsinhabern im Sinne von § 8d Absatz 3 entsprechend.

(7) Soweit im Rahmen dieser Vorschrift personenbezogene Daten verarbeitet werden, ist eine über die vorstehenden Absätze hinausgehende Verarbeitung zu anderen Zwecken unzulässig. § 5 Absatz 7 Satz 3 bis 8 ist entsprechend anzuwenden.

§ 8c Besondere Anforderungen an Anbieter digitaler Dienste

(1) Anbieter digitaler Dienste haben geeignete und verhältnismäßige technische und organisatorische Maßnahmen zu treffen, um Risiken für die Sicherheit der Netz- und Informationssysteme, die sie zur Bereitstellung der digitalen Dienste innerhalb der Europäischen Union nutzen, zu bewältigen. Sie haben Maßnahmen zu treffen, um den Auswirkungen von Sicherheitsvorfällen auf innerhalb der Europäischen Union erbrachte digitale Dienste vorzubeugen oder die Auswirkungen so gering wie möglich zu halten.

(2) Maßnahmen zur Bewältigung von Risiken für die Sicherheit der Netz- und Informationssysteme nach Absatz 1 Satz 1 müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist. Dabei ist folgenden Aspekten Rechnung zu tragen:

1. der Sicherheit der Systeme und Anlagen,
2. der Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen,
3. dem Betriebskontinuitätsmanagement,
4. der Überwachung, Überprüfung und Erprobung,
5. der Einhaltung internationaler Normen.

Die notwendigen Maßnahmen werden durch Durchführungsrechtsakte der Kommission nach Artikel 16 Absatz 8 der Richtlinie (EU) 2016/1148 näher bestimmt.

(3) Anbieter digitaler Dienste haben jeden Sicherheitsvorfall, der erhebliche Auswirkungen auf die Bereitstellung eines von ihnen innerhalb der Europäischen Union erbrachten digitalen Dienstes hat, unverzüglich dem Bundesamt zu melden. Die Voraussetzungen, nach denen Auswirkungen eines Sicherheitsvorfalls erheblich sind, werden durch Durchführungsakte der Kommission nach Artikel 16 Absatz 8 der Richtlinie (EU) 2016/1148 unter Berücksichtigung insbesondere der folgenden Parameter näher bestimmt:

1. die Zahl der von dem Sicherheitsvorfall betroffenen Nutzer, insbesondere der Nutzer, die den Dienst für die Bereitstellung ihrer eigenen Dienste benötigen,
2. die Dauer des Sicherheitsvorfalls,
3. das von dem Sicherheitsvorfall betroffene geographische Gebiet,
4. das Ausmaß der Unterbrechung der Bereitstellung des Dienstes,
5. das Ausmaß der Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten.

Die Pflicht zur Meldung eines Sicherheitsvorfalls entfällt, wenn der Anbieter keinen ausreichenden Zugang zu den Informationen hat, die erforderlich sind, um die Auswirkung eines Sicherheitsvorfalls gemessen an den Parametern nach Satz 2 zu bewerten. Für den Inhalt der Meldungen gilt § 8b Absatz 4 entsprechend, soweit nicht Durchführungsakte der Kommission nach Artikel 16 Absatz 9 der Richtlinie (EU) 2016/1148 etwas anderes bestimmen. Über nach Satz 1 gemeldete Sicherheitsvorfälle, die Auswirkungen in einem anderen Mitgliedstaat der Europäischen Union haben, hat das Bundesamt die zuständige Behörde dieses Mitgliedstaats zu unterrichten.

(4) Liegen Anhaltspunkte dafür vor, dass ein Anbieter digitaler Dienste die Anforderungen des Absatzes 1 in Verbindung mit den Durchführungsrechtsakten der Kommission nach Artikel 16 Absatz 8 der Richtlinie (EU) 2016/1148 und des Absatzes 2 in Verbindung mit den Durchführungsrechtsakten der Kommission nach Artikel 16 Absatz 9 der Richtlinie (EU) 2016/1148 nicht erfüllt, kann das Bundesamt von dem Anbieter digitaler Dienste folgende Maßnahmen verlangen:

1. die Übermittlung der zur Beurteilung der Sicherheit seiner Netz- und Informationssysteme erforderlichen Informationen, einschließlich Nachweisen über ergriffene Sicherheitsmaßnahmen,
2. die Beseitigung von Mängeln bei der Erfüllung der in den Absätzen 1 und 2 bestimmten Anforderungen.

Die Anhaltspunkte können sich auch aus Feststellungen ergeben, die dem Bundesamt von den zuständigen Behörden eines anderen Mitgliedstaats der Europäischen Union vorgelegt werden.

(5) Hat ein Anbieter digitaler Dienste seine Hauptniederlassung, einen Vertreter oder Netz- und Informationssysteme in einem anderen Mitgliedstaat der Europäischen Union, so arbeitet das Bundesamt bei der Erfüllung der Aufgaben nach Absatz 4 mit der zuständigen Behörde dieses Mitgliedstaats zusammen. Diese Zusammenarbeit kann das Ersuchen umfassen, die Maßnahmen in Absatz 4 Satz 1 Nummer 1 und 2 zu ergreifen.

§ 8d Anwendungsbereich

(1) Die §§ 8a und 8b sind nicht anzuwenden auf Kleinstunternehmen im Sinne der Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36). Artikel 3 Absatz 4 des Anhangs der Empfehlung ist nicht anzuwenden.

(1a) § 8f ist nicht anzuwenden auf Kleinstunternehmen und kleine Unternehmen im Sinne der Empfehlung 2003/361/EG. Artikel 3 Absatz 4 des Anhangs zu der Empfehlung ist nicht anzuwenden.

(2) § 8a ist nicht anzuwenden auf

1. Betreiber Kritischer Infrastrukturen, soweit sie ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen,
2. Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 3 des Gesetzes vom 17. Juli 2015 (BGBl. I S. 1324) geändert worden ist, in der jeweils geltenden Fassung, soweit sie den Regelungen des § 11 des Energiewirtschaftsgesetzes unterliegen,
3. die Gesellschaft für Telematik nach § 306 Absatz 1 Satz 3 des Fünften Buches Sozialgesetzbuch, Betreiber von Diensten der Telematikinfrastruktur im Hinblick auf die nach § 311 Absatz 6 und § 325 des Fünften Buches Sozialgesetzbuch zugelassenen Dienste und Betreiber von Diensten, soweit sie die Telematikinfrastruktur für nach § 327 Absatz 2 bis 5 des Fünften Buches Sozialgesetzbuch bestätigte Anwendungen nutzen,
4. Genehmigungsinhaber nach § 7 Absatz 1 des Atomgesetzes in der Fassung der Bekanntmachung vom 15. Juli 1985 (BGBl. I S. 1565), das zuletzt durch Artikel 2 des Gesetzes vom 17. Juli 2015 (BGBl. I S. 1324) geändert worden ist, in der jeweils geltenden Fassung für den Geltungsbereich der Genehmigung sowie
5. sonstige Betreiber Kritischer Infrastrukturen, soweit sie auf Grund von Rechtsvorschriften Anforderungen erfüllen müssen, die mit den Anforderungen nach § 8a vergleichbar oder weitergehend sind.

(3) § 8b Absatz 4 und 4a ist nicht anzuwenden auf

1. Betreiber Kritischer Infrastrukturen, soweit sie ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen,

2. Betreiber von Energieversorgungsnetzen oder Energieanlagen, soweit sie den Regelungen des § 11 des Energiewirtschaftsgesetzes unterliegen,
3. die Gesellschaft für Telematik nach § 306 Absatz 1 Satz 3 des Fünften Buches Sozialgesetzbuch, Betreiber von Diensten der Telematikinfrastruktur im Hinblick auf die nach § 311 Absatz 6 und § 325 des Fünften Buches Sozialgesetzbuch zugelassenen Dienste und Betreiber von Diensten, soweit sie die Telematikinfrastruktur für nach § 327 Absatz 2 bis 5 des Fünften Buches Sozialgesetzbuch bestätigte Anwendungen nutzen,
4. Genehmigungsinhaber nach § 7 Absatz 1 des Atomgesetzes für den Geltungsbereich der Genehmigung sowie
5. sonstige Betreiber Kritischer Infrastrukturen, die auf Grund von Rechtsvorschriften Anforderungen erfüllen müssen, die mit den Anforderungen nach § 8b Absatz 4 vergleichbar oder weitergehend sind.

(4) § 8c Absatz 1 bis 3 gilt nicht für Kleinstunternehmen und kleine Unternehmen im Sinne der Empfehlung 2003/361/EG. § 8c Absatz 3 gilt nicht für Anbieter,

1. die ihren Hauptsitz in einem anderen Mitgliedstaat der Europäischen Union haben oder
2. die, soweit sie nicht in einem Mitgliedstaat der Europäischen Union niedergelassen sind, einen Vertreter in einem anderen Mitgliedstaat der Europäischen Union benannt haben, in dem die digitalen Dienste ebenfalls angeboten werden.

Für Anbieter nach Satz 2 gilt § 8c Absatz 4 nur, soweit sie in der Bundesrepublik Deutschland Netz- und Informationssysteme betreiben, die sie zur Bereitstellung der digitalen Dienste innerhalb der Europäischen Union nutzen.

§ 8e Auskunftsverlangen

(1) Das Bundesamt kann Dritten auf Antrag Auskunft zu den im Rahmen von § 8a Absatz 2 und 3, § 8c Absatz 4 und § 8f erhaltenen Informationen sowie zu den Meldungen nach § 8b Absatz 4, 4a und 4b sowie § 8c Absatz 4 nur erteilen, wenn

1. schutzwürdige Interessen des betroffenen Betreibers einer Kritischen Infrastruktur, des Unternehmens im besonderen öffentlichen Interesse oder des Anbieters digitaler Dienste dem nicht entgegenstehen und
2. durch die Auskunft keine Beeinträchtigung von Sicherheitsinteressen eintreten kann.

Zugang zu personenbezogenen Daten wird nicht gewährt.

(2) Zugang zu den Akten des Bundesamtes in Angelegenheiten nach den §§ 8a bis 8c und 8f wird bei Vorliegen der Voraussetzungen des § 29 des Verwaltungsverfahrensgesetzes nur gewährt, wenn

1. schutzwürdige Interessen des betroffenen Betreibers einer Kritischen Infrastruktur, des Unternehmens im besonderen öffentlichen Interesse oder des Anbieters digitaler Dienste dem nicht entgegenstehen und

2. durch den Zugang zu den Akten keine Beeinträchtigung von Sicherheitsinteressen eintreten kann.

(3) Für Betreiber nach § 8d Absatz 2 und 3 gelten die Absätze 1 und 2 entsprechend.

(4) Informationsansprüche nach dem Umweltinformationsgesetz bleiben von dieser Vorschrift unberührt.

§ 8f Sicherheit in der Informationstechnik bei Unternehmen im besonderen öffentlichen Interesse

(1) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 1 und 2 sind verpflichtet, spätestens bis zum ersten Werktag, der darauf folgt, dass diese erstmalig oder erneut als Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 1 oder 2 gelten, und danach mindestens alle zwei Jahre eine Selbsterklärung zur IT-Sicherheit beim Bundesamt vorzulegen, aus der hervorgeht,

1. welche Zertifizierungen im Bereich der IT-Sicherheit in den letzten zwei Jahren durchgeführt, welche Prüfgrundlage und welcher Geltungsbereich hierfür festgelegt wurden,
2. welche sonstigen Sicherheitsaudits oder Prüfungen im Bereich der IT-Sicherheit in den letzten zwei Jahren durchgeführt, welche Prüfgrundlage und welcher Geltungsbereich hierfür festgelegt wurden oder
3. wie sichergestellt wird, dass die für das Unternehmen besonders schützenswerten informationstechnischen Systeme, Komponenten und Prozesse angemessen geschützt werden, und ob dabei der Stand der Technik eingehalten wird.

(2) Das Bundesamt kann für die Selbsterklärung nach Absatz 1 zu verwendende Formulare einführen.

(3) Das Bundesamt kann auf Grundlage der Selbsterklärung nach Absatz 1 Hinweise zu angemessenen organisatorischen und technischen Vorkehrungen nach Absatz 1 Nummer 3 zur Einhaltung des Stands der Technik geben.

(4) Für Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 1 gilt die Pflicht nach Absatz 1 nicht vor dem 1. Mai 2023. Für Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 2 gilt diese Pflicht frühestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 5.

(5) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 1 und 2 sind verpflichtet, sich gleichzeitig mit der Vorlage der ersten Selbsterklärung zur IT-Sicherheit nach Absatz 1 beim Bundesamt zu registrieren und eine zu den üblichen Geschäftszeiten erreichbare Stelle zu benennen. Die Übermittlung von Informationen durch das Bundesamt nach § 8b Absatz 2 Nummer 4 erfolgt an diese Stelle.

(6) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 3 können eine freiwillige Registrierung beim Bundesamt und die Benennung einer zu den üblichen Geschäftszeiten erreichbaren Stelle vornehmen. Die Übermittlung von Informationen durch das Bundesamt nach § 8b Absatz 2 Nummer 4 erfolgt an diese Stelle.

(7) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 1 und 2 haben ab dem Zeitpunkt, zu dem eine Pflicht zur Vorlage der Selbsterklärung zur IT-

Sicherheit nach Absatz 1 besteht, die folgenden Störungen unverzüglich über die nach Absatz 5 benannte Stelle an das Bundesamt zu melden:

1. Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Erbringung der Wertschöpfung geführt haben,
2. erhebliche Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Erbringung der Wertschöpfung führen können.

Die Meldung muss Angaben zu der Störung, zu den technischen Rahmenbedingungen, insbesondere zu der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik und der Art der betroffenen Einrichtung oder Anlage enthalten.

(8) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 3 haben spätestens ab dem 1. November 2021 die folgenden Störungen unverzüglich an das Bundesamt zu melden:

1. Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Störfall nach der Störfall-Verordnung in der jeweils geltenden Fassung geführt haben,
2. erhebliche Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Störfall nach der Störfall-Verordnung in der jeweils geltenden Fassung führen können.

Die Meldung muss Angaben zu der Störung, zu den technischen Rahmenbedingungen, insbesondere zu der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik und der Art der betroffenen Einrichtung oder Anlage enthalten.

(9) Rechtfertigen Tatsachen die Annahme, dass ein Unternehmen ein Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 2 ist, aber seine Pflichten nach Absatz 5 nicht erfüllt, so kann das Bundesamt verlangen:

1. eine rechnerische Darlegung, wie hoch die vom Unternehmen erbrachte inländische Wertschöpfung nach der in der Rechtsverordnung nach § 10 Absatz 5 festgelegten Berechnungsmethode ist, oder
2. eine Bestätigung einer anerkannten Wirtschaftsprüfungsgesellschaft, dass das Unternehmen nach der in der Rechtsverordnung nach § 10 Absatz 5 festgelegten Berechnungsmethode kein Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 2 ist.

§ 9 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 wer-

den. Die Anträge werden in der zeitlichen Reihenfolge ihres Eingangs bearbeitet; hiervon kann abgewichen werden, wenn das Bundesamt wegen der Zahl und des Umfangs anhängiger Prüfungsverfahren eine Prüfung in angemessener Zeit nicht durchführen kann und an der Erteilung eines Zertifikats ein öffentliches Interesse besteht. Der Antragsteller hat dem Bundesamt die Unterlagen vorzulegen und die Auskünfte zu erteilen, deren Kenntnis für die Prüfung und Bewertung des Systems oder der Komponente oder der Eignung der Person sowie für die Erteilung des Zertifikats erforderlich ist.

(3) Die Prüfung und Bewertung kann durch vom Bundesamt anerkannte sachverständige Stellen erfolgen.

(4) Das Sicherheitszertifikat wird erteilt, wenn

1. informationstechnische Systeme, Komponenten, Produkte oder Schutzprofile den vom Bundesamt festgelegten Kriterien entsprechen und
2. das Bundesministerium des Innern, für Bau und Heimat die Erteilung des Zertifikats nicht nach Absatz 4a untersagt hat.

Vor Erteilung des Sicherheitszertifikats legt das Bundesamt den Vorgang dem Bundesministerium des Innern, für Bau und Heimat zur Prüfung nach Absatz 4a vor.

(4a) Das Bundesministerium des Innern, für Bau und Heimat kann eine Zertifikatserteilung nach Absatz 4 im Einzelfall untersagen, wenn überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung entgegenstehen.

(5) Für die Zertifizierung von Personen und IT-Sicherheitsdienstleistern gilt Absatz 4 entsprechend.

(6) Eine Anerkennung nach Absatz 3 wird erteilt, wenn

1. die sachliche und personelle Ausstattung sowie die fachliche Qualifikation und Zuverlässigkeit der Konformitätsbewertungsstelle den vom Bundesamt festgelegten Kriterien entspricht und
2. das Bundesministerium des Innern, für Bau und Heimat festgestellt hat, dass überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung nicht entgegenstehen.

Das Bundesamt stellt durch die notwendigen Maßnahmen sicher, dass das Fortbestehen der Voraussetzungen nach Satz 1 regelmäßig überprüft wird.

(7) Sicherheitszertifikate anderer anerkannter Zertifizierungsstellen aus dem Bereich der Europäischen Union werden vom Bundesamt anerkannt, soweit sie eine den Sicherheitszertifikaten des Bundesamtes gleichwertige Sicherheit ausweisen und die Gleichwertigkeit vom Bundesamt festgestellt worden ist.

§ 9a Nationale Behörde für die Cybersicherheitszertifizierung

(1) Das Bundesamt ist die nationale Behörde für die Cybersicherheitszertifizierung im Sinne des Artikels 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 § 9 dieses Gesetzes tätig werden, eine Befugnis erteilen, als solche tätig zu werden, wenn die Voraussetzungen des maßgeblichen eu-

ropäischen Schemas für die Cybersicherheitszertifizierung nach Artikel 54 der Verordnung (EU) 2019/881 oder des § 9 dieses Gesetzes erfüllt sind. Ohne eine Befugniserteilung durch das Bundesamt dürfen Konformitätsbewertungsstellen im Anwendungsbereich der Verordnung (EU) 2019/881 nicht tätig werden.

(3) Soweit dies zur Erfüllung seiner Aufgaben nach Artikel 58 Absatz 7 der Verordnung (EU) 2019/881 und nach § 9 dieses Gesetzes erforderlich ist, kann das Bundesamt von Konformitätsbewertungsstellen, denen eine Befugnis nach Absatz 2 erteilt wurde, von Inhabern europäischer Cybersicherheitszertifikate und 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 zu prüfen, soweit dies zur Erfüllung seiner Aufgaben nach Artikel 58 Absatz 7 der Verordnung (EU) 2019/881 sowie nach § 9 dieses Gesetzes erforderlich ist. § 3 Absatz 1 Satz 1 bis 3 des Akkreditierungsstellengesetzes gilt entsprechend.

(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 dieser das Bundesamt bei der Wahrnehmung seiner Befugnisse nach Absatz 4 oder im Falle eines Inhabers eines europäischen Cybersicherheitszertifikats auch nach Absatz 5 behindert hat.

(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 § 9 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 diese das Bundesamt bei der Wahrnehmung seiner Befugnisse nach den Absätzen 4 und 5 behindert hat.

§ 9b Untersagung des Einsatzes kritischer Komponenten

(1) Der Betreiber einer Kritischen Infrastruktur hat den geplanten erstmaligen Einsatz einer kritischen Komponente gemäß § 2 Absatz 13 dem Bundesministerium des Innern, für Bau und Heimat vor ihrem Einsatz anzuzeigen. In der Anzeige sind die kritische Komponente und die geplante Art ihres Einsatzes anzugeben. Satz 1 gilt für einen Betreiber einer Kritischen Infrastruktur nicht, wenn dieser den Einsatz einer anderen kritischen Komponente desselben Typs für dieselbe Art des Einsatzes bereits nach Satz 1 angezeigt hat und ihm dieser nicht untersagt wurde.

(2) Das Bundesministerium des Innern, für Bau und Heimat kann den geplanten erstmaligen Einsatz einer kritischen Komponente gegenüber dem Betreiber der Kritischen Infrastruktur im Benehmen mit den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt bis zum Ablauf von zwei Monaten nach Eingang der Anzeige nach Absatz 1 untersagen oder Anordnungen erlassen, wenn der Einsatz die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt. Bei der Prüfung einer voraussichtlichen Beeinträchtigung der öffentlichen Ordnung oder Sicherheit kann insbesondere berücksichtigt werden, ob

1. der Hersteller unmittelbar oder mittelbar von der Regierung, einschließlich sonstiger staatlicher Stellen oder Streitkräfte, eines Drittstaates kontrolliert wird,
2. der Hersteller bereits an Aktivitäten beteiligt war oder ist, die nachteilige Auswirkungen auf die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland oder eines anderen Mitgliedstaates der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages oder auf deren Einrichtungen hatten, oder
3. der Einsatz der kritischen Komponente im Einklang mit den sicherheitspolitischen Zielen der Bundesrepublik Deutschland, der Europäischen Union oder des Nordatlantikvertrages steht.

Vor Ablauf der Frist von zwei Monaten nach Anzeige nach Absatz 1 ist der Einsatz nicht gestattet. Das Bundesministerium des Innern, für Bau und Heimat kann die Frist gegenüber dem Betreiber um weitere zwei Monate verlängern, wenn die Prüfung besondere Schwierigkeiten tatsächlicher oder rechtlicher Art aufweist.

(3) Kritische Komponenten gemäß § 2 Absatz 13 dürfen nur eingesetzt werden, wenn der Hersteller eine Erklärung über seine Vertrauenswürdigkeit (Garantieerklärung) gegenüber dem Betreiber der Kritischen Infrastruktur abgeben hat. Die Garantieerklärung ist der Anzeige nach Absatz 1 beizufügen. Aus der Garantieerklärung muss hervorgehen, wie der Hersteller sicherstellt, dass die kritische Komponente nicht über technische Eigenschaften verfügt, die spezifisch geeignet sind, missbräuchlich, insbesondere zum Zwecke von Sabotage, Spionage oder Terrorismus auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder

Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können. Das Bundesministerium des Innern, für Bau und Heimat legt die Einzelheiten der Mindestanforderungen an die Garantieerklärung im Einvernehmen mit den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt durch Allgemeinverfügung fest, die im Bundesanzeiger bekannt zu machen ist. Die Einzelheiten der Mindestanforderungen an die Garantieerklärung müssen aus den Schutzzielen der Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur folgen und die Vermeidung von Gefahren für die öffentliche Sicherheit und Ordnung, insbesondere im Sinne von Absatz 2 Satz 2, adressieren, die aus der Sphäre des Herstellers der kritischen Komponente, insbesondere dessen Organisationsstruktur, stammen. Die Sätze 1 und 2 gelten erst ab der Bekanntmachung der Allgemeinverfügung nach Satz 5 und nicht für bereits vor diesem Zeitpunkt eingesetzte kritische Komponenten. Soweit Änderungen der Allgemeinverfügung erfolgen, sind diese für bereits nach diesem Absatz abgegebene Garantieerklärungen unbeachtlich.

(4) Das Bundesministerium des Innern, für Bau und Heimat kann den weiteren Einsatz einer kritischen Komponente gegenüber dem Betreiber der Kritischen Infrastruktur im Einvernehmen mit den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt untersagen oder Anordnungen erlassen, wenn der weitere Einsatz die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt, insbesondere, wenn der Hersteller der kritischen Komponente nicht vertrauenswürdig ist. Absatz 2 Satz 2 gilt entsprechend.

(5) Ein Hersteller einer kritischen Komponente kann insbesondere dann nicht vertrauenswürdig sein, wenn hinreichende Anhaltspunkte dafür bestehen, dass

1. er gegen die in der Garantieerklärung eingegangen Verpflichtungen verstoßen hat,
2. in der Garantieerklärung angegebene Tatsachenbehauptungen unwahr sind,
3. er Sicherheitsüberprüfungen und Penetrationsanalysen an seinem Produkt und in der Produktionsumgebung nicht im erforderlichen Umfang in angemessener Weise unterstützt,
4. Schwachstellen oder Manipulationen nicht unverzüglich, nachdem er davon Kenntnis erlangt, beseitigt und dem Betreiber der Kritischen Infrastruktur meldet,
5. die kritische Komponente auf Grund von Mängeln ein erhöhtes Gefährdungspotenzial aufweist oder aufgewiesen hat, missbräuchlich auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können oder
6. die kritische Komponente über technische Eigenschaften verfügt oder verfügt hat, die spezifisch geeignet sind oder waren, missbräuchlich auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können.

(6) Wurde nach Absatz 4 der weitere Einsatz einer kritischen Komponente untersagt, kann das Bundesministerium des Innern, für Bau und Heimat im Einvernehmen mit den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt

1. den geplanten Einsatz weiterer kritischer Komponenten desselben Typs und desselben Herstellers untersagen und

2. den weiteren Einsatz kritischer Komponenten desselben Typs und desselben Herstellers unter Einräumung einer angemessenen Frist untersagen.

(7) Bei schwerwiegenden Fällen nicht vorliegender Vertrauenswürdigkeit nach Absatz 5 kann das Bundesministerium des Innern, für Bau und Heimat den Einsatz aller kritischen Komponenten des Herstellers im Einvernehmen mit den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt untersagen.

§ 9c 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 § 10 Absatz 3 geregelt wird, festgestellt hat, dass die Norm oder der Standard oder die branchenabgestimmte IT-Sicherheitsvorgabe geeignet ist, ausreichende IT-Sicherheitsanforderungen für die Produktkategorie abzubilden. Ein Anspruch auf diese Feststellung besteht nicht. Liegt keine Feststellung nach Satz 1 vor, ergeben sich die IT-Sicherheitsvorgaben aus einer vom Bundesamt veröffentlichten Technischen Richtlinie, die die jeweilige Produktkategorie umfasst, sofern das Bundesamt eine solche Richtlinie bereits veröffentlicht hat. Wird ein Produkt von mehr als einer oder einem bestehenden, als geeignet festgestellten Norm, 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 § 10 Absatz 3 bestimmt wird. Den genauen Ablauf des Antragsverfahrens und die beizufügenden Unterlagen regelt die Rechtsverordnung nach § 10 Absatz 3.

(6) Hat das Bundesamt die Freigabe erteilt, ist das Etikett des IT-Sicherheitskennzeichens auf dem jeweiligen Produkt oder auf dessen Umverpackung anzubringen, sofern dies nach der Beschaffenheit des Produktes möglich ist. Das IT-Sicherheitskennzeichen kann auch elektronisch veröffentlicht werden. Wenn nach der Beschaffenheit des Produktes das Anbringen nicht möglich ist, muss die Veröffentlichung des IT-Sicherheitskennzeichens elektronisch erfolgen. Das Etikett des IT-Sicherheitskennzeichens verweist auf eine Internetseite des Bundesamtes, auf der die Herstellererklärung und die Sicherheitsinformationen abrufbar sind. Das genaue Verfahren und die Gestaltung des Verweises sind in der Rechtsverordnung nach § 10 Absatz 3 festzulegen.

(7) Nach Ablauf der festgelegten Dauer nach Absatz 3 Satz 5 oder 6 oder nach Rücknahmeerklärung des Herstellers oder Diensteanbieters gegenüber dem Bundesamt erlischt die Freigabe. Das Bundesamt nimmt einen Hinweis auf das Erlöschen der Freigabe in die Sicherheitsinformation auf.

(8) Das Bundesamt kann prüfen, ob die Anforderungen an die Freigabe des IT-Sicherheitskennzeichens für ein Produkt eingehalten werden. Werden bei der Prüfung Abweichungen von der abgegebenen Herstellererklärung oder Sicherheitslücken festgestellt, kann das Bundesamt die geeigneten Maßnahmen zum Schutz des Vertrauens der Verbraucher in das IT-Sicherheitskennzeichen treffen, insbesondere

1. Informationen über die Abweichungen oder Sicherheitslücken 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 Gelegenheit ein, die festgestellten Abweichungen oder Sicherheitslücken innerhalb eines angemessenen Zeitraumes zu beseitigen, es sei denn, gewichtige Gründe der Sicherheit der Produkte erfordern eine sofortige Maßnahme. Die Befugnis des Bundesamtes zur Warnung nach § 7 bleibt davon unberührt.

§ 10 Ermächtigung zum Erlass von Rechtsverordnungen

(1) Das Bundesministerium des Innern, für Bau und Heimat bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr und digitale Infrastruktur, dem Bundesministerium der Verteidigung und dem Bun-

desministerium für Umwelt, Naturschutz und nukleare Sicherheit unter Festlegung der in den jeweiligen Sektoren im Hinblick auf § 2 Absatz 10 Satz 1 Nummer 2 wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrads, welche Einrichtungen, Anlagen oder Teile davon als Kritische Infrastrukturen im Sinne dieses Gesetzes gelten. Der nach Satz 1 als bedeutend anzusehende Versorgungsgrad ist anhand von branchenspezifischen Schwellenwerten für jede wegen ihrer Bedeutung als kritisch anzusehende Dienstleistung im jeweiligen Sektor zu bestimmen. Zugang zu Akten, die die Erstellung oder Änderung dieser Verordnung betreffen, wird nicht gewährt.

(2) Das Bundesministerium des Innern, für Bau und Heimat bestimmt nach Anhörung der betroffenen Wirtschaftsverbände und im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, das Nähere über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen nach § 9 und deren Inhalt.

(3) Das Bundesministerium des Innern, für Bau und Heimat bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie und dem Bundesministerium der Justiz und für Verbraucherschutz die Einzelheiten der Gestaltung, des Inhalts und der Verwendung des IT-Sicherheitskennzeichens nach § 9c, um eine einheitliche Gestaltung des Kennzeichens und eine eindeutige Erkennbarkeit der gekennzeichneten informationstechnischen Produkte zu gewährleisten, sowie die Einzelheiten des Verfahrens zur Feststellung der Eignung branchenabgestimmter IT-Sicherheitsvorgaben und des Antragsverfahrens auf Freigabe einschließlich der diesbezüglichen Fristen und der beizufügenden Unterlagen sowie das Verfahren und die Gestaltung des Verweises auf Sicherheitsinformationen.

(4) Soweit die Durchführungsrechtsakte der Kommission nach Artikel 16 Absatz 8 und 9 der Richtlinie (EU) 2016/1148 keine abschließenden Bestimmungen über die von Anbietern digitaler Dienste nach § 8c Absatz 2 zu treffenden Maßnahmen oder über die Parameter zur Beurteilung der Erheblichkeit der Auswirkungen von Sicherheitsvorfällen nach § 8c Absatz 3 Satz 2 oder über Form und Verfahren der Meldungen nach § 8c Absatz 3 Satz 4 enthalten, werden diese Bestimmungen vom Bundesministerium des Innern, für Bau und Heimat im Einvernehmen mit den jeweils betroffenen Ressorts durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, getroffen.

(5) Das Bundesministerium des Innern, für Bau und Heimat bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung von Vertretern der Wissenschaft, der betroffenen Unternehmen und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr und digitale Infrastruktur, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit, welche wirtschaftlichen Kennzahlen bei der Berechnung der inländischen Wertschöpfung heranzuziehen sind, wie die Berechnung mit Hilfe der Methodik der direkten Wertschöpfungsstaffel zu erfolgen hat und welche Schwellenwerte maßgeblich dafür sind, dass ein Unternehmen zu den größten Unternehmen in Deutschland im Sinne des § 2 Absatz 14 Satz 1 Nummer 2 gehört. Unter den Voraussetzungen nach Satz 1 kann das Bundesministerium des Innern, für Bau und Heimat durch Rechtsverordnung bestimmen, welche Alleinstellungsmerkmale maßgeblich dafür sind, dass Zulieferer für Unternehmen, die nach

ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören, von wesentlicher Bedeutung im Sinne des § 2 Absatz 14 Satz 1 Nummer 2 sind.

§ 11 Einschränkung von Grundrechten

Das Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) wird durch die §§ 4a, 5 bis 5c, 7b und 7c eingeschränkt.

§ 12 Rat der IT-Beauftragten der Bundesregierung

Wird der Rat der IT-Beauftragten der Bundesregierung aufgelöst, tritt an dessen Stelle die von der Bundesregierung bestimmte Nachfolgeorganisation. Die Zustimmung des Rats der IT-Beauftragten kann durch Einvernehmen aller Bundesministerien ersetzt werden. Wird der Rat der IT-Beauftragten ersatzlos aufgelöst, tritt an Stelle seiner Zustimmung das Einvernehmen aller Bundesministerien.

§ 13 Berichtspflichten

(1) Das Bundesamt unterrichtet das Bundesministerium des Innern, für Bau und Heimat über seine Tätigkeit.

(2) Die Unterrichtung nach Absatz 1 dient auch der Aufklärung der Öffentlichkeit durch das Bundesministerium des Innern, für Bau und Heimat über Gefahren für die Sicherheit in der Informationstechnik, die mindestens einmal jährlich in einem zusammenfassenden Bericht erfolgt. § 7 Absatz 1a ist entsprechend anzuwenden.

(3) Das Bundesministerium des Innern, für Bau und Heimat unterrichtet kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres den Ausschuss für Inneres und Heimat des Deutschen Bundestages über die Anwendung dieses Gesetzes. Es geht dabei auch auf die Fortentwicklung des maßgeblichen Unionsrechts ein.

(4) Das Bundesamt übermittelt bis zum 9. November 2018 und danach alle zwei Jahre die folgenden Informationen an die Kommission:

1. die nationalen Maßnahmen zur Ermittlung der Betreiber Kritischer Infrastrukturen;
2. eine Aufstellung der im in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren, die nach § 2 Absatz 10 Satz 1 Nummer 2 wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrad;
3. eine zahlenmäßige Aufstellung der Betreiber der in Nummer 2 genannten Sektoren, die in den in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren ermittelt werden, einschließlich eines Hinweises auf ihre Bedeutung für den jeweiligen Sektor.

Die Übermittlung darf keine Informationen enthalten, die zu einer Identifizierung einzelner Betreiber führen können. Das Bundesamt übermittelt die nach Satz 1 übermittelten Informationen unverzüglich dem Bundesministerium des Innern, für Bau und Heimat, dem Bundeskanzleramt, dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Ver-

kehr und digitale Infrastruktur, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit.

(5) Sobald bekannt wird, dass eine Einrichtung oder Anlage nach § 2 Absatz 10 oder Teile einer Einrichtung oder Anlage eine wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistung in einem der in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren in einem anderen Mitgliedstaat der Europäischen Union bereitstellt, nimmt das Bundesamt zum Zweck der gemeinsamen Ermittlung der Betreiber, die kritische Dienstleistungen in den in Anhang II der Richtlinie (EU) 2016/1148 genannten Teilsektoren erbringen, mit der zuständigen Behörde dieses Mitgliedstaats Konsultationen auf.

(6) Das Bundesamt übermittelt bis zum 9. August 2018 und danach jährlich an die Kooperationsgruppe nach Artikel 11 der Richtlinie (EU) 2016/1148 einen zusammenfassenden Bericht zu den Meldungen, die die in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren oder digitale Dienste betreffen. Der Bericht enthält auch die Zahl der Meldungen und die Art der gemeldeten Sicherheitsvorfälle sowie die ergriffenen Maßnahmen. Der Bericht darf keine Informationen enthalten, die zu einer Identifizierung einzelner Meldungen oder einzelner Betreiber oder Anbieter führen können.

§ 14 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer entgegen § 8a Absatz 3 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 10 Absatz 1 Satz 1 einen Nachweis nicht richtig oder nicht vollständig erbringt.

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. einer vollziehbaren Anordnung nach
   a) § 5b Absatz 6, § 7c Absatz 1 Satz 1, auch in Verbindung mit § 7c Absatz 3, § 7d, oder § 8a Absatz 3 Satz 5,
   b) § 7a Absatz 2 Satz 1 oder
   c) § 8b Absatz 6 Satz 1, auch in Verbindung mit Satz 2, oder § 8c Absatz 4 Satz 1

   zuwiderhandelt,
2. entgegen § 8a Absatz 1 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 10 Absatz 1 Satz 1 eine dort genannte Vorkehrung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig trifft,
3. entgegen § 8a Absatz 3 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 10 Absatz 1 Satz 1 einen Nachweis nicht oder nicht rechtzeitig erbringt,
4. entgegen § 8a Absatz 4 Satz 2 oder § 8b Absatz 3a das Betreten eines dort genannten Raums nicht gestattet, eine dort genannte Unterlage nicht oder nicht rechtzeitig vorlegt, eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder Unterstützung nicht oder nicht rechtzeitig gewährt,
5. entgegen § 8b Absatz 3 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 10 Absatz 1 Satz 1 oder entgegen § 8f Absatz 5 Satz 1 eine Registrierung nicht oder nicht rechtzeitig vornimmt oder eine dort genannte Stelle nicht oder nicht rechtzeitig benennt,
6. entgegen § 8b Absatz 3 Satz 4 nicht sicherstellt, dass er erreichbar ist,

7. entgegen § 8b Absatz 4 Satz 1, § 8c Absatz 3 Satz 1 oder § 8f Absatz 7 Satz 1 oder Absatz 8 Satz 1 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,
8. entgegen § 8c Absatz 1 Satz 1 eine dort genannte Maßnahme nicht trifft,
9. entgegen § 8f Absatz 1 eine Selbsterklärung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vorlegt,
10. entgegen § 9a Absatz 2 Satz 2 als Konformitätsbewertungsstelle tätig wird oder
11. entgegen § 9c Absatz 4 Satz 1 das IT-Sicherheitskennzeichen verwendet.

(3) Ordnungswidrig handelt, wer eine in Absatz 1 bezeichnete Handlung fahrlässig begeht.

(4) Ordnungswidrig handelt, wer gegen die Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15) verstößt, indem er vorsätzlich oder fahrlässig

1. entgegen Artikel 55 Absatz 1 eine dort genannte Angabe nicht, nicht richtig, nicht vollständig oder nicht binnen eines Monats nach Ausstellung zugänglich macht oder
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 in den Fällen des Absatzes 2 Nummer 1 Buchstabe a mit einer Geldbuße bis zu zwei Millionen Euro sowie in den Fällen der Absätze 1, 2 Nummer 2 und 3 mit einer Geldbuße bis zu einer Million Euro geahndet werden. Die Ordnungswidrigkeit kann in den Fällen des Absatzes 2 Nummer 1 Buchstabe c, Nummer 5 und 7 bis 11 und des Absatzes 4 mit einer Geldbuße bis zu fünfhunderttausend Euro sowie in den Fällen des Absatzes 2 Nummer 1 Buchstabe b, Nummer 4 und 6 und des Absatzes 3 mit einer Geldbuße bis zu einhunderttausend Euro geahndet werden. In den Fällen des Satzes 1 ist § 30 Absatz 2 Satz 3 des Gesetzes über Ordnungswidrigkeiten anzuwenden.

(6) Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist das Bundesamt.

§ 14a Institutionen der Sozialen Sicherung

Bei Zuwiderhandlungen gegen eine in § 14 Absatz 1 bis 4 genannte Vorschrift, die von Körperschaften gemäß § 29 des Vierten Buches Sozialgesetzbuch, Arbeitsgemeinschaften gemäß § 94 des Zehnten Buches Sozialgesetzbuch sowie der Deutschen Post AG, soweit sie mit der Berechnung oder Auszahlung von Sozialleistungen betraut ist (Institutionen der Sozialen Sicherung), begangen werden, finden die Sätze 2 bis 4 Anwendung. Bei einer in Satz 1 genannten Zuwiderhandlung von Institutionen der Sozialen Sicherung in Trägerschaft des Bundes stellt das Bundesamt das Einvernehmen über die zu ergreifenden Maßnahmen mit der für die Institution der Sozialen Sicherung zuständigen Aufsichtsbehörde her. Bei einer in Satz 1 genannten Zuwiderhandlung von Institutionen der Sozialen Sicherung in Trägerschaft der Länder informiert das Bundesamt die zuständige Aufsichtsbehörde und schlägt

geeignete Maßnahmen vor. Die jeweils zuständige Aufsichtsbehörde informiert das Bundesamt über die Einleitung und Umsetzung von Aufsichtsmitteln und sorgt für deren Durchsetzung.

§ 15 Anwendbarkeit der Vorschriften für Anbieter digitaler Dienste

Die Vorschriften, die Anbieter digitaler Dienste betreffen, sind ab dem 10. Mai 2018 anwendbar.

Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - BSI-KritisV)

Eingangsformel

Auf Grund des § 10 Absatz 1 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821), der zuletzt durch die Artikel 1 Nummer 8 des Gesetzes vom 17. Juli 2015 (BGBl. I S. 1324) geändert worden ist, verordnet das Bundesministerium des Innern im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr und digitale Infrastruktur, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit nach Anhörung der beteiligten Kreise:

§ 1 Begriffsbestimmungen

(1) Im Sinne dieser Verordnung ist oder sind

1. Anlagen
   a) Betriebsstätten und sonstige ortsfeste Einrichtungen,
   b) Maschinen, Geräte und sonstige ortsveränderliche Einrichtungen oder
   c) Software und IT-Dienste,

   die für die Erbringung einer kritischen Dienstleistung notwendig sind,
2. Betreiber
   eine natürliche oder juristische Person, die unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände bestimmenden Einfluss auf die Beschaffenheit und den Betrieb einer Anlage oder Teilen davon ausübt,
3. kritische Dienstleistung
   eine Dienstleistung zur Versorgung der Allgemeinheit in den Sektoren nach den §§ 2 bis 8, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde,
4. Versorgungsgrad
   ein Wert, mittels dessen der Beitrag einer Anlage oder Teilen davon im jeweiligen Sektor zur Versorgung der Allgemeinheit mit einer kritischen Dienstleistung bestimmt wird,
5. Schwellenwert
   ein Wert, bei dessen Erreichen oder dessen Überschreitung der Versorgungsgrad einer Anlage oder Teilen davon als bedeutend im Sinne von § 10 Absatz 1 Satz 1 des BSI-Gesetzes anzusehen ist.

(2) Einer Anlage sind alle vorgesehenen Anlagenteile und Verfahrensschritte zuzurechnen, die zum Betrieb notwendig sind, sowie Nebeneinrichtungen, die mit den Anlagenteilen und

Verfahrensschritten in einem betriebstechnischen Zusammenhang stehen und die für die Erbringung einer kritischen Dienstleistung notwendig sind. Mehrere Anlagen derselben Kategorie, die durch einen betriebstechnischen Zusammenhang verbunden sind, gelten als gemeinsame Anlage, wenn sie gemeinsam zur Erbringung derselben kritischen Dienstleistung notwendig sind. Betreiben zwei oder mehr Personen gemeinsam eine Anlage, so ist jeder für die Erfüllung der Pflichten als Betreiber verantwortlich.

§ 2 Sektor Energie

(1) Wegen ihrer besonderen Bedeutung für das Funktionieren des Gemeinwesens sind im Sektor Energie kritische Dienstleistungen im Sinne des § 10 Absatz 1 Satz 1 des BSI-Gesetzes:

1. die Versorgung der Allgemeinheit mit Elektrizität (Stromversorgung);
2. die Versorgung der Allgemeinheit mit Gas (Gasversorgung);
3. die Versorgung der Allgemeinheit mit Kraftstoff und Heizöl (Kraftstoff- und Heizölversorgung);
4. die Versorgung der Allgemeinheit mit Fernwärme (Fernwärmeversorgung).

(2) Die Stromversorgung wird in den Bereichen Stromerzeugung, Stromhandel, Stromübertragung und Stromverteilung erbracht.

(3) Die Gasversorgung wird in den Bereichen Gasförderung, Gashandel, Gastransport und Gasverteilung erbracht.

(4) Die Kraftstoff- und Heizölversorgung wird in den Bereichen Erdölförderung, Produktenherstellung, Mineralölhandel, Öltransport und -lagerung sowie Kraftstoff- und Heizölverteilung erbracht.

(5) Die Fernwärmeversorgung wird in den Bereichen Erzeugung von Fernwärme, Steuerung und Überwachung von Fernwärme sowie Verteilung von Fernwärme erbracht.

(6) Im Sektor Energie sind Kritische Infrastrukturen solche Anlagen oder Teile davon, die

1. den in Anhang 1 Teil 3 Spalte B genannten Kategorien zuzuordnen sind und
2. den Schwellenwert nach Anhang 1 Teil 3 Spalte D erreichen oder überschreiten.

§ 3 Sektor Wasser

(1) Wegen ihrer besonderen Bedeutung für das Funktionieren des Gemeinwesens sind im Sektor Wasser kritische Dienstleistungen im Sinne des § 10 Absatz 1 Satz 1 des BSI-Gesetzes:

1. die Versorgung der Allgemeinheit mit Trinkwasser (Trinkwasserversorgung);
2. die Beseitigung von Abwasser der Allgemeinheit (Abwasserbeseitigung).

(2) Die Trinkwasserversorgung wird in den Bereichen Gewinnung, Aufbereitung, Verteilung sowie Steuerung und Überwachung von Trinkwasser erbracht.

(3) Die Abwasserbeseitigung wird in den Bereichen Siedlungsentwässerung, Abwasserbehandlung und Gewässereinleitung sowie Steuerung und Überwachung erbracht.

(4) Im Sektor Wasser sind Kritische Infrastrukturen solche Anlagen oder Teile davon, die

1. den in Anhang 2 Teil 3 Spalte B genannten Kategorien zuzuordnen sind und

2. den Schwellenwert nach Anhang 2 Teil 3 Spalte D erreichen oder überschreiten.

§ 4 Sektor Ernährung

(1) Wegen ihrer besonderen Bedeutung für das Funktionieren des Gemeinwesens ist im Sektor Ernährung die Versorgung der Allgemeinheit mit Lebensmitteln (Lebensmittelversorgung) kritische Dienstleistung im Sinne des § 10 Absatz 1 Satz 1 des BSI-Gesetzes.

(2) Die Lebensmittelversorgung wird in den Bereichen Lebensmittelherstellung und -behandlung sowie Lebensmittelhandel erbracht.

(3) Im Sektor Ernährung sind Kritische Infrastrukturen solche Anlagen oder Teile davon, die

1. den in Anhang 3 Teil 3 Spalte B genannten Kategorien zuzuordnen sind und
2. den Schwellenwert nach Anhang 3 Teil 3 Spalte D erreichen oder überschreiten.

§ 5 Sektor Informationstechnik und Telekommunikation

(1) Wegen ihrer besonderen Bedeutung für das Funktionieren des Gemeinwesens sind im Sektor Informationstechnik und Telekommunikation kritische Dienstleistungen im Sinne des § 10 Absatz 1 Satz 1 des BSI-Gesetzes:

1. die Sprach- und Datenübertragung;
2. die Datenspeicherung und -verarbeitung.

(2) Die Sprach- und Datenübertragung wird in den Bereichen Zugang, Übertragung, Vermittlung und Steuerung erbracht.

(3) Die Datenspeicherung und -verarbeitung wird in den Bereichen Housing, IT-Hosting und Vertrauensdienste erbracht.

(4) Im Sektor Informationstechnik und Telekommunikation sind Kritische Infrastrukturen solche Anlagen oder Teile davon, die

1. den in Anhang 4 Teil 3 Spalte B genannten Kategorien zuzuordnen sind und
2. den Schwellenwert nach Anhang 4 Teil 3 Spalte D erreichen oder überschreiten.

§ 6 Sektor Gesundheit

(1) Wegen ihrer besonderen Bedeutung für das Funktionieren des Gemeinwesens sind im Sektor Gesundheit kritische Dienstleistungen im Sinne des § 10 Absatz 1 Satz 1 des BSI-Gesetzes:

1. die stationäre medizinische Versorgung;
2. die Versorgung mit unmittelbar lebenserhaltenden Medizinprodukten, die Verbrauchsgüter sind;
3. die Versorgung mit verschreibungspflichtigen Arzneimitteln und Blut- und Plasmakonzentraten zur Anwendung im oder am menschlichen Körper;
4. die Laboratoriumsdiagnostik.

(2) Die Versorgung mit unmittelbar lebenserhaltenden Medizinprodukten, die Verbrauchsgüter sind, wird in den Bereichen Herstellung und Abgabe erbracht.

(3) Die Versorgung mit verschreibungspflichtigen Arzneimitteln und Blut- und Plasmakonzentraten zur Anwendung im oder am menschlichen Körper wird in den Bereichen Herstellung, Vertrieb und Abgabe erbracht.

(4) Im Sektor Gesundheit sind Kritische Infrastrukturen solche Anlagen oder Teile davon, die

1. den in Anhang 5 Teil 3 Spalte B genannten Kategorien zuzuordnen sind und
2. den Schwellenwert nach Anhang 5 Teil 3 Spalte D erreichen oder überschreiten.

§ 7 Sektor Finanz- und Versicherungswesen

(1) Wegen ihrer besonderen Bedeutung für das Funktionieren des Gemeinwesens sind im Sektor Finanz- und Versicherungswesen kritische Dienstleistungen im Sinne des § 10 Absatz 1 Satz 1 des BSI-Gesetzes:

1. die Bargeldversorgung;
2. der kartengestützte Zahlungsverkehr;
3. der konventionelle Zahlungsverkehr;
4. der Handel mit Wertpapieren und Derivaten sowie die Verrechnung und die Abwicklung von Wertpapier- und Derivatgeschäften;
5. Versicherungsdienstleistungen und Leistungen der Sozialversicherung sowie der Grundsicherung für Arbeitsuchende.

(2) Die Bargeldversorgung wird in den Bereichen Autorisierung einer Abhebung, Einbringen in den Zahlungsverkehr, Belastung Kundenkonto und Bargeldlogistik erbracht.

(3) Der kartengestützte Zahlungsverkehr wird bei kartengebundenen Zahlungsvorgängen im Sinne der Verordnung (EU) 2015/751 des Europäischen Parlaments und des Rates vom 29. April 2015 über Interbankenentgelte für kartengebundene Zahlungsvorgänge (ABl. L 123 vom 19.5.2015, S. 1) in den Bereichen Autorisierung, Einbringen in den Zahlungsverkehr sowie Belastung auf dem Konto des Zahlers und Gutschrift auf dem Konto des Zahlungsempfängers erbracht.

(4) Der konventionelle Zahlungsverkehr wird bei Zahlungsvorgängen mittels Überweisung und Lastschrift im Sinne der Verordnung (EU) Nr. 260/2012 des Europäischen Parlaments und des Rates vom 14. März 2012 zur Festlegung der technischen Vorschriften und der Geschäftsanforderungen für Überweisungen und Lastschriften in Euro (ABl. L 94 vom 30.3.2012, S. 22) in den Bereichen Annahme einer Überweisung oder Lastschrift, Einbringen in den Zahlungsverkehr sowie Belastung und Gutschrift auf Kundenkonten erbracht.

(5) Der Handel mit Wertpapieren und Derivaten sowie die Verrechnung und die Abwicklung von Wertpapier- und Derivatgeschäften wird in den Bereichen Einbringen von Aufträgen in den Handel, Ausführung des Handels und Bestandsführung für den Kunden sowie Verrechnung von Wertpapier- und Derivatgeschäften, Verbuchung Wertpapiere und Verbuchung Geld erbracht.

(6) Versicherungsdienstleistungen werden im Bereich Inanspruchnahme von Versicherungsleistungen erbracht. Leistungen der Sozialversicherung werden im Bereich Inanspruchnahme von Sozialversicherungsleistungen erbracht. Leistungen der Grundsicherung für Arbeitsuchende werden im Bereich der Inanspruchnahme von Leistungen, die der Sicherung des Lebensunterhalts dienen, mithilfe von IT-Systemen der Bundesagentur für Arbeit erbracht.

(7) Im Sektor Finanz- und Versicherungswesen sind Kritische Infrastrukturen solche Anlagen oder Teile davon, die

1. den in Anhang 6 Teil 3 Spalte B genannten Kategorien zuzuordnen sind und
2. den Schwellenwert nach Anhang 6 Teil 3 Spalte D erreichen oder überschreiten.

(8) Abweichend von § 1 Nummer 2 hat im Sektor Finanz- und Versicherungswesen bestimmenden Einfluss auf eine Anlage, die den in Anhang 6 Teil 3 Spalte A Nummer 1 bis 4 genannten Anlagenkategorien zuzuordnen ist, wer die tatsächliche Sachherrschaft ausübt. Die rechtlichen und wirtschaftlichen Umstände bleiben insoweit unberücksichtigt.

§ 8 Sektor Transport und Verkehr

(1) Wegen ihrer besonderen Bedeutung für das Funktionieren des Gemeinwesens ist im Sektor Transport und Verkehr die Versorgung der Allgemeinheit mit Leistungen zum Transport von Personen und Gütern (Personen- und Güterverkehr) kritische Dienstleistung im Sinne des § 10 Absatz 1 Satz 1 des BSI-Gesetzes.

(2) Der Personen- und Güterverkehr wird in den Bereichen Luftverkehr, Eisenbahnverkehr, See- und Binnenschifffahrt, Straßenverkehr, öffentlicher Personennahverkehr (ÖPNV) und Logistik sowie verkehrsträgerübergreifend erbracht.

(3) Im Sektor Transport und Verkehr sind Kritische Infrastrukturen solche Anlagen oder Teile davon, die

1. den in Anhang 7 Teil 3 Spalte B genannten Kategorien zuzuordnen sind und
2. den Schwellenwert nach Anhang 7 Teil 3 Spalte D erreichen oder überschreiten.

§ 9 Sektor Siedlungsabfallentsorgung

(1) Wegen ihrer besonderen Bedeutung für das Funktionieren des Gemeinwesens ist im Sektor Siedlungsabfallentsorgung die Entsorgung von Siedlungsabfällen kritische Dienstleistung im Sinne des § 10 Absatz 1 Satz 1 des BSI-Gesetzes.

(2) Die Siedlungsabfallentsorgung wird in den Bereichen „Abfallsammlung und -beförderung“ und „Abfallverwertung und -beseitigung“ erbracht.

(3) Im Sektor Siedlungsabfallentsorgung sind Kritische Infrastrukturen solche Anlagen oder Teile davon, die

1. den in Anhang 8 Teil 3 Spalte B genannten Kategorien zuzuordnen sind und
2. den Schwellenwert nach Anhang 8 Teil 3 Spalte D erreichen oder überschreiten.

§ 10 Evaluierung

Zwei Jahre nach Inkrafttreten dieser Rechtsverordnung und danach alle zwei Jahre sind unter Beteiligung der in § 10 Absatz 1 Satz 1 des BSI-Gesetzes genannten Ressorts und unter Berücksichtigung von Erkenntnissen der Betreiber Kritischer Infrastrukturen, von deren Verbänden sowie von Vertretern der Wissenschaft zu evaluieren

1. die Festlegung der kritischen Dienstleistungen und Bereiche,
2. die Festlegung der Anlagenkategorien, die für die Erbringung der kritischen Dienstleistungen erforderlich sind, und
3. die Bestimmung der Schwellenwerte.

Anhang 1 (zu § 1 Nummer 4 und 5, § 2 Absatz 5 Nummer 1 und 2) Anlagenkategorien und Schwellenwerte im Sektor Energie

Teil 1 Grundsätze und Fristen

1. Für die in Teil 3 Spalte B genannten Anlagenkategorien gelten vorrangig die Begriffsbestimmungen nach § 3 des Energiewirtschaftsgesetzes und nach § 2 des Kraft-Wärme-Kopplungsgesetzes in der jeweils geltenden Fassung.

2. Im Sinne von Anhang 1 ist oder sind

2.1 Erzeugungsanlage

eine Anlage im Sinne des § 3 Nummer 18d des Energiewirtschaftsgesetzes. Diese Kategorie umfasst auch Anlagen zur Speicherung von elektrischer Energie sowie dezentrale Energieerzeugungsanlagen im Sinne des § 3 Nummer 11 des Energiewirtschaftsgesetzes.

2.2 Anlage oder System zur Bündelung und Steuerung elektrischer Leistung

eine Anlage oder ein System zur Bündelung elektrischer Leistung und Steuerung von Erzeugungsanlagen oder dezentraler Energieerzeugungsanlagen, insbesondere zur Anwendung bei Direktvermarktungsunternehmen im Sinne des § 3 Nummer 17 des Erneuerbare-Energien-Gesetzes. Unter den Begriff der Steuerung fallen auch die die Anlagen betreffenden Schalthandlungen.

2.3 Übertragungsnetz

ein Netz zur Übertragung im Sinne des § 3 Nummer 32 des Energiewirtschaftsgesetzes.

2.4 Zentrale Anlage oder System für den Stromhandel

eine Anlage oder ein elektronisches Handelssystem, das den physischen, kurzfristigen Spothandel sowie den Terminhandel mit Energie für das deutsche Marktgebiet betrifft.

2.5 Stromverteilernetz

ein Netz zur Verteilung von Elektrizität im Sinne des § 3 Nummer 37 des Energiewirtschaftsgesetzes.

2.6 Gasförderanlage

eine Anlage zur Förderung von Erdgas aus einer Bohrung.

2.7 Anlage zur zentralen standortübergreifenden Steuerung

eine Anlage oder ein IT-System, durch das eine oder mehrere Anlagen standortübergreifend gesteuert oder überwacht werden.

2.8 Fernleitungsnetz

ein Netz zur Fernleitung im Sinne des § 3 Nummer 19 des Energiewirtschaftsgesetzes.

2.9 Gasgrenzübergabestelle

eine Netzkoppelstelle, die in der Regel zwischen einem deutschen Fernleitungsnetz und dem eines anderen Staates besteht, soweit diese nicht von einem deutschen Fernleitungsnetzbetreiber als Bestandteil dessen Fernleitungsnetzes betrieben wird.

2.10 Gasspeicher

eine Speicheranlage im Sinne des § 3 Nummer 19c des Energiewirtschaftsgesetzes.

2.11 Gasverteilernetz

ein Netz zur Verteilung von Gas im Sinne des § 3 Nummer 37 des Energiewirtschaftsgesetzes.

2.12 Gas- oder Kapazitätshandelssystem

eine Anlage oder ein elektronisches Handelssystem für den Handel von Gasmengen oder -kapazitäten.

2.13 LNG-Anlage

schwimmende oder landgebundene stationäre Anlagen oder Systeme zur Verflüssigung von Gas nach § 3 Nr. 19a EnWG oder zur Einfuhr, Entladung und Wiederverdampfung von verflüssigtem Gas, einschließlich der Anlagenteile für Hilfsdienste und für die vorübergehende Speicherung von verflüssigtem Erdgas, die für die Wiederverdampfung und die anschließende Einspeisung in das Fernleitungsnetz erforderlich sind.

2.14 Ölförderanlage

eine Anlage zur Förderung von Erdöl aus einer Bohrung.

2.15 Raffinerie

eine Anlage zur Destillation oder Raffination oder sonstigen Weiterverarbeitung von Erdöl in Mineralölraffinerien im Sinne der Nummer 4.3 der Anlage 1 des Gesetzes über die Umweltverträglichkeitsprüfung.

2.16 Mineralölfernleitung

eine Rohrfernleitung im Sinne der Rohrfernleitungsverordnung zum Transport von Erdöl oder Erdölprodukten.

2.17 Erdöl- und Erdölproduktenlager

eine Anlage zur Lagerung von Erdöl oder Mineralölprodukten.

2.18 Anlage oder System von Aggregatoren zum Vertrieb von Kraftstoff und Heizöl

eine Anlage oder ein IT-System, das zur Disposition insbesondere von Tankkraftwagen, Kesselwagen oder Binnenschiffen verwendet wird, mit dem Ziel, den Vertrieb von Kraftstoff oder Heizöl abzuwickeln, zu koordinieren oder zu optimieren, unabhängig davon, ob durch die Anlage oder das IT-System Verbraucher beliefert werden.

2.19 Tankstellennetz

eine Anlage oder ein System zur Verbindung voneinander unabhängiger Tankstellen oder Flugfeldbetankungsanlagen mittels zentraler Komponenten (beispielsweise physischer oder datentechnischer Verbindungen). Eine zentrale Komponente dient der zentralen Erbringung wichtiger Aufgaben für den Betrieb der Tankstellen oder Flugfeldbetankungsanlagen eines Tankstellennetzes zur Versorgung mit Kraftstoff.

2.20 Anlage oder System zur zentralen kommerziellen Steuerung

eine Anlage oder ein System zur zentralen Steuerung oder Koordinierung der Betriebsplanung einer oder mehrerer Anlagen oder zur kommerziellen Abwicklung für eine oder mehrere Anlagen, soweit diese zum Betrieb notwendig sind. Dazu zählen auch Clearing-Instanzen oder Kollaborationslösungen, die als Cloud-Lösung betrieben werden.

2.21 Heizwerk

eine Anlage zur Erzeugung von Wärme zur Belieferung von Endkunden im Sinne der Verordnung über Allgemeine Bedingungen für die Versorgung mit Fernwärme.

2.22 Heizkraftwerk

eine KWK-Anlage im Sinne des § 2 Nummer 14 des Kraft-Wärme-Kopplungsgesetzes.

2.23 Fernwärmenetz

ein Netz zur Versorgung der Allgemeinheit mit Wärme.

3. Eine Anlage, die einer in Teil 3 Spalte B genannten Anlagenkategorie zuzuordnen ist, gilt ab dem 1. April des Kalenderjahres, das auf das Kalenderjahr folgt, in dem ihr Versorgungsgrad den in Teil 3 Spalte D genannten Schwellenwert erstmals erreicht oder überschreitet, als Kritische Infrastruktur. Nicht mehr als Kritische Infrastruktur gilt eine solche Anlage ab dem 1. April des Kalenderjahres, das auf das Kalenderjahr folgt, in dem ihr Versorgungsgrad den genannten Schwellenwert unterschreitet. Anlagen nach Teil 3 Nummer 2.2.4 gelten ab dem ersten Tag des dritten Kalendermonats, der auf den Kalendermonat folgt, in dem ihr Versorgungsgrad den in Teil 3 Spalte D genannten Schwellenwert erreicht oder überschreitet als Kritische Infra-

struktur. Diese Anlagen gelten nicht mehr als Kritische Infrastruktur ab dem 1. April des Kalenderjahres, in dem ihr Versorgungsgrad den genannten Schwellenwert unterschreitet.

4. Der Betreiber hat den Versorgungsgrad seiner Anlage für das zurückliegende Kalenderjahr jeweils bis zum 31. März des Folgejahres zu ermitteln. Betreiber von Anlagen nach Teil 3 Nummer 2.2.4 haben den aktuellen Versorgungsgrad ihrer Anlage jeweils zur Inbetriebnahme und zum 31. März eines jeden Kalenderjahres zu ermitteln.

5. Ist der Versorgungsgrad anhand der Anzahl angeschlossener Haushalte zu ermitteln, ist der Versorgungsgrad zum 30. Juni des zurückliegenden Kalenderjahres maßgeblich.

6. Ist der Versorgungsgrad anhand der Kapazität (installierte Netto-Nennleistung) einer Anlage zu ermitteln, ist auf den rechtlich und tatsächlich möglichen Betriebsumfang der durch denselben Betreiber betriebenen Anlage abzustellen.

7. Stehen mehrere Anlagen derselben Art in einem engen räumlichen und betrieblichen Zusammenhang (gemeinsame Anlage) und erreichen oder überschreiten die in Teil 3 Spalte D genannten Schwellenwerte zusammen, gilt die gemeinsame Anlage als Kritische Infrastruktur. Ein enger räumlicher und betrieblicher Zusammenhang ist gegeben, wenn die Anlagen

   a) auf demselben Betriebsgelände liegen,

   b) mit gemeinsamen Betriebseinrichtungen verbunden sind,

   c) einem vergleichbaren technischen Zweck dienen und

   d) unter gemeinsamer Leitung stehen.

Teil 2
Berechnungsformeln zur Ermittlung der Schwellenwerte

8. Der für die Anlagenkategorien des Teils 3 Nummer 1.1.1 und 1.1.2 genannte Schwellenwert von 104 MW ist unter Annahme eines Durchschnittsverbrauchs von 1 815 kWh pro versorgter Person pro Jahr und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

$$900\ \text{GWh/Jahr} \approx 908\ \text{GWh/Jahr} = 1\,815\ \text{kWh / Jahr} \times 500\,000$$

Die durchschnittliche elektrische Arbeit zur Versorgung von 500 000 Personen im Jahr entspricht im Falle der Nummern 1.1.1 und 1.1.2 einer installierten Nettonennleistung von:

$$104\ \text{MW} \approx (908\ \text{GWh/Jahr}) / (8\,760\ \text{h/Jahr})$$

Der Schwellenwert von 36 MW für zur Erbringung von Primärregelleistung präqualifizierter Anlagen ergibt sich aus Artikel 5 Absatz 3 der Verordnung (EU) 2016/631 der Kommission vom 14. April 2016 zur Festlegung eines Netzkodex mit Netzanschlussbestimmungen für Stromerzeuger.

9. Der für die Anlagenkategorien des Teils 3 Nummer 1.4.1 genannte Schwellenwert ist unter Annahme eines Gesamthandelsvolumens rund 7 400 TWh und eines Durch-

schnittshandelsvolumens pro Person pro Jahr von 92,6 MWh und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

$$46{,}3\ \text{TWh} \approx 92{,}6\ \text{MWh/Jahr} \times 500\,000$$

10. Der für die Anlagenkategorien des Teils 3 Nummer 2 genannte Schwellenwert ist unter Annahme eines Durchschnittsverbrauchs von 10 380 kWh pro versorgter Person pro Jahr und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

$$5\,190\ \text{GWh/Jahr} = 10\,380\ \text{kWh/Jahr} \times 500\,000$$

11. Der für die Anlagenkategorien des Teils 3 Nummer 3.1.2, 3.1.3, 3.2.2, 3.2.3, 3.3.1 und 3.3.3 genannte Schwellenwert ist unter Annahme einer durchschnittlichen Produktionsmenge von 0,84 Tonnen Kraftstoff zur Versorgung einer Person pro Jahr und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

$$420\,000\ \text{t/Jahr} = 0{,}84\ \text{t/Jahr} \times 500\,000$$

12. Der für Erdöl in den Anlagenkategorien des Teils 3 Nummer 3.1.1, 3.1.3, 3.2.1, 3.2.2, 3.2.3 und 3.4.1 genannte Schwellenwert ist unter Annahme einer durchschnittlichen Produktionsmenge von 1,24 Tonnen leichtem Heizöl zur Versorgung einer Person pro Jahr und damit einer durchschnittlichen Gesamtproduktionsmenge von 620 000 Tonnen leichtem Heizöl für 500 000 versorgte Personen sowie unter der Annahme, dass aus einer Tonne Rohöl etwa 0,14 Tonnen leichtes Heizöl hergestellt werden, wie folgt berechnet:

$$4\,400\,000\ \text{t/Jahr} = 620\,000\ \text{t/Jahr} / 0{,}14$$

13. Der für Kraftstoff in den Anlagenkategorien des Teils 3 Nummer 3.1.2, 3.1.3, 3.2.1, 3.2.2, 3.2.3, 3.3.1, 3.3.2, 3.3.3 und 3.4.1 genannte Schwellenwert ist unter Annahme einer durchschnittlichen Produktionsmenge von 0,84 Tonnen Kraftstoff zur Versorgung einer Person pro Jahr und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

$$420\,000\ \text{t/Jahr} = 0{,}84\ \text{t/Jahr} \times 500\,000$$

14. Der für Flugkraftstoff in den Anlagenkategorien des Teils 3 Nummer 3.1.2, 3.1.3, 3.2.1., 3.2.2, 3.2.3, 3.3.1, 3.3.2, 3.3.3 und 3.4.1 genannte Schwellenwert ist unter Annahme eines Durchschnittsverbrauchs einer Person pro Jahr von 0,1275 Tonnen Flugkraftstoff und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

$$63\,750\ \text{t/Jahr} = 0{,}1275\ \text{t/Jahr} \times 500\,000$$

15. Der für Heizöl in den Anlagenkategorien des Teils 3 Nummer 3.1.2, 3.1.3, 3.2.1, 3.2.2, 3.2.3, 3.3.1, 3.3.3 und 3.4.1 genannte Schwellenwert ist unter Annahme einer durchschnittlichen Produktionsmenge von 1,24 Tonnen leichtem Heizöl zur Versorgung einer Person pro Jahr und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

$$620\,000\ \text{t/Jahr} = 1{,}24\ \text{t/Jahr} \times 500\,000$$

Teil 3
Anlagenkategorien und Schwellenwerte

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
1	**Stromversorgung**		
1.1	Stromerzeugung		
1.1.1	Erzeugungsanlage	Installierte Nettonennleistung (elektrisch oder direkt mit Wärmeauskopplung verbundene elektrische Wirkleistung bei Wärmenennleistung ohne Kondensationsanteil) in MW oder	104
		installierte Nettonennleistung in MW, wenn die Anlage als Schwarzstartanlage nach § 3 Absatz 2 des Beschlusses der Bundesnetzagentur vom 20. Mai 2020, Aktenzeichen BK6-18-249 kontrahiert ist, oder	0
		installierte Nettonennleistung in MW, wenn die Anlage zur Erbringung von Primärregelleistung nach § 2 Nummer 8 StromNZV präqualifiziert ist	36
1.1.2	Anlage oder System zur Steuerung/Bündelung elektrischer Leistung	Installierte Nettonennleistung (elektrisch) in MW oder	104
		installierte Nettonennleistung in MW, wenn die Anlage als Schwarzstartanlage nach § 3 Absatz 2 des Beschlusses BK6-18-249 kontrahiert ist, oder	0
		installierte Nettonennleistung in MW, wenn die Anlage zur Erbringung von Primärregelleistung nach § 2 Nummer 8 StromNZV präqualifiziert ist	36
1.2	Stromübertragung		
1.2.1	Übertragungsnetz	Durch Letztverbraucher und Weiterverteiler entnommene Jahresarbeit in GWh/Jahr	3 700
1.3	Stromverteilung		
1.3.1	Stromverteilernetz	Durch Letztverbraucher und Weiterverteiler entnommene Jahresarbeit in GWh/Jahr	3 700

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
1.4	Stromhandel		
1.4.1	Zentrale Anlage oder System für den Stromhandel	Abgewickeltes Handelsvolumen in TWh/Jahr	3,7
2	**Gasversorgung**		
2.1	Gasförderung		
2.1.1	Gasförderanlage	Energie des geförderten Gases in GWh/Jahr	5 190
2.1.2	Anlage zur zentralen standortübergreifenden Steuerung	Energie des geförderten Gases in GWh/Jahr	5 190
2.2	Gastransport und -speicherung		
2.2.1	Fernleitungsnetz	Durch Letztverbraucher und Weiterverteiler entnommene Jahresarbeit in GWh/Jahr	5 190
2.2.2	Gasgrenzübergabestelle	Durchgeleitete Arbeit in GWh/Jahr	5 190
2.2.3	Gasspeicher	Entnommene Arbeit in GWh/Jahr	5 190
2.2.4	LNG-Anlage	Technische Regasifizierungskapazität in GWh/Jahr	5 190
2.3	Gasverteilung		
	Gasverteilernetz	Entnommene Arbeit in GWh/Jahr	5 190
2.4	Gashandel		
2.4.1	Gas- oder Kapazitätshandelssystem	Energie der gehandelten Gasmengen in GWh/Jahr oder	5 190
		Menge der gehandelten Gastransportkapazitäten in GWh/h/Jahr	5 190
3	**Kraftstoff- und Heizölversorgung**		
3.1	Erdölförderung und Produktenherstellung		
3.1.1	Ölförderanlage	Gefördertes Erdöl in Tonnen/Jahr	4 400 000
3.1.2	Raffinerie	Erzeugter Kraftstoff in Tonnen/Jahr oder	420 000 (≈ 420 Millionen Liter)
		erzeugter Flugkraftstoff in Tonnen/Jahr oder	63 750
		erzeugtes Heizöl in Tonnen/Jahr	620 000
3.1.3	Anlage zur zentralen standortübergreifenden Steuerung	Gefördertes Rohöl in Tonnen/Jahr oder	4 400 000
		erzeugter Kraftstoff in Tonnen/Jahr oder	420 000

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
		erzeugter Flugkraftstoff in Tonnen/Jahr oder	63 750
		erzeugtes Heizöl in Tonnen/Jahr	620 000
3.2	Erdöltransport und -lagerung		
3.2.1	Mineralölfernleitung	Transportierte entnommene Rohölmenge in Tonnen/Jahr oder	4 400 000
		transportierte Kraftstoffmenge in Tonnen/Jahr oder	420 000
		transportierte Flugkraftstoffmenge in Tonnen/Jahr oder	63 750
		transportierte Heizölmenge in Tonnen/Jahr	620 000
3.2.2	Erdöl- und Erdölproduktenlager	Umgeschlagenes Rohöl in Tonnen/Jahr oder	4 400 000
		umgeschlagener Kraftstoff in Tonnen/Jahr oder	420 000
		umgeschlagener Flugkraftstoff in Tonnen/Jahr oder	63 750
		umgeschlagenes Heizöl in Tonnen/Jahr	620 000
3.2.3	Anlage zur zentralen standortübergreifenden Steuerung	Gesamtmenge des transportierten Rohöls und der transportierten Ölprodukte in Tonnen/Jahr oder	4 400 000
		umgeschlagenes Rohöl in Tonnen/Jahr oder	4 400 000
		umgeschlagener Kraftstoff in Tonnen/Jahr oder	420 000
		umgeschlagener Flugkraftstoff in Tonnen/Jahr oder	63 750
		umgeschlagenes Heizöl in Tonnen/Jahr	620 000
3.3	Kraftstoff- und Heizölverteilung		
3.3.1	Anlage oder System von Aggregatoren zum Vertrieb von Kraftstoff und Heizöl	Verteilter Kraftstoff in Tonnen/Jahr oder	420 000
		verteilter Flugkraftstoff in Tonnen/Jahr oder	63 750
		verteiltes Heizöl in Tonnen/Jahr	620 000
3.3.2	Tankstellennetz	Verteilter Kraftstoff in Tonnen/Jahr oder	420 000

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
		verteilter Flugkraftstoff in Tonnen/Jahr	63 750
3.3.3	Anlage zur zentralen standortübergreifenden Steuerung	Verteilter Kraftstoff in Tonnen/Jahr oder	420 000
		verteilter Flugkraftstoff in Tonnen/Jahr oder	63 750
		verteiltes Heizöl in Tonnen/Jahr	620 000
3.4	Mineralölhandel		
3.4.1	Anlagen oder Systeme zur zentralen kommerziellen Steuerung	Abgewickeltes Erdöl in Tonnen/Jahr oder	4 400 000
		abgewickelter Kraftstoff in Tonnen/Jahr oder	420 000
		abgewickelter Flugkraftstoff in Tonnen/Jahr oder	63 750
		abgewickeltes Heizöl in Tonnen/Jahr	620 000
4	**Fernwärmeversorgung**		
4.1	Erzeugung von Fernwärme		
4.1.1	Heizwerk	Ausgeleitete Wärmeenergie in GWh/Jahr	2 300
4.1.2	Heizkraftwerk	Ausgeleitete Wärmeenergie in GWh/Jahr	2 300
4.2	Verteilung von Fernwärme		
4.2.1	Fernwärmenetz	Angeschlossene Haushalte	250 000
4.3	Steuerung und Überwachung		
4.3.1	Anlage zur zentralen standortübergreifenden Steuerung	Angeschlossene Haushalte oder	250 000
		ausgeleitete Wärmeenergie in GWh/Jahr	2 300

Anhang 2 (zu § 1 Nummer 4 und 5, § 3 Absatz 4 Nummer 1 und 2)
Anlagenkategorien und Schwellenwerte im Sektor Wasser

Teil 1
Grundsätze und Fristen

1. Im Sinne von Anhang 2 ist oder sind

1.1. Gewinnungsanlage

ein Brunnen oder eine Brunnenreihe, eine Sickerleitung, ein Sickerstollen, eine Zisterne, ein Entnahmebauwerk oder eine Stauanlage zur Gewinnung, Bevorratung

oder Bewirtschaftung von Oberflächenwasser oder andere Wasserfassung zur Gewinnung von Rohwasser.

1.2. Aufbereitungsanlage (Wasserwerk)

die Gesamtheit aller technischen Einrichtungen zur Trinkwasseraufbereitung einschließlich der zugehörigen Nebenanlagen sowie der Mess-, Steuerungs- und Regelungstechnik.

1.3. Wasserverteilungssystem

ein Teil eines Wasserversorgungssystems mit Rohrleitungen, Trinkwasserbehältern, Förderanlagen und sonstigen Einrichtungen zum Zweck der Verteilung von Wasser an die Verbraucher. Dieses System beginnt nach der Wasseraufbereitungsanlage oder, wenn keine Aufbereitung erfolgt, nach der Wassergewinnung oder bei Weiterverteilern an der Übergabestelle des Vorlieferanten und endet an der Übergabestelle zum Verbraucher.

1.4. Leitzentrale

eine Anlage, insbesondere eine Leitwarte, Leitstelle oder Prozessleitwarte, in der ein oder mehrere Prozessschritte auch räumlich verteilter Anlagen zentral überwacht und/oder gesteuert werden können.

1.5. Kanalisation

ein Netz von Rohrleitungen und Zusatzbauten (zum Beispiel Regenüberlaufbecken, Regenrückhaltebecken, Regenklärbecken und Pumpstationen), das Abwasser von Anschlusskanälen zu Kläranlagen oder zu anderen Entsorgungsstellen ableitet.

1.6. Kläranlage

eine Anlage, in der Abwasser physikalisch, biologisch oder chemisch behandelt wird. Die Anlagen zur Gewässereinleitung (zum Beispiel Hochwasserpumpwerke und Ableitungskanäle) werden als Bestandteil der Kläranlage angesehen.

2. Eine Anlage, die einer in Teil 3 Spalte B genannten Anlagenkategorie zuzuordnen ist, gilt ab dem 1. April des Kalenderjahres, das auf das Kalenderjahr folgt, in dem ihr Versorgungsgrad den in Teil 3 Spalte D genannten Schwellenwert erstmals erreicht oder überschreitet, als Kritische Infrastruktur. Nicht mehr als Kritische Infrastruktur gilt eine solche Anlage ab dem 1. April des Kalenderjahres, das auf das Kalenderjahr folgt, in dem ihr Versorgungsgrad den genannten Schwellenwert unterschreitet. Nicht mehr als Kritische Infrastruktur gilt eine solche Anlage ab dem 1. April des Kalenderjahres, das auf das Kalenderjahr folgt, in dem ihr Versorgungsgrad den genannten Schwellenwert unterschreitet.

3. Der Betreiber hat den Versorgungsgrad seiner Anlage für das zurückliegende Kalenderjahr jeweils bis zum 31. März des Folgejahres zu ermitteln.

4. Für die Anlagenkategorien des Teils 3 Nummer 1.1.1 bis 1.3.1 ist der Versorgungsgrad zum 30. Juni des zurückliegenden Kalenderjahres maßgeblich.

5. Stehen mehrere Anlagen derselben Art in einem engen räumlichen und betrieblichen Zusammenhang (gemeinsame Anlage) und erreichen oder überschreiten die in

Teil 3 Spalte D genannten Schwellenwerte zusammen, gilt die gemeinsame Anlage als Kritische Infrastruktur. Ein enger räumlicher und betrieblicher Zusammenhang ist gegeben, wenn die Anlagen

a) auf demselben Betriebsgelände liegen,

b) mit gemeinsamen Betriebseinrichtungen verbunden sind,

c) einem vergleichbaren technischen Zweck dienen und

d) unter gemeinsamer Leitung stehen.

Teil 2
Berechnungsformeln zur Ermittlung der Schwellenwerte

6. Der für die Anlagenkategorien des Teils 3 Nummer 1.1.1 bis 1.4.1 genannte Schwellenwert ist unter Annahme eines Durchschnittsverbrauchs von 44 m3 pro versorgter Person pro Jahr und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

22 Millionen m3/Jahr = 44 m3/Jahr x 500 000

Teil 3
Anlagenkategorien und Schwellenwerte

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
1	**Trinkwasserversorgung**		
1.1	Gewinnung		
1.1.1	Gewinnungsanlage	Gewonnene Wassermenge in Millionen m³/Jahr	22
1.2	Aufbereitung		
1.2.1	Aufbereitungsanlage (Wasserwerk)	Aufbereitete Trinkwassermenge in Millionen m³/Jahr	22
1.3	Verteilung		
1.3.1	Wasserverteilungssystem	Verteilte Wassermenge in Millionen m³/Jahr	22
1.4	Steuerung und Überwachung		
1.4.1	Leitzentrale	Von den gesteuerten/überwachten Anlagen gewonnene, transportierte oder aufbereitete Wassermenge in Millionen m³/Jahr	22
2	**Abwasserbeseitigung**		

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
2.1	Siedlungsentwässerung		
2.1.1	Kanalisation	Angeschlossene Einwohner	500 000
2.2	Abwasserbehandlung und Gewässereinleitung		
2.2.1	Kläranlage	Ausbaugröße in Einwohnerwerten	500 000
2.3	Steuerung und Überwachung		
2.3.1	Leitzentrale	Ausbaugrößen der Anlagen in Einwohnerwerten oder angeschlossene Einwohner der gesteuerten oder überwachten Anlagen	500 000

Anhang 3 (zu § 1 Nummer 4 und 5, § 4 Absatz 3 Nummer 1 und 2) Anlagenkategorien und Schwellenwerte im Sektor Ernährung

Teil 1 Grundsätze und Fristen

1. Für die in Teil 3 Spalte B Nummer 1 genannten Anlagenkategorien gelten grundsätzlich die Begriffsbestimmungen des § 3 Nummer 1 bis 3 des Lebensmittel-, Bedarfsgegenstände- und Futtermittelgesetzbuches in der jeweils geltenden Fassung.

2. Im Sinne von Anhang 3 ist oder sind

2.1 Anlage oder System zur Herstellung von Lebensmitteln

eine Anlage zum Herstellen von Lebensmitteln im Sinne des § 3 Absatz 1 Nummer 1 des Lebensmittel- und Futtermittelgesetzbuches.

2.2 Anlage oder System zur Behandlung von Lebensmitteln

eine Anlage zum Behandeln von Lebensmitteln im Sinne des § 3 Absatz 1 Nummer 2 des Lebensmittel- und Futtermittelgesetzbuches.

2.3 Anlage oder System zur Distribution von Lebensmitteln

eine Anlage oder ein System zur Planung, Steuerung, Bereitstellung und Verteilung von Produktionsmitteln oder Lebensmitteln, zum Beispiel Fuhrpark-, Hof- oder Flottenmanagementsysteme.

2.4 Anlage oder System zur zentralen Steuerung oder Überwachung

eine Anlage oder ein System, durch die oder das eine oder mehrere andere Anlagen oder Systeme gesteuert oder überwacht werden, zum Beispiel ERP-, Warenwirtschafts- oder Lagerverwaltungssysteme.

2.5 Anlage oder System zur Bestellung von Lebensmitteln

eine Anlage oder ein System zur Aufgabe oder Entgegennahme von Lebensmittelbestellungen, zum Beispiel EDI-Dispositionssysteme, Lieferanten- und Kundenstammdatensysteme.

2.6 Anlage oder System zum Inverkehrbringen von Lebensmitteln

eine Anlage oder ein System zum Inverkehrbringen von Lebensmitteln im Sinne des Artikels 3 Nummer 8 der Verordnung (EG) Nr. 178/2002 des Europäischen Parlaments und des Rates vom 28. Januar 2002 zur Festlegung der allgemeinen Grundsätze und Anforderungen des Lebensmittelrechts, zur Errichtung der Europäischen Behörde für Lebensmittelsicherheit und zur Festlegung von Verfahren zur Lebensmittelsicherheit (ABl. L 31 vom 1.2.2002, S. 1), die zuletzt durch die Verordnung (EU) 2019/1381 (ABl. L 231 vom 6.9.2019, S. 1) geändert worden ist, zum Beispiel eine Verkaufsstelle des Einzel- oder Großhandels.

3. Eine Anlage, die einer in Teil 3 Spalte B genannten Anlagenkategorie zuzuordnen ist, gilt ab dem 1. April des Kalenderjahres, das auf das Kalenderjahr folgt, in dem ihr Versorgungsgrad den in Teil 3 Spalte D genannten Schwellenwert erstmalig erreicht oder überschreitet, als Kritische Infrastruktur. Nicht mehr als Kritische Infrastruktur gilt eine solche Anlage ab dem 1. April des Kalenderjahres, das auf das Kalenderjahr folgt, in dem ihr Versorgungsgrad den genannten Schwellenwert unterschreitet.

4. Der Betreiber hat den Versorgungsgrad seiner Anlage für das zurückliegende Kalenderjahr jeweils bis zum 31. März des Folgejahres zu ermitteln.

5. Stehen mehrere Anlagen derselben Art in einem engen räumlichen und betrieblichen Zusammenhang (gemeinsame Anlage) und erreichen oder überschreiten die in Teil 3 Spalte D genannten Schwellenwerte zusammen, gilt die gemeinsame Anlage als Kritische Infrastruktur. Ein enger räumlicher und betrieblicher Zusammenhang ist gegeben, wenn die Anlagen

   a) auf demselben Betriebsgelände liegen,

   b) mit gemeinsamen Betriebseinrichtungen verbunden sind,

   c) einem vergleichbaren technischen Zweck dienen und

   d) unter gemeinsamer Leitung stehen.

6. Die Ermittlung des Versorgungsgrads kann, bei einer Anlage, die den Anlagenkategorien des Teils 3 Spalte A Nummer 1.2 zuzuordnen ist, mittels einer pauschalierten Umrechnung der in Teil 3 Spalte D genannten Schwellenwerte auf den in einem Kalenderjahr erzielten Bruttoumsatz in einem Verhältnis von 3,90 Euro pro kg oder l erfolgen.

Teil 2
Berechnungsformeln zur Ermittlung der Schwellenwerte

7. Der für die Anlagenkategorien des Teils 3 genannte Schwellenwert (Lebensmittel außer Getränke) ist unter Annahme einer durchschnittlichen Produktionsmenge zur Versorgung einer Person mit Lebensmitteln aller Produktgruppen außer Getränken

von 0,869 Tonnen/Jahr sowie eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

434 500 t/Jahr = 0,869 t/Jahr x 500 000

8. Der für die Anlagenkategorien des Teils 3 genannte Schwellenwert (Getränke) ist unter Annahme eines Durchschnittsverbrauchs von 700 l/Jahr von Getränken mit Ausnahme von Getränken mit einem Alkoholgehalt von mehr als 1,2 Volumenprozent sowie eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

350 Millionen l/Jahr = 700 l/Jahr x 500 000

Teil 3
Anlagenkategorien und Schwellenwerte

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
1	**Lebensmittelversorgung**		
1.1	Lebensmittelherstellung und -behandlung		
1.1.1	Anlage oder System zur Herstellung von Lebensmitteln	Hergestellte Lebensmittel außer Getränke in Tonnen/Jahr oder	434 500
		hergestellte Getränke außer Getränke mit einem Alkoholgehalt von mehr als 1,2 Volumenprozent in Liter/Jahr	350 000 000
1.1.2	Anlage oder System zur Behandlung von Lebensmitteln	Behandelte Lebensmittel außer Getränke in Tonnen/Jahr oder	434 500
		behandelte Getränke außer Getränke mit einem Alkoholgehalt von mehr als 1,2 Volumenprozent in Liter/Jahr	350 000 000
1.1.3	Anlage oder System zur Distribution von Lebensmitteln	Umgeschlagene Lebensmittel außer Getränke in Tonnen/Jahr oder	434 500
		umgeschlagene Getränke außer Getränke mit einem Alkoholgehalt von mehr als 1,2 Volumenprozent in Liter/Jahr	350 000 000
1.1.4	Anlage oder System zur zentralen Steuerung oder Überwachung	Hergestellte, behandelte, umgeschlagene, bestellte oder in Verkehr gebrachte Lebensmittel außer Getränke aller durch die Anlage oder das System gesteuerten oder überwachten Anlagen in Tonnen/Jahr oder	434 500
		hergestellte, behandelte, umgeschlagene, bestellte oder in Verkehr gebrachte Getränke außer Getränke mit einem Alkoholgehalt von mehr als 1,2 Volumenprozent aller durch die Anlage oder das System gesteuerten oder überwachten Anlagen in Liter/Jahr	350 000 000

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
1.2	Lebensmittelhandel		
1.2.1	Anlage oder System zur Behandlung von Lebensmitteln	Behandelte Lebensmittel außer Getränke in Tonnen/Jahr oder	434 500
		behandelte Getränke außer Getränke mit einem Alkoholgehalt von mehr als 1,2 Volumenprozent in Liter/Jahr	350 000 000
1.2.2	Anlage oder System zur Distribution von Lebensmitteln	Umgeschlagene Lebensmittel außer Getränke in Tonnen/Jahr oder	434 500
		umgeschlagene Getränke außer Getränke mit einem Alkoholgehalt von mehr als 1,2 Volumenprozent in Liter/Jahr	350 000 000
1.2.3	Anlage oder System zur Bestellung von Lebensmitteln	Bestellte Lebensmittel außer Getränke in Tonnen/Jahr oder	434 500
		bestellte Getränke außer Getränke mit einem Alkoholgehalt von mehr als 1,2 Volumenprozent in Liter/Jahr	350 000 000
1.2.4	Anlage oder System zum Inverkehrbringen von Lebensmitteln	In Verkehr gebrachte Lebensmittel außer Getränke in Tonnen/Jahr oder	434 500
		in Verkehr gebrachte Getränke außer Getränke mit einem Alkoholgehalt von mehr als 1,2 Volumenprozent in Liter/Jahr	350 000 000
1.2.5	Anlage oder System zur zentralen Steuerung oder Überwachung	Behandelte, umgeschlagene, bestellte oder in Verkehr gebrachte Lebensmittel außer Getränke aller durch die Anlage oder das System gesteuerten oder überwachten Anlagen in Tonnen/Jahr oder	434 500
		behandelte, umgeschlagene, bestellte oder in Verkehr gebrachte Getränke außer Getränke mit einem Alkoholgehalt von mehr als 1,2 Volumenprozent aller durch die Anlage oder das System gesteuerten oder überwachten Anlagen in Liter/Jahr	350 000 000

Anhang 4 (zu § 1 Nummer 4 und 5, § 5 Absatz 4 Nummer 1 und 2) Anlagenkategorien und Schwellenwerte im Sektor Informationstechnik und Telekommunikation

Teil 1 Grundsätze und Fristen

1. Für die in Teil 3 Spalte B genannten Anlagenkategorien gelten vorrangig die Begriffsbestimmungen nach § 3 des Telekommunikationsgesetzes in der jeweils geltenden Fassung.

2. Im Sinne von Anhang 4 ist oder sind

2.1 Zugangsnetz

eine Anlage, über die der Zugang zu einem Sprachkommunikationsdienst, zu einem öffentlich zugänglichen Datenübertragungsdienst oder zu einem Internetzugangsdienst erfolgt, zum Beispiel Glasfaseranschlüsse und Mobilfunkzugangsnetze.

2.2 Übertragungsnetz

eine Anlage zur Übertragung von Sprache und Daten für Sprachkommunikationsdienste und öffentlich zugängliche Datenübertragungsdienste oder für Internetzugangsdienste, zum Beispiel Backbone- und Core-Netze.

2.3 Seekabelanlandestation

eine Anlandestation zur Anbindung primär der Sprach- und Datenübertragung dienender Seekabel an landgestützte Telekommunikationsnetze.

2.4 IXP

eine von den angeschlossenen autonomen Systemen unabhängige Netzeinrichtung, die die Zusammenschaltung von mehr als zwei unabhängigen autonomen Systemen für den Zweck des Austausches von Internetdatenverkehr ermöglicht. Eine Anlage ist auch dann ein IXP, wenn der Internetdatenverkehr zwischen zwei beliebigen teilnehmenden autonomen Systemen nicht über ein intermediäres autonomes System läuft.

2.5 DNS-Resolver

eine Anlage oder ein System im Zugangsnetz eines Anbieters von Internetzugangsdiensten zur Beantwortung von Anfragen zur Namensauflösung, die oder das bei Unkenntnis der Antwort die Anfragen an übergeordnete DNS-Instanzen weiterreicht, wenn die Anlage oder das System zur Nutzung von Sprachkommunikationsdiensten, öffentlich zugänglichen Datenübertragungsdiensten oder Internetzugangsdiensten angeboten wird.

2.6 Autoritativer DNS-Server

eine Anlage oder ein System zur Beantwortung von Anfragen zur Namensauflösung gemäß Kapitel 5 des RFC 7719, in der oder in dem durch lokal vorliegende Informationen über den Inhalt einer DNS-Zone Anfragen über diese DNS-Zone beantwortet werden oder die Anfragen an andere Server delegiert werden.

2.7 Top-Level-Domain-Name-Registry

eine Anlage, welche die Registrierung von Internet-Domain-Namen innerhalb einer spezifischen Top-Level-Domain (TLD) verwaltet und betreibt.

2.8 Rechenzentrum (Housing)

ein oder mehrere Gebäude, zumindest aber ein geschlossener Raum mit dem vorrangigen Zweck, eine geeignete Umgebung für die Unterbringung und den Betrieb von zentralen IT-Komponenten, zum Beispiel Server oder Netzwerktechnik, in mindestens zehn Racks bereitzustellen.

2.9 Serverfarm (Hosting)

zwei oder mehrere physische oder virtuelle Instanzen, die im IT-Netzwerk Dienste bereitstellen. Dabei gelten virtuelle Maschinen, die mit einem eigenen Betriebssystem auf einer physischen Instanz betrieben werden, als virtuelle Instanzen.

2.10 Content Delivery Network

ein Netz regional verteilter und über das Internet verbundener Server, mit dem Inhalte ausgeliefert und zwischengespeichert werden, um insbesondere die Verfügbarkeit und Performanz zu erhöhen.

2.11 Anlage zur Erbringung von Vertrauensdiensten

eine vertrauenswürdige dritte Instanz (Trusted Third Party), die in elektronischen Kommunikationsprozessen die jeweilige Identität des Kommunikationspartners bescheinigt.

3. Eine Anlage, die einer in Teil 3 Spalte B genannten Anlagenkategorie zuzuordnen ist, gilt ab dem 1. April des Kalenderjahres, das auf das Kalenderjahr folgt, in dem ihr Versorgungsgrad den in Teil 3 Spalte D genannten Schwellenwert erstmals erreicht oder überschreitet, als Kritische Infrastruktur. Nicht mehr als Kritische Infrastruktur gilt eine solche Anlage ab dem 1. April des Kalenderjahres, das auf das Kalenderjahr folgt, in dem ihr Versorgungsgrad den genannten Schwellenwert unterschreitet.

4. Der Betreiber hat den Versorgungsgrad seiner Anlage für das zurückliegende Kalenderjahr bis zum 31. März des Folgejahres zu ermitteln.

5. Für die Anlagenkategorien des Teils 3 Nummer 1.1.1 bis 1.2.1 und 2.1.1 ist der Versorgungsgrad zum 30. Juni des zurückliegenden Kalenderjahres jeweils maßgeblich.

6. Stehen mehrere Anlagen derselben Art in einem engen betrieblichen Zusammenhang (gemeinsame Anlage) und erreichen oder überschreiten die in Teil 3 Spalte D genannten Schwellenwerte zusammen, gilt die gemeinsame Anlage als Kritische Infrastruktur. Ein enger betrieblicher Zusammenhang ist unabhängig von der räumlichen Distanz der Anlagen gegeben, wenn die Anlagen

   a) mit gemeinsamen Betriebseinrichtungen oder untereinander verbunden sind,

   b) einem vergleichbaren technischen Zweck dienen und

   c) unter gemeinsamer Leitung oder Steuerung stehen.

Teil 2
Berechnungsformeln zur Ermittlung der Schwellenwerte

7. Der für die Anlagenkategorien des Teils 3 Nummer 1.1 und 1.2 genannte Schwellenwert ergibt sich aus § 185 Absatz 1 Satz 1 des Telekommunikationsgesetzes in der jeweils geltenden Fassung.

8. Der für die Anlagenkategorie des Teils 3 Nummer 1.3.1 genannte Schwellenwert von 100 autonomen Systemen basiert auf der wirtschaftlichen und regionalen Relevanz der betroffenen IXPs.

9. Der für die Anlagenkategorie des Teils 3 Nummer 1.4.2 und 1.4.3 genannte Schwellenwert ist unter Annahme von 40 Millionen in der Bundesrepublik Deutschland verwalteten Domains und einer Bedarfsabdeckung von 500 000 versorgten Personen bei einer Gesamtbevölkerung von 80 Millionen Personen wie folgt berechnet:

$$250\,000 \approx (500\,000 / 80\,000\,000) \times 40\,000\,000$$

10. Die für die Anlagenkategorie des Teils 3 Nummer 2.2.1 genannten Schwellenwerte sind unter Annahme von 1,6 Millionen physischen und 2,4 Millionen virtuellen in der Bundesrepublik Deutschland verwalteten Serverinstanzen und einer Bedarfsabdeckung von 500 000 versorgten Personen bei einer Gesamtbevölkerung von 80 Millionen Personen wie folgt berechnet:

$$\text{Physische Instanzen: } 1\,600\,000 \times 500\,000 / 80\,000\,000 = 10\,000$$

$$\text{Virtuelle Instanzen: } 2\,400\,000 \times 500\,000 / 80\,000\,000 = 15\,000$$

11. Der für die Anlagenkategorie des Teils 3 Nummer 2.2.2 genannte Schwellenwert ist unter Annahme eines Transportvolumens von 11 826 000 Terabyte/Jahr und einer Bedarfsabdeckung von 500 000 versorgten Personen bei 80 Millionen Personen Gesamtbevölkerung wie folgt berechnet:

$$75\,000\ \text{TByte/Jahr} \approx (500\,000 / 80\,000\,000) \times 11\,826\,000\ \text{TByte/Jahr}$$

Teil 3
Anlagenkategorien und Schwellenwerte

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
1.	**Sprach- und Datenübertragung**		
1.1	Zugang		
1.1.1	Zugangsnetz	Teilnehmeranschlüsse des Zugangsnetzes nach § 3 Nummer 58 TKG	100 000
1.2	Übertragung		
1.2.1	Übertragungsnetz	Vertragspartner des jeweiligen Dienstes	100 000

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
1.2.2	Seekabelanlandestation	Anzahl der angebundenen Seekabel	1
1.3	Vermittlung		
1.3.1	IXP	Anzahl angeschlossener autonomer Systeme (Jahresdurchschnitt)	100
1.4	Steuerung		
1.4.1	DNS-Resolver	Anzahl der Vertragspartner des Zugangsnetzes, in dem der DNS-Resolver betrieben wird	100 000
1.4.2	Autoritativer DNS-Server	Anzahl der Domains, für die der Server autoritativ ist oder die aus der Zone delegiert werden	250 000
1.4.3	Top-Level-Domain-Name-Registry	Anzahl der Domains, die verwaltet oder betrieben werden	250 000
2.	**Datenspeicherung- und Verarbeitung**		
2.1	Housing		
2.1.1	Rechenzentrum (Housing)	Vertraglich vereinbarte Leistung in MW	3,5
2.2	IT-Hosting		
2.2.1	Serverfarm (Hosting)	Anzahl der für Nutzer betriebenen physischen Instanzen (Jahresdurchschnitt)	10 000
		Anzahl der für Nutzer betriebenen virtuellen Instanzen (Jahresdurchschnitt)	15 000
2.2.2	Content Delivery Network	Ausgeliefertes Datenvolumen (in TByte/Jahr)	75 000
2.3	Vertrauensdienste		
2.3.1	Anlage zur Erbringung von Vertrauensdiensten	Anzahl der ausgegebenen qualifizierten Zertifikate oder	500 000
		Anzahl der Zertifikate zur Authentifizierung öffentlich zugänglicher Server (Serverzertifikate, z. B. für Webserver, E-Mailserver, Cloudserver (z. B. TLS/SSL-Zertifikate))	10 000

Anhang 5 (zu § 1 Nummer 4 und 5, § 6 Absatz 6 Nummer 1 und 2) Anlagenkategorien und Schwellenwerte im Sektor Gesundheit

Teil 1 Grundsätze und Fristen

1. Im Sinne von Anhang 5 ist oder sind

1.1 Krankenhaus

ein zugelassenes Krankenhaus im Sinne des § 108 des Fünften Buches Sozialgesetzbuch.

1.2 Produktionsstätte für unmittelbar lebenserhaltende Medizinprodukte, die Verbrauchsgüter sind

eine Betriebsstätte, in der Medizinprodukte für Beatmung/Tracheostomie, parenterale Ernährung, enterale Ernährung, ableitende Inkontinenz, Dialyse und Diabetes – Typ 1 hergestellt werden.

1.3 Abgabestelle

eine Einrichtung, in der Medizinprodukte für Beatmung/Tracheostomie, parenterale Ernährung, enterale Ernährung, ableitende Inkontinenz und Diabetes – Typ 1 abgegeben werden.

1.4 Produktionsstätte für verschreibungspflichtige Arzneimittel zur Anwendung im oder am menschlichen Körper

eine Betriebsstätte, die auf der Grundlage einer Herstellungserlaubnis nach § 13 des Arzneimittelgesetzes Hilfsstoffe und Hilfsmaterialien sowie Wirkstoffe zu verschreibungspflichtigen Arzneimitteln zur Anwendung im oder am menschlichen Körper nach § 48 Absatz 1 des Arzneimittelgesetzes verarbeitet.

1.5 Blut- oder Plasmaspendensteuerungssystem

ein zentrales IT-System in Blutspendeeinrichtungen oder Herstellungseinheiten zur Steuerung und Verwaltung von Entnahme und Weiterverarbeitung von Blut- oder Plasmaspenden zur Anwendung im oder am menschlichen Körper.

1.7 Betriebs- und Lagerraum

eine Einrichtung zur kurzzeitigen Lagerung von verschreibungspflichtigen Arzneimitteln, von Blutspenden und Blut- und Plasmaderivaten sowie zur Weiterverarbeitung oder Aufbereitung von Blutspenden und Blut- und Plasmaderivaten zur Anwendung im oder am menschlichen Körper; Teil der Einrichtung sind Anlagen und Systeme für den Wareneingang, die Lagerung und den Warenausgang.

1.8 Anlage oder System zum Vertrieb von verschreibungspflichtigen Arzneimitteln

ein zentrales Logistikmanagementsystem für den Vertrieb und die Disposition von verschreibungspflichtigen Arzneimitteln zur Anwendung im oder am menschlichen Körper.

1.9 Apotheke

eine Einrichtung im Sinne des ersten Abschnitts des Apothekengesetzes zur Bereitstellung verschreibungspflichtiger Arzneimittel für Patienten.

1.10 Labor

eine Einrichtung, in der medizinische labordiagnostische Verfahren für Diagnose und Therapiekontrolle in der Humanmedizin durchgeführt und deren Ergebnisse fachärztlich befundet werden.

1.11 Laborinformationsverbund

ein Verbund von Anlagen oder Systemen, die IT-Dienstleistungen für Diagnose und Therapiekontrolle in der Humanmedizin für mindestens ein Labor zur Verfügung stellen; zu den IT-Dienstleistungen zählen insbesondere die Steuerung des Probentransports, die Kommunikation zum Auftragseingang und zur Befundübermittlung sowie der Betrieb eines Laborinformationssystems.

2. Eine Anlage, die einer in Teil 3 Spalte B genannten Anlagenkategorie zuzuordnen ist, gilt ab dem 1. April des Kalenderjahres, das auf das Kalenderjahr folgt, in dem ihr Versorgungsgrad den in Teil 3 Spalte D genannten Schwellenwert erstmals erreicht oder überschreitet, als Kritische Infrastruktur. Nicht mehr als Kritische Infrastruktur gilt eine solche Anlage ab dem 1. April des Kalenderjahres, das auf das Kalenderjahr folgt, in dem ihr Versorgungsgrad den genannten Schwellenwert unterschreitet.

3. Der Betreiber hat den Versorgungsgrad seiner Anlage für das zurückliegende Kalenderjahr jeweils bis zum 31. März des Folgejahres zu ermitteln.

4. Stehen mehrere Anlagen derselben Art in einem engen räumlichen und betrieblichen Zusammenhang (gemeinsame Anlage) und erreichen oder überschreiten die in Teil 3 Spalte D genannten Schwellenwerte zusammen, gilt die gemeinsame Anlage als Kritische Infrastruktur. Ein enger räumlicher und betrieblicher Zusammenhang ist gegeben, wenn die Anlagen

   a) auf demselben Betriebsgelände liegen,

   b) mit gemeinsamen Betriebseinrichtungen verbunden sind,

   c) einem vergleichbaren technischen Zweck dienen und

   d) unter gemeinsamer Leitung stehen.

5. Nummer 4 findet keine Anwendung auf Anlagen, die der in Teil 3 Nummer 1.1 genannten Anlagenkategorie zuzuordnen sind.

Teil 2
Berechnungsformeln zur Ermittlung der Schwellenwerte

6. Der für die Anlagenkategorien des Teils 3 Nummer 2.1.1 und 2.2.1 genannte Schwellenwert ist unter Annahme von durchschnittlichen Ausgaben für Medizinprodukte, die Verbrauchsgüter sind, von 181,36 Euro pro versorgter Person pro Jahr und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

90 680 000 Euro Umsatz/Jahr = 181,36 Euro Umsatz/Jahr x 500 000

7. Der für die Anlagenkategorien des Teils 3 Nummer 3.1.1 sowie 3.2.1 bis 3.3.1 genannte Schwellenwert ist unter Annahme eines Durchschnittsverbrauchs von 9,3 Packungen verschreibungspflichtiger Arzneimittel pro versorgter Person pro Jahr und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

4 650 000 Packungen/Jahr = 9,3 Packungen/Jahr x 500 000

8. Der für die Anlagenkategorie des Teils 3 Nummer 3.1.2 genannte Schwellenwert ist unter Annahme eines Durchschnittswerts von 0,068 Einheiten hergestellten Erythrozytenkonzentrats, Thrombozytenkonzentrats und Plasmas zur Transfusion pro versorgter Person pro Jahr und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

34 000 Einheiten/Jahr = 0,068 Einheiten/Jahr x 500 000

9. Der für die Anlagenkategorien des Teils 3 Nummer 4 genannte Schwellenwert ist unter Annahme eines Durchschnittswerts von 3 Aufträgen für eine labormedizinische Untersuchung pro versorgter Person pro Jahr und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

1 500 000 Aufträge/Jahr = 3 Aufträge/Jahr x 500 000

Teil 3
Anlagenkategorien und Schwellenwerte

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
1	**Stationäre medizinische Versorgung**		
1.1	Krankenhaus	Vollstationäre Fallzahl/Jahr	30 000
2	**Versorgung mit unmittelbar lebenserhaltenden Medizinprodukten, die Verbrauchsgüter sind**		
2.1	Herstellung		
2.1.1	Produktionsstätte	Umsatz in Euro/Jahr	90 680 000
2.2	Abgabe		
2.2.1	Abgabestelle	Umsatz in Euro/Jahr	90 680 000
3	**Versorgung mit verschreibungspflichtigen Arzneimitteln und Blut- und Plasmakonzentraten zur Anwendung im oder am menschlichen Körper**		
3.1	Herstellung		
3.1.1	Produktionsstätte	In Verkehr gebrachte Packungen/Jahr	4 650 000
3.1.2	Blut- oder Plasmaspendensteuerungssystem	Hergestellte oder in Verkehr gebrachte Produkte/Jahr	34 000
3.2	Vertrieb		
3.2.1	Betriebs- und Lagerraum	Umgeschlagene Packungen/Jahr	4 650 000

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
3.2.2	Anlage oder System zum Vertrieb verschreibungspflichtiger Arzneimittel	Transportierte Packungen/Jahr	4 650 000
3.3	Abgabe		
3.3.1	Apotheke	Abgegebene Packungen/Jahr	4 650 000
4	**Laboratoriumsdiagnostik**		
4.1	Labor	Anzahl der Aufträge/Jahr oder	1 500 000
4.2	Laborinformationsverbund	kumulierte Anzahl der Aufträge im Verbund/Jahr	1 500 000

Anhang 6 (zu § 1 Nummer 4 und 5, § 7 Absatz 7 Nummer 1 und 2) Anlagenkategorien und Schwellenwerte im Sektor Finanz- und Versicherungswesen

Teil 1 Grundsätze und Fristen

1. Im Sinne von Anhang 6 ist oder sind

1.1 Autorisierungssystem

ein System, mit dem ein angefragter Transaktionsbetrag bei Transaktionen aus Geldautomatensystemen oder aus dem kartengestützten Zahlungsverkehr nach Prüfung der Kartendaten durch das kontoführende Institut oder den Zahlungsdienstleister genehmigt oder abgelehnt wird.

1.2 System zur Anbindung an ein Autorisierungssystem aus Sicht des Geldautomatenbetreibers

ein System, das der Anbindung des Geldautomatenbetreibers an ein Autorisierungssystem des kontoführenden Instituts dient.

1.3 System zur Aufbereitung durch den Geldautomatenbetreiber

ein System eines Geldautomatenbetreibers, welches Nachrichten oder Transaktionen aus Geldautomatensystemen verarbeitet, um die Transaktion in den Zahlungsverkehr einzubringen.

1.4 System zur Anbindung an ein Interbanken-Zahlungsverkehrssystem

ein System, das den Zahlungsdienstleister an die Interbanken-Zahlungsverkehrssysteme anbindet.

1.5 Clearing-System

ein System, das im Interbankenverkehr die Transaktionsdaten (Clearing-Daten) an das kontoführende Institut weiterleitet.

1.6 Settlement-System

ein System zur Verrechnung von Beträgen zwischen den partizipierenden Instituten.

1.7 Kontoführungssystem

ein System des Zahlungsdienstleisters des Zahlers oder des Zahlungsdienstleisters des Zahlungsempfängers zur elektronischen Führung und Verwaltung der Konten.

1.8 Cash Center

Einrichtungen von Wertdienstleistern, in denen Bargeld geprüft, gezählt, sortiert, gelagert oder wieder ausgegeben wird.

1.9 IT-System für das Cash Management

ein System des Wertdienstleisters zur Berichterstattung, zur Bestellung von Bargeld und zum Cash Management des Wertdienstleisters.

1.10 System zur Anbindung an ein Autorisierungssystem aus Sicht des Terminalbetreibers

ein System, das der Anbindung des Terminalbetreibers (zum Beispiel des Netzbetreibers) an ein Autorisierungssystem dient oder Transaktionen zum zuständigen Autorisierungssystem weiterleitet.

1.11 System zur Aufbereitung durch den POS-Terminalbetreiber

ein System eines Netzbetreibers oder POS-Terminalbetreibers, welches Nachrichten oder Transaktionen von POS-Terminals verarbeitet, um Transaktionen in den Zahlungsverkehr einzubringen.

1.12 System zur Annahme der POS-Transaktionsdaten beim Zahlungsdienstleister des Zahlungsempfängers

ein System, das Transaktionen von einem Acquirer annimmt.

1.13 System zur Annahme einer Überweisung oder Lastschrift

ein System, mit dem Überweisungsaufträge oder Aufträge zum Einzug von Lastschriften durch den Zahlungsdienstleister des Zahlers oder des Zahlungsempfängers als kontoführendes Institut angenommen und verarbeitet werden. Hiervon umfasst sind auch Überweisungsaufträge, die über einen Zahlungsauslösedienstleister im Sinne von Artikel 4 Nummer 18 der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 eingereicht werden.

1.14 System einer Clearingstelle oder einer zentralen Gegenpartei zur Verrechnung von Wertpapier- und Derivatgeschäften

ein System der Clearingstelle oder einer zentralen Gegenpartei gemäß § 1 Absatz 31 des Kreditwesengesetzes.

1.15 System zur Anbindung für die Verrechnung und Verbuchung von Wertpapier- und Derivatgeschäften

ein System, das der Anbindung eines Teilnehmers oder einer Handelsplattform zu einer Clearingstelle oder zentralen Gegenpartei sowie von einer Clearingstelle oder zentralen Gegenpartei zu einer Verbuchungsstelle dient.

1.16 Wertpapier-Settlement-System

ein Wertpapierliefer- und -abrechnungssystem gemäß Artikel 2 Absatz 1 Nummer 10 der Verordnung (EU) Nr. 909/2014.

1.17 Depotführungssystem eines Finanzmarktinfrastrukturbetreibers

ein System eines Finanzmarktinfrastrukturbetreibers, das zur Prüfung des Depotbestands und für Transaktionen von Depots genutzt wird.

1.18 System eines Zentralverwahrers

ein System eines Zentralverwahrers gemäß Artikel 2 Absatz 1 Nummer 1 der Verordnung (EU) Nr. 909/2014.

1.19 System zur Aufbereitung von Zahlungsanweisungen

ein System eines Finanzmarktbetreibers, welches Wertpapier- oder Derivattransaktionen mittelbar oder unmittelbar verarbeitet, um die Transaktionen in den Zahlungsverkehr einzubringen.

1.20 System für das Erzeugen und Weiterleiten von Aufträgen zum Handel von Wertpapieren und Derivaten an einen Handelsplatz

ein System, in dem Kundenaufträge zum Handel von Wertpapieren und Derivaten entgegengenommen, aufbereitet und an Handelsplätze weitergeleitet werden.

1.21 System eines Handelsplatzes

System eines Handelsplatzes im Sinne des Artikels 4 Nummer 24 der Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014.

1.22 Sonstiges Depotführungssystem

ein System, das zur Prüfung des Depotbestands und für Transaktionen von Depots genutzt wird und nicht zur unmittelbaren Infrastruktur eines Zentralverwahrers in der Rolle eines Finanzmarktinfrastrukturbetreibers gehört.

1.23 Vertragsverwaltungssystem

ein System zur Speicherung und Verarbeitung von Informationen zum Versicherungsvertragsverhältnis eines Lebensversicherers, einer privaten Krankenversicherung oder einer Kompositversicherung.

1.24 Leistungssystem

ein System zur Bearbeitung von Leistungen im Bereich Lebensversicherung und privater Krankenversicherung oder ein integriertes Anwendungssystem zur Erfassung, Prüfung und Berechnung von sozialversicherungsrechtlichen Entgeltersatzleistungen der gesetzliche Unfall- und Arbeitslosenversicherung, der gesetzlichen Rentenversicherung oder ein IT-System der Bundesagentur für Arbeit zur Erfassung, Speicherung, Berechnung und Bewilligung von Leistungen der Grundsicherung für Arbeitsuchende zur Sicherung des Lebensunterhalts nach dem Zweiten Buch Sozialgesetzbuch.

1.25 Schadensystem (Komposit)

ein System zur Bearbeitung von Schäden im Bereich der Schaden- und Unfallversicherungen.

1.26 Auszahlungssystem

ein System zur Auszahlung der Entschädigung, Versicherungsleistung oder Leistungen der Sozialversicherung oder ein IT-System der Bundesagentur für Arbeit zur Auszahlung von Leistungen der Grundsicherung für Arbeitsuchende zur Sicherung des Lebensunterhaltes nach dem Zweiten Buch Sozialgesetzbuch an den Zahlungsempfänger.

1.27 Verwaltungs- und Zahlungssystem der gesetzlichen Kranken- und Pflegeversicherung

ein integriertes Anwendungssystem im Bereich der gesetzlichen Kranken- und Pflegeversicherung.

2. Eine Anlage, die einer in Teil 3 Spalte B genannten Anlagenkategorie zuzuordnen ist, gilt ab dem 1. April des Kalenderjahres, das auf das Kalenderjahr folgt, in dem ihr Versorgungsgrad den in Teil 3 Spalte D genannten Schwellenwert erstmals erreicht oder überschreitet, als Kritische Infrastruktur. Nicht mehr als Kritische Infrastruktur gilt eine solche Anlage ab dem 1. April des Kalenderjahres, das auf das Kalenderjahr folgt, in dem ihr Versorgungsgrad den genannten Schwellenwert unterschreitet.

3. Abweichend von Nummer 1 gilt eine Anlage, die den Anlagenkategorien des Teils 3 Spalte A Nummer 5.1.3, 5.1.7 oder 5.1.11 zuzuordnen ist, ab dem 1. April des Kalenderjahres, das auf die drei Kalenderjahre folgt, deren durchschnittlicher Versorgungsgrad den in Teil 3 Spalte D genannten Schwellenwert erstmals erreicht oder überschreitet, als Kritische Infrastruktur.

4. Der Betreiber hat den Versorgungsgrad seiner Anlage für das zurückliegende Kalenderjahr jeweils bis zum 31. März des Folgejahres zu ermitteln.

5. Bei der Ermittlung des Versorgungsgrades einer Anlage, die den Anlagenkategorien des Teils 3 Spalte A Nummer 5.1.1, 5.1.4 oder 5.1.8 zuzuordnen ist, sind nur ablaufende Verträge mit Auszahlung der Versicherungsleistung zu berücksichtigen. Ungeachtet der Auszahlungsweise ist jeder Leistungsfall nur einmalig, bei wiederkehrenden Auszahlungen nur bei der erstmaligen Leistungsbearbeitung zu berücksichtigen.

6. Stehen mehrere Anlagen derselben Art in einem engen betrieblichen Zusammenhang (gemeinsame Anlage) und erreichen oder überschreiten die in Teil 3 Spalte D genannten Schwellenwerte zusammen, gilt die gemeinsame Anlage als Kritische Infrastruktur. Ein enger betrieblicher Zusammenhang ist gegeben, wenn die Anlagen

   a) mit gemeinsamen Betriebseinrichtungen verbunden sind,

   b) einem identischen technischen Zweck dienen und

   c) unter gemeinsamer Leitung stehen.

Teil 2 -
Berechnungsformeln zur Ermittlung der Schwellenwerte

7. Der für die Anlagenkategorien des Teils 3 Nummer 1.1.1 bis 1.2.1 und 1.3.1 genannte Schwellenwert ist unter Annahme von 30 Transaktionen mit im Inland ausgegebenen Karten an Terminals (Geldautomaten) in- und ausländischer Zahlungsdienst-

leister pro versorgter Person pro Jahr und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

15 000 000 Transaktionen/Jahr = 30 Transaktionen/Jahr x 500 000

8. Der für die Anlagenkategorie des Teils 3 Nummer 1.4 genannte Schwellenwert ist unter der Annahme von 187 im Cash-Center bearbeiteten Banknoten zur Versorgung einer Person pro Jahr und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

93 500 000 Banknoten/Jahr = 187 Banknoten/Jahr x 500 000

9. Der für die Anlagenkategorien des Teils 3 Nummer 1.2.2 bis 1.2.4 und 2.2.3 bis 2.2.5 genannte Schwellenwert ist unter Annahme von 36 Transaktionen als Mittelwert mit im Inland ausgegebenen Karten an POS-Terminals und Geldautomaten in- und ausländischer Zahlungsdienstleister pro versorgter Person pro Jahr und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

18 000 000 Transaktionen/Jahr = 36 Transaktionen/Jahr x 500 000

10. Der für die Anlagenkategorien des Teils 3 Nummer 2.1.1 bis 2.2.2 und 2.3.1 genannte Schwellenwert ist unter Annahme von 43 Transaktionen mit im Inland ausgegebenen Karten an Terminals (POS) in- und ausländischer Zahlungsdienstleister und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

21 500 000 Transaktionen/Jahr = 43 Transaktionen/Jahr x 500 000

11. Der für die Anlagenkategorien des Teils 3 Nummer 3 genannte Schwellenwert ist unter Annahme von 200 Transaktionen bei Überweisungen und Lastschriften pro versorgter Person und pro Jahr und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

100 000 000 Transaktionen/Jahr = 200 Transaktionen/Jahr x 500 000

12. Der für die Anlagenkategorien des Teils 3 Nummer 4.1.1, 4.1.2, 4.2.1, 4.2.2, 4.2.3, 4.3.1 und 4.5.1 genannte Schwellenwert ist unter Annahme von 1,7 Abwicklungstransaktionen im In- und Ausland pro versorgter Person pro Jahr und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

850 000 Transaktionen/Jahr = 1,7 Transaktionen/Jahr x 500 000

13. Der für die Anlagenkategorien des Teils 3 Nummer 4.4.1 und 4.6.1 genannte Schwellenwert ist unter Annahme von 13,5 Transaktionen pro versorgter Person pro Jahr und eines Regelschwellenwertes von 500 000 Personen wie folgt berechnet:

6 750 000 Transaktionen/Jahr = 13,5 Transaktionen/Jahr x 500 000

14. Der für die Anlagenkategorien des Teils 3 Nummer 5.1.1, 5.1.2 und 5.1.4 genannte Schwellenwert für die private Krankenversicherung ist unter Annahme von vier Leistungsfällen pro versorgter Person pro Jahr und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

2 000 000 Leistungsfälle/Jahr = 4 Leistungsfälle/Jahr x 500 000

Teil 3
Anlagenkategorien und Schwellenwerte

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
1	**Bargeldversorgung**		
1.1	Autorisierung einer Abhebung		
1.1.1	Autorisierungssystem	Anzahl der Transaktionen/Jahr	15 000 000
1.1.2	System zur Anbindung an ein Autorisierungssystem aus Sicht des Geldautomatenbetreibers	Anzahl der Transaktionen/Jahr	15 000 000
1.2	Einbringen in den Zahlungsverkehr		
1.2.1	System zur Aufbereitung durch den Geldautomatenbetreiber	Anzahl der Transaktionen/Jahr	15 000 000
1.2.2	System zur Anbindung an ein Interbanken-Zahlungsverkehrssystem (Clearing und Settlement)	Anzahl der Transaktionen/Jahr	18 000 000
1.2.3	Clearing-System	Anzahl der Transaktionen/Jahr	18 000 000
1.2.4	Settlement-System	Anzahl der Transaktionen des zugehörigen Clearing-Systems/Jahr	18 000 000
1.3	Belastung Kundenkonto		
1.3.1	Kontoführungssystem	Anzahl der in diesem System bei der Erbringung einer kritischen Dienstleistung verbuchten Transaktionen	15 000 000
1.4	Bargeldlogistik		
1.4.1	Cash Center	Anzahl bearbeiteter Banknoten/Jahr	93 500 000
1.4.2	IT-System für das Cash Management	Anzahl bearbeiteter Banknoten/Jahr	93 500 000
2	**Kartengestützter Zahlungsverkehr**		
2.1	Autorisierung		
2.1.1	Autorisierungssystem	Anzahl der in diesem System bei der Erbringung einer kritischen Dienstleistung autorisierten Transaktionen	21 500 000
2.1.2	System zur Anbindung an ein Autorisierungssystem aus Sicht des Terminalbetreibers	Anzahl der in diesem System bei der Erbringung einer kritischen Dienstleistung	21 500 000

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
		autorisierten Transaktionen	
2.2	Einbringen in den Zahlungsverkehr		
2.2.1	System zur Aufbereitung durch den POS-Terminalbetreiber	Anzahl der Transaktionen/Jahr	21 500 000
2.2.2	System zur Annahme der POS-Transaktionsdaten beim Zahlungsdienstleister des Zahlungsempfängers	Anzahl der Transaktionen/Jahr	21 500 000
2.2.3	System zur Anbindung an ein Interbanken-Zahlungsverkehrssystem (Clearing und Settlement)	Anzahl der Transaktionen/Jahr	18 000 000
2.2.4	Clearing-System	Anzahl der Transaktionen/Jahr	18 000 000
2.2.5	Settlement-System	Anzahl der Transaktionen des zugehörigen Clearing-Systems/Jahr	18 000 000
2.3	Belastung auf dem Konto des Zahlers und Gutschrift auf dem Konto des Zahlungsempfängers		
2.3.1	Kontoführungssystem	Anzahl der in diesem System bei der Erbringung der jeweiligen kritischen Dienstleistung verbuchten Transaktionen	21 500 000
3	**Konventioneller Zahlungsverkehr**		
3.1	Annahme einer Überweisung oder Lastschrift		
3.1.1	System zur Annahme einer Überweisung oder Lastschrift	Anzahl der Transaktionen/Jahr	100 000 000
3.2	Einbringen in den Zahlungsverkehr		
3.2.1	System zur Anbindung an ein Interbanken-Zahlungsverkehrssystem (Clearing und Settlement)	Anzahl der Transaktionen/Jahr	100 000 000
3.2.2	Clearing-System	Anzahl der Transaktionen/Jahr	100 000 000
3.2.3	Settlement-System	Anzahl der Transaktionen des zugehörigen Clearing-Systems/Jahr	100 000 000
3.3	Belastung und Gutschrift auf Kundenkonten		
3.3.1	Kontoführungssystem	Anzahl der Transaktionen/Jahr	100 000 000
4	**Handel, Verrechnung und Abwicklung von Wertpapier- und Derivatgeschäften**		
4.1	Verrechnung von Wertpapier- und Derivatgeschäften		

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
4.1.1	System einer Clearingstelle oder zentralen Gegenpartei zur Verrechnung von Wertpapier- und Derivatgeschäften	Anzahl der Transaktionen/Jahr	850 000
4.1.2	System zur Anbindung für die Verrechnung und Verbuchung von Wertpapier- und Derivatgeschäften	Anzahl der Transaktionen/Jahr	850 000
4.2	Verbuchung Wertpapiere		
4.2.1	Wertpapier-Settlement-System	Anzahl der Transaktionen/Jahr	850 000
4.2.2	Depotführungssystem eines Finanzmarktinfrastrukturbetreibers	Anzahl der Transaktionen/Jahr	850 000
4.2.3	System eines Zentralverwahrers	Anzahl der Transaktionen/Jahr	850 000
4.3	Verbuchung Geld		
4.3.1	System zur Aufbereitung der Zahlungsanweisung	Anzahl der Transaktionen/Jahr	850 000
4.4	Einbringen von Aufträgen in den Handel		
4.4.1	System für das Erzeugen von Aufträgen zum Handel von Wertpapieren und Derivaten und Weiterleiten an einen Handelsplatz	Anzahl der Transaktionen/Jahr	6 750 000
4.5	Ausführung des Handels		
4.5.1	System eines Handelsplatzes	Anzahl der Transaktionen/Jahr	850 000
4.6	Bestandsführung für den Kunden		
4.6.1	Sonstiges Depotführungssystem	Anzahl der Transaktionen/Jahr	6 750 000
5	**Versicherungsdienstleistungen und Leistungen der Sozialversicherung sowie der Grundsicherung für Arbeitsuchende**		
5.1	Versicherungsdienstleistungen		
5.1.1	Vertragsverwaltungssystem	Leistungsfälle Lebensversicherung/Jahr oder	500 000
		Leistungsfälle private Krankenversicherung/Jahr oder	2 000 000
		Schadensfälle Kompositversicherung/Jahr	500 000
5.1.2	Leistungssystem	Leistungsfälle Lebensversicherung/Jahr oder	500 000
		Leistungsfälle private	2 000 000

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
		Krankenversicherung/Jahr oder	
5.1.3	Schadensystem (Komposit)	Schadensfälle Kompositversicherung/Jahr	500 000
5.1.4	Auszahlungssystem	Leistungsfälle Lebensversicherung/Jahr oder	500 000
		Leistungsfälle private Krankenversicherung/Jahr oder	2 000 000
		Schadensfälle Kompositversicherung/Jahr	500 000
5.2	Leistungen der Sozialversicherung sowie der Grundsicherung für Arbeitsuchende		
5.2.1	Verwaltungs- und Zahlungssystem der gesetzlichen Kranken- und Pflegeversicherung	Anzahl der Versicherten	500 000
5.2.2	Leistungssystem	Leistungsfälle Sozialversicherungsträger der gesetzlichen Unfall- und Arbeitslosenversicherung/Jahr oder	500 000
		Anzahl der Versicherungskonten des Sozialversicherungsträgers der gesetzlichen Rentenversicherung oder	500 000
		Leistungsfälle zur Sicherung des Lebensunterhalts in der Grundsicherung für Arbeitsuchende nach dem Zweiten Buch Sozialgesetzbuch	500 000
5.2.3	Auszahlungssystem	Leistungsfälle Sozialversicherungsträger der gesetzlichen Unfall- und Arbeitslosenversicherung/Jahr oder	500 000
		Anzahl der Versicherungskonten des Sozialversicherungsträgers der gesetzlichen Rentenversicherung oder	500 000
		Leistungsfälle zur Sicherung des Lebensunterhalts in der Grundsicherung für Arbeitsuchende nach dem	500 000

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
		Zweiten Buch Sozialgesetzbuch	

Anhang 7 (zu § 1 Nummer 4 und 5, § 8 Absatz 3 Nummer 1 und 2) Anlagenkategorien und Schwellenwerte im Sektor Transport und Verkehr

Teil 1 Grundsätze und Fristen

1. Im Sinne von Anhang 7 ist oder sind

1.1 Anlage oder System zur Passagierabfertigung an Flugplätzen

eine Anlage oder ein System für die Passagier- oder Gepäckabfertigung im Sinne von § 2 Nummer 4 in Verbindung mit Anlage 1 Nummer 2 oder 3 der Bodenabfertigungsdienst-Verordnung.

1.2 Anlage oder System zur Frachtabfertigung an Flugplätzen

eine Anlage oder ein System zur Abfertigung von Fracht im Luftverkehr im Sinne von § 2 Nummer 4 in Verbindung mit Anlage 1 Nummer 4 der Bodenabfertigungsdienst-Verordnung.

1.3 Infrastrukturbetrieb eines Flugplatzes

die Gesamtheit aller Anlagen oder Systeme zur Erbringung von sonstigen Bodenabfertigungsdiensten nach § 2 Nummer 4 in Verbindung mit Anlage 1 Nummer 5, 7, 9 oder 10 der Bodenabfertigungsdienst-Verordnung.

1.4 Anlage zur Erbringung von Flugsicherungsdiensten

eine Anlage oder ein System der Flugsicherungsdienste nach der Durchführungsverordnung (EU) 2017/373 der Kommission vom 1. März 2017 zur Festlegung gemeinsamer Anforderungen an Flugverkehrsmanagementanbieter und Anbieter von Flugsicherungsdiensten sowie sonstiger Funktionen des Flugverkehrsmanagementnetzes und die Aufsicht hierüber sowie zur Aufhebung der Verordnung (EG) Nr. 482/2008, der Durchführungsverordnungen (EU) Nr. 1034/2011, (EU) Nr. 1035/2011 und (EU) 2016/1377 und zur Änderung der Verordnung (EU) Nr. 677/2011 (ABl. L 62 vom 8.3.2017, S. 1; L 15 vom 20.1.2020, S. 9), die durch die Durchführungsverordnung (EU) 2020/469 (ABl. L 104 vom 3.4.2020, S. 1) geändert worden ist.

1.5 Verkehrszentrale einer Fluggesellschaft

eine Anlage oder ein System einer Fluggesellschaft zur Planung, Steuerung oder Überwachung des Flugbetriebs, zur Disposition von Personal oder zur Disposition des Wartungsbetriebs.

1.6 Flughafenleitungsorgan

eine Anlage oder ein System zur Verwaltung oder zum Betrieb der Einrichtungen eines Flughafens oder Flughafennetzes oder zur Koordinierung oder Überwachung der Tätigkeiten der verschiedenen Akteure auf einem Flughafen oder in einem Flughafennetz.

1.7 Personenbahnhof der Eisenbahn

ein Bahnhof zur Abwicklung des Reiseverkehrs gemäß § 4 Absatz 1 und 2 der Eisenbahn-Bau- und Betriebsordnung.

1.8 Güterbahnhof

ein Bahnhof zur Abwicklung des Güterverkehrs gemäß § 4 Absatz 1 und 2 der Eisenbahn-Bau- und Betriebsordnung.

1.9 Zugbildungsbahnhof

ein Bahnhof zur Bildung von Zügen (Einzelwagen, Ganzzüge sowie kombinierter Verkehr).

1.10 Schienennetz und Stellwerke der Eisenbahn

ein Schienennetz gemäß § 4 Absatz 3 bis 7 und 10 bis 11 der Eisenbahn-Bau- und Betriebsordnung einschließlich der zugehörigen Stellwerke.

1.11 Verkehrssteuerungs- und Leitsystem der Eisenbahn

die zentrale Einrichtung des Eisenbahninfrastrukturbetreibers, die den Zugbetrieb vorausschauend und bei unerwartet eintretenden Ereignissen disponiert.

1.12 Leitzentrale der Eisenbahn

eine regionale oder überregionale zentrale Einrichtung des Eisenbahnverkehrsunternehmens zur Überwachung des betrieblichen Ist-Zustandes, zur Einleitung von Maßnahmen bei Verspätungen oder Störungsfällen oder zur Disposition der unternehmenseigenen Züge, des Personals oder der Instandhaltung der Fahrzeuge.

1.13 Anlage oder System zum Betrieb von Bundeswasserstraßen

eine Anlage oder ein System zum sicheren Betrieb einer Wasserstraße nach § 1 Absatz 4 Nummer 1 des Bundeswasserstraßengesetzes.

1.14 Verkehrssteuerungs- und Leitsystem der See- und Binnenschifffahrt

Revier- und Verkehrszentralen der Wasserstraßen- und Schifffahrtsverwaltung des Bundes.

1.15 Leitzentrale von Betreibern und Verkehrsunternehmen der Seeschifffahrt

eine Anlage oder ein System zur operativen Steuerung oder zur Disposition des Schiffsraums von Seeschiffen.

1.16 Leitzentrale von Betreibern und Verkehrsunternehmen der Binnenschifffahrt (nur Güterverkehr)

eine Anlage oder ein System zur operativen Steuerung oder zur Disposition des Schiffsraums der Binnenschifffahrtsflotte.

1.17 Umschlaganlage in See- und Binnenhäfen

eine Umschlaganlage in einem See- oder Binnenhafen, in der Container oder lose, unverpackte Güter zwischen Verkehrsträgern (auch den gleichen) be- und entladen, umgeschlagen, sortiert oder zwischenabgestellt werden.

1.18 Hafenleitungsorgan (nur Güterverkehr)

eine Anlage oder ein System zur Koordinierung des Hafenverkehrs, zur Verwaltung des Hafenverkehrs oder zur Koordinierung oder zur Überwachung der Tätigkeiten der Akteure in dem betreffenden Hafen.

1.19 Hafeninformationssystem

eine Anlage oder ein System einer übergreifenden IT-Plattform, welches als Port Community System (PCS), Cargo Community System (CCS) oder Single Submission Portal (SSP) oder der Erfüllung der gesetzlichen Anforderungen an die Hafenanmeldungen nach Artikel 4 der Richtlinie 2010/65/EU des Europäischen Parlaments und des Rates vom 20. Oktober 2010 über Meldeformalitäten für Schiffe beim Einlaufen in und/oder Auslaufen aus Häfen der Mitgliedstaaten und zur Aufhebung der Richtlinie 2002/6/EG (ABl. L 283 vom 29.10.2010, S. 1), die zuletzt durch die Richtlinie (EU) 2019/883 (ABl. L 151 vom 7.6.2019, S. 116) geändert worden ist, dient.

1.20 Verkehrssteuerungs- und Leitsystem

eine Anlage oder ein System zur Verkehrsbeeinflussung im Straßenverkehr einschließlich der in § 1 Absatz 4 Nummer 1, 3 und 4 des Bundesfernstraßengesetzes genannten Einrichtungen, zum Beispiel Verkehrs-, Betriebs- und Tunnelleitzentralen, Entwässerungsanlagen, intelligente Verkehrssysteme und Fachstellen für Informationstechnik und -sicherheit im Straßenbau, sowie der Telekommunikationsnetze der Bundesautobahnen.

1.21 Verkehrssteuerungs- und Leitsystem im kommunalen Straßenverkehr

ein System für die kommunale Steuerung und Überwachung von Lichtsignalanlagen, von Verkehrsbeeinflussungsanlagen sowie von Verkehrswarn- und Informationssystemen.

1.22 Intelligentes Verkehrssystem

ein intelligentes Verkehrssystem im Sinne des § 2 Nummer 1 des Intelligente Verkehrssysteme Gesetz.

1.23 Schienennetz und Stellwerke des öffentlichen Straßenpersonenverkehrs (ÖSPV)

das schienengebundene Netz des ÖSPV im Sinne des § 4 Absatz 1 bis 3 des Personenbeförderungsgesetzes einschließlich der zu diesen Strecken und Haltestellen gehörenden Stellwerke und Beeinflussungsanlagen sowie der Fahrstromversorgung.

1.24 Leitzentrale des ÖSPV

eine Anlage oder ein System zur betreiberseitigen Überwachung und Steuerung des Verkehrs einschließlich Systeme für die Fahrgastsicherheit und Fahrgastinformation, zur Personaldisposition und Fahrzeugdisposition, auch zur Fahrzeugbereitstellung im Betriebshof, sowie der Flottentelematik. Systeme für die Fahrgastsicherheit und Fahrgastinformation sowie zur Personaldisposition und Fahrzeugdis-

position sind nur insoweit erfasst, als deren Störung das Potenzial aufweist, die kritische Dienstleistung erheblich kapazitiv zu beeinträchtigen, oder sie zur Evakuierung im Notfall kritisch sind, insbesondere in unterirdischen Verkehrsanlagen.

1.25 Anlage oder System zur Erbringung operativer Logistikleistungen

eine Anlage oder ein System zur Bereitstellung, Verteilung, Lagerung, Bearbeitung oder zum Transport oder Umschlag von Gütern in den Segmenten Massengut, Ladungsverkehr, Stückgut, Kontraktlogistik sowie See- und Luftfracht.

1.26 IT-System zur Logistiksteuerung oder -verwaltung

ein betreiberseitiges, zentrales IT-System zur Gesamtkoordinierung und -steuerung von Logistikdienstleistungen in den Segmenten Massengut, Ladungsverkehr, Stückgut, Kontraktlogistik sowie See- und Luftfracht.

1.27 Anlage zur Wettervorhersage, zur Gezeitenvorhersage oder zur Wasserstandsmeldung

eine Anlage oder ein System zur Erbringung von Wettervorhersagen, insbesondere im Kürzestfristbereich (bis zu 12 Stunden), sowie zur Messung von Gezeiten- und Wasserstand (Pegelstation).

1.28 Bodenstation eines europäischen Satellitennavigationssystems

eine Bodenstation im Sinne des Artikels 28 der Verordnung (EU) Nr. 1285/2013 des Europäischen Parlaments und des Rates vom 11. Dezember 2013 betreffend den Aufbau und den Betrieb der europäischen Satellitennavigationssysteme und zur Aufhebung der Verordnung (EG) Nr. 876/2002 des Rates und der Verordnung (EG) Nr. 683/2008 des Europäischen Parlaments und des Rates (ABl. L 347 vom 20.12.2013, S. 1).

2. Eine Anlage, die einer in Teil 3 Spalte B genannten Anlagenkategorie zuzuordnen ist, gilt ab dem 1. April des Kalenderjahres, das auf das Kalenderjahr folgt, in dem ihr Versorgungsgrad den in Teil 3 Spalte D genannten Schwellenwert erstmals erreicht oder überschreitet, als Kritische Infrastruktur. Nicht mehr als Kritische Infrastruktur gilt eine solche Anlage ab dem 1. April des Kalenderjahres, das auf das Kalenderjahr folgt, in dem ihr Versorgungsgrad den genannten Schwellenwert unterschreitet.

3. Der Betreiber hat den Versorgungsgrad seiner Anlage für das zurückliegende Kalenderjahr jeweils bis zum 31. März des Folgejahres zu ermitteln.

4. Stehen mehrere Anlagen derselben Art in einem engen räumlichen und betrieblichen Zusammenhang (gemeinsame Anlage) und erreichen oder überschreiten die in Teil 3 Spalte D genannten Schwellenwerte zusammen, gilt die gemeinsame Anlage als Kritische Infrastruktur. Ein enger räumlicher und betrieblicher Zusammenhang ist gegeben, wenn die Anlagen

   a) auf demselben Betriebsgelände liegen,

   b) mit gemeinsamen Betriebseinrichtungen verbunden sind,

   c) einem vergleichbaren technischen Zweck dienen und

   d) unter gemeinsamer Leitung stehen.

Teil 2
Berechnungsformeln zur Ermittlung der Schwellenwerte

5. Der für die Anlagenkategorie des Teils 3 Nummer 1.1.4 genannte Schwellenwert ist unter Annahme von durchschnittlich 0,035 Flugbewegungen zur Versorgung einer Person pro Jahr und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

17 500 Flugbewegungen/Jahr = 0,035 Flugbewegungen/Jahr x 500 000

6. Der für die Anlagenkategorien des Teils 3 Nummer 1.2.2 und 1.2.3 genannte Schwellenwert ist unter Annahme einer durchschnittlichen disponierten Transportleistung im Schienengüterverkehr von 1 460 Tonnenkilometern zur Versorgung einer Person, eines Regelschwellenwertes von 500 000 versorgten Personen sowie einer durchschnittlichen Transportleistung von 32 000 Tonnenkilometern pro Güterzug pro Jahr wie folgt berechnet:

23 000 Züge/Jahr ≈ (1 460 tkm/Jahr x 500 000) / (32 000 tkm/Zug)

7. Der für die Anlagenkategorie des Teils 3 Nummer 1.2.6 genannte Schwellenwert ist unter Annahme einer durchschnittlichen disponierten Transportleistung im Güterschienenverkehr von 1 460 Tonnenkilometern zur Versorgung einer Person pro Jahr und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

730 000 000 tkm/Jahr = 1 460 tkm/Jahr x 500 000

8. Der für die Anlagenkategorie des Teils 3 Nummer 1.3.5 genannte Schwellenwert ist unter Annahme einer durchschnittlichen Gesamttransportmenge der Binnenschifffahrt von 223 000 000 Tonnen und einer durchschnittlichen Güterumschlagsmenge in deutschen Seehäfen von 300 000 000 Tonnen für einen Regelschwellenwert von 500 000 versorgten Personen bei einer Gesamtbevölkerung von 80 000 000 wie folgt berechnet:

3 270 000 t/Jahr ≈ (223 000 000 t/Jahr + 300 000 000 t/Jahr) / (80 000 000/500 000)

9. Der für die Anlagenkategorie des Teils 3 Nummer 1.3.6 genannte Schwellenwert ist unter Annahme einer durchschnittlichen Frachtmenge der Seeschifffahrtsflotte von 3,75 Tonnen zur Versorgung einer Person pro Jahr und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

1 875 000 t/Jahr = 3,75 t/Jahr x 500 000

10. Der für die Anlagenkategorie des Teils 3 Nummer 1.3.7 genannte Schwellenwert ist unter Annahme einer durchschnittlichen Transportleistung der durch die Binnenschifffahrtsflotte transportierten Fracht von 691 Tonnenkilometern zur Versorgung einer Person pro Jahr und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

345 500 000 tkm/Jahr = 691 tkm/Jahr x 500 000

11. Der für die Anlagenkategorien des Teils 3 Nummer 1.6.1 und 1.6.2 genannte Schwellenwert ist unter Annahme einer durchschnittlichen Gütermenge im Straßenverkehr von 35,1 Tonnen pro Jahr zur Versorgung einer Person und eines Regelschwellenwertes von 500 000 versorgten Personen wie folgt berechnet:

17 550 000 t/Jahr = 35,1 t/Jahr x 500 000

Das ermittelte Gewicht von 17 550 000 Tonnen pro Jahr entspricht unter Annahme eines durchschnittlichen Gewichts einer Stückgutsendung von 330 Kilogramm der Anzahl von 53 200 000 Sendungen pro Jahr:

53 200 000 Sendungen/Jahr ≈ (17 550 000 t/Jahr) / (0,33t/Sendung)

Teil 3
Anlagenkategorien und Schwellenwerte

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
1	**Personen- und Güterverkehr**		
1.1	Luftverkehr		
1.1.1	Anlage oder System zur Passagierabfertigung an Flugplätzen	Anzahl der Passagiere/Jahr	20 000 000
1.1.2	Anlage oder System zur Frachtabfertigung an Flugplätzen	Gütermenge in Tonnen/Jahr	750 000
1.1.3	Infrastrukturbetrieb eines Flugplatzes	Anzahl der Passagiere/Jahr oder	20 000 000
		Gütermenge in Tonnen/Jahr	750 000
1.1.4	Anlage zur Erbringung von Flugsicherungsdiensten	Anzahl der Flugbewegungen/Jahr	17 500
1.1.5	Verkehrszentrale einer Fluggesellschaft	Anzahl der Passagiere/Jahr oder	20 000 000
		Gütermenge in Tonnen/Jahr	750 000
1.1.6	Flughafenleitungsorgan	Anzahl der Passagiere/Jahr oder	20 000 000
		Gütermenge in Tonnen/Jahr	750 000
1.2	Eisenbahnverkehr		
1.2.1	Personenbahnhof der Eisenbahn	Bahnhofskategorie	jeweils höchste Kategorie
1.2.2	Güterbahnhof	Anzahl ausgehender Züge/Jahr	23 000
1.2.3	Zugbildungsbahnhof	Anzahl gebildete Züge/Jahr	23 000
1.2.4	Schienennetz und Stellwerke der Eisenbahn	Einordnung des Schienennetzes nach der Verordnung (EU) Nr. 1315/2013 des Europäischen Parlaments und des Rats vom 11. Dezember 2013 über Leitlinien der Union für den Aufbau eines transeuropäischen Verkehrsnetzes und zur Aufhebung des Beschlusses Nr. 661/2010/EU (ABl. L 348 vom 20.12.2013, S. 1),	Deutscher Teil des Kernnetzes

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
		die zuletzt durch die Delegierte Verordnung (EU) 2019/254 (ABl. L 43 vom 14.2.2019, S. 1) geändert worden ist	
1.2.5	Verkehrssteuerungs- und Leitsystem der Eisenbahn	Einordnung des zu dem System gehörenden Schienennetzes nach der Verordnung (EU) Nr. 1315/2013	Deutscher Teil des Kernnetzes
1.2.6	Leitzentrale der Eisenbahn	Disponierte Transportleistung (Personenverkehr) in Zugkilometer/Jahr pro Netz/Teilnetz oder	8 200 000
		disponierte Transportleistung (Güterverkehr) in Tonnenkilometer/Jahr	730 000 000
1.3	See- und Binnenschifffahrt		
1.3.1	Anlage oder System zum Betrieb von Bundeswasserstraßen	Güterverkehrsdichte in Tonnen	17 000 000
1.3.2	Verkehrssteuerungs- und Leitsystem der See- und Binnenschifffahrt	Güterverkehrsdichte in Tonnen	17 000 000
1.3.3	Hafenleitungsorgan (nur Güterverkehr)	Gesamtmenge der bereitgestellten, verteilten, gelagerten oder umgeschlagenen Güter im Zuständigkeitsbereich des Hafens in Tonnen/Jahr	50 000 000
1.3.4	Hafeninformationssystem	Gesamtmenge der bereitgestellten, verteilten, gelagerten oder umgeschlagenen Güter im Zuständigkeitsbereich des Hafens, in dem die Anlage oder das System eingesetzt wird, in Tonnen/Jahr	50 000 000
1.3.5	Umschlaganlage in See- und Binnenhäfen	Abgefertigte Fracht in Tonnen/Jahr	3 270 000
1.3.6	Leitzentrale von Betreibern und Verkehrsunternehmen der Seeschifffahrt	Disponierte Frachtmenge der Seeschiffe des Betreibers einschließlich gecharterter Schiffe in Tonnen/Jahr	1 875 000
1.3.7	Leitzentrale von Betreibern und Verkehrsunternehmen der Binnenschifffahrt (nur Güterverkehr)	Disponierte Transportleistung der Binnenschiffe des Betreibers einschließlich gecharterter Schiffe in Tonnenkilometer/Jahr	345 500 000
1.4	Straßenverkehr		

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
1.4.1	Verkehrssteuerungs- und Leitsystem	Art der zu dem Verkehrssteuerungs- und Leitsystem gehörenden Bundesfernstraßen	Bundesautobahn
1.4.2	Verkehrssteuerungs- und Leitsystem im kommunalen Straßenverkehr	Anzahl Einwohner der versorgten Stadt	500 000
1.4.3	Intelligentes Verkehrssystem	Anzahl angeschlossener Nutzer oder durchschnittlich im Versorgungsgebiet versorgter Nutzer	500 000
1.5	ÖPNV		
1.5.1	Schienennetz und Stellwerke des öffentlichen Straßenpersonenverkehrs (ÖSPV)	Anzahl unternehmensbezogene Fahrgastfahrten/Jahr	125 000 000
1.5.2	Leitzentrale des ÖSPV	Anzahl unternehmensbezogene Fahrgastfahrten/Jahr	125 000 000
1.6	Logistik		
1.6.1	Anlage oder System zum Betrieb eines Logistikzentrums in den Segmenten Massengut-, Ladungs-, Stückgut-, Kontrakt-, See- oder Luftfrachtlogistik	Transportmengen im Im- und Export, sowie im Binnenverkehr in Tonnen/Jahr, soweit diese im Unternehmen erfasst werden, im Übrigen	17 550 000
		Anzahl der Sendungen pro Jahr	53 200 000
1.6.2	Anlage oder IT-System zur Logistiksteuerung oder -verwaltung in den Segmenten Massengut, Ladungsverkehr, Stückgut, Kontraktlogistik sowie See- und Luftfracht	Gesamtmenge bereitgestellte, verteilte, gelagerte, bearbeitete oder umgeschlagene Transporte im Im- und Export, sowie im Binnenverkehr in Tonnen/Jahr, soweit diese im Unternehmen erfasst werden, im Übrigen	17 550 000
		Anzahl der Sendungen pro Jahr	53 200 000
1.7	Verkehrsträgerübergreifende Anlagen		
1.7.1	Anlage zur Wettervorhersage, zur Gezeitenvorhersage oder zur Wasserstandsvorhersage	Einsatz der Anlage zur Erbringung von Wettervorhersagen insbesondere im Kürzestfristbereich (bis zu 12 Stunden) zur Erfüllung der gesetzlichen Aufgaben nach § 4 Absatz 1 des Gesetzes über den Deutschen Wetterdienst oder	zur Aufgabenerfüllung eingesetzte Anlage
		Einsatz der Anlage zur Erfüllung der gesetzlichen Aufgaben nach § 1 Nummer 9 des	zur Aufgabenerfüllung eingesetzte Anlage

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
		Seeaufgabengesetzes	
1.7.2	Bodenstation eines Satellitennavigationssystems	Einordnung der Anlage nach der Verordnung (EU) Nr. 1285/2013	Bodenstationen

Anhang 8 (zu § 1 Nummer 4 und 5, § 9 Absatz 3 Nummer 1 und 2)
Anlagenkategorien und Schwellenwerte im Sektor Siedlungsabfallentsorgung

Teil 1
Grundsätze und Fristen

1. Im Sinne von Anhang 8 ist oder sind

1.1 Anlage zur Disposition der Siedlungsabfallsammlung oder -beförderung

eine Anlage zur Planung, Steuerung, Optimierung und Durchführung der Sammlung oder Beförderung von Siedlungsabfällen, zum Beispiel Dispositionssysteme, Flottenmanagement- oder Enterprise Resource Planning-Systeme (ERP-Systeme).

1.2 Anlage zur Lagerung, Zwischenlagerung und Umladung von Siedlungsabfällen

eine Anlage zur Planung, Steuerung, Optimierung und Durchführung der Lagerung, Zwischenlagerung und Umladung von Siedlungsabfällen zum Zweck des Weitertransports, zum Beispiel Zwischenlager oder Umladestationen.

1.3 Anlage zur thermischen Behandlung von Siedlungsabfällen

eine Anlage zur Verbrennung von Siedlungsabfällen, zum Beispiel Müllverbrennungsanlagen (MVA) oder Ersatzbrennstoffkraftwerke (EBS-Kraftwerke).

1.4 Anlage zur mechanisch-biologischen oder mechanisch-physikalischen Behandlung von Siedlungsabfällen

eine Anlage zur Trennung, Sortierung, Zerkleinerung, Pressung, aeroben oder anaeroben Behandlung von Siedlungsabfällen, zum Beispiel mechanisch-biologische Abfallbehandlungsanlagen (MBA), mechanisch-biologische Stabilisierungsanlagen (MBS) oder mechanisch-physikalische Abfallbehandlungsanlagen (MPS).

1.5 Anlage zur biologischen Behandlung von Siedlungsabfällen

eine Anlage zum hygienisierenden oder biologisch-stabilisierenden Behandeln von getrennt erfassten Bioabfällen, zum Beispiel Kompostierungs- und Vergärungsanlagen.

1.6 Anlage zur mechanischen Behandlung von Siedlungsabfällen

eine Anlage zur Zerkleinerung, Klassierung, Sortierung, Pressung und Palettierung von Siedlungsabfällen.

1.7 Anlage zur Sortierung von Siedlungsabfällen

eine Anlage zur Trennung und Sortierung von Siedlungsabfällen, zum Beispiel Sortieranlagen.

2. Eine Anlage, die einer in Teil 3 Spalte B genannten Anlagenkategorie zuzuordnen ist, gilt ab dem 1. April des Kalenderjahres, das auf das Kalenderjahr folgt, in dem ihr Versorgungsgrad den in Teil 3 Spalte D genannten Schwellenwert erstmals erreicht oder überschreitet, als Kritische Infrastruktur. Nicht mehr als Kritische Infrastruktur gilt eine solche Anlage ab dem 1. April des Kalenderjahres, das auf das Kalenderjahr folgt, in dem ihr Versorgungsgrad den genannten Schwellenwert unterschreitet.

3. Der Betreiber hat den Versorgungsgrad seiner Anlage für das zurückliegende Kalenderjahr jeweils bis zum 31. März des Folgejahres zu ermitteln.

4. Stehen mehrere Anlagen derselben Art in einem engen räumlichen und betrieblichen Zusammenhang (gemeinsame Anlage) und erreichen oder überschreiten die in Teil 3 Spalte D genannten Schwellenwerte zusammen, gilt die gemeinsame Anlage als Kritische Infrastruktur. Ein enger räumlicher und betrieblicher Zusammenhang ist gegeben, wenn die Anlagen

   a) auf demselben Betriebsgelände liegen,

   b) mit gemeinsamen Betriebseinrichtungen verbunden sind,

   c) einem vergleichbaren technischen Zweck dienen und

   d) unter gemeinsamer Leitung stehen.

Teil 2
Berechnungsformen zur Ermittlung der Schwellenwerte

5. Der für die Anlagekategorien des Teils 3 genannte Schwellenwert (Rest- oder gemischter Gewerbeabfall) ist unter Annahme eines durchschnittlichen Abfallaufkommens von 159 kg Rest- oder Hausmüll sowie hausmüllähnliche Gewerbeabfälle, in Bezug auf übliche Restmülltonnen, einer Person pro Jahr wie folgt berechnet:

$$79\,500\ \text{Mg} = 159\ \text{kg} \times 500\,000$$

6. Der für die Anlagekategorien des Teils 3 genannte Schwellenwert (Bioabfall) ist unter Annahme eines durchschnittlichen Abfallaufkommens von 67 kg Abfälle aus der Biotonne einer Person pro Jahr wie folgt berechnet:

$$33\,500\ \text{Mg} = 67\ \text{kg} \times 500\,000$$

7. Der für die Anlagekategorien des Teils 3 genannte Schwellenwert (LVP- und Kunststoffabfall) ist unter Annahme eines durchschnittlichen Abfallaufkommens von 35 kg Leichtverpackungen und 2 kg Kunststoff (Gesamtmenge: 37 kg) einer Person pro Jahr wie folgt berechnet:

$$18\,500\ \text{Mg} = 37\ \text{kg} \times 500\,000$$

8. Der für die Anlagekategorien des Teils 3 genannte Schwellenwert (PPK-Abfall) ist unter Annahme eines durchschnittlichen Abfallaufkommens von 65 kg Papier, Pappe und Karton einer Person pro Jahr wie folgt berechnet:

$$32\,500\ \text{Mg} = 65\ \text{kg} \times 500\,000$$

9. Der für die Anlagekategorien des Teils 3 genannte Schwellenwert (Glasabfall) ist unter Annahme eines durchschnittlichen Abfallaufkommens von 24 kg Glas einer Person pro Jahr wie folgt berechnet:

12 000 Mg = 24 kg x 500 000

Teil 3
Anlagekategorien und Schwellenwerte

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
1.	**Sammlung und Beförderung**		
1.1	Anlage zur Disposition der Siedlungsabfallsammlung oder -beförderung	Anzahl Einwohner, die an die Abfallsammlung angeschlossen sind, oder	500 000
		gesammelter oder beförderter Rest- oder gemischter Gewerbeabfall in Mg/Jahr oder	79 500
		gesammelter oder beförderter Bioabfall in Mg/Jahr oder	33 500
		gesammelter oder beförderter LVP- und Kunststoffabfall in Mg/Jahr oder	18 500
		gesammelter PPK-Abfall in Mg/Jahr oder	32 500
		gesammelter Glasabfall in Mg/Jahr	12 000
1.2	Anlage zur Lagerung, Zwischenlagerung und Umladung von Siedlungsabfällen	Zugang an Rest- oder gemischtem Gewerbeabfall in Mg/Jahr oder	79 500
		Zugang an Bioabfall in Mg/Jahr oder	33 500
		Zugang an LVP- und Kunststoffabfall in Mg/Jahr	18 500
2.	**Verwertung und Beseitigung**		
2.1	Anlage zur thermischen Behandlung von Siedlungsabfällen	Genehmigte Behandlungskapazität von Rest- oder gemischtem Gewerbeabfall in Mg/Jahr	79 500
2.2	Anlage zur mechanisch-biologischen	Genehmigte	79 500

Spalte A	Spalte B	Spalte C	Spalte D
Nr.	Anlagenkategorie	Bemessungskriterium	Schwellenwert
	oder mechanisch-physikalischen Behandlung von Siedlungsabfällen	Behandlungskapazität von Rest- oder gemischtem Gewerbeabfall in Mg/Jahr	
2.3	Anlage zur biologischen Behandlung von Siedlungsabfällen	Genehmigte Behandlungskapazität von Bioabfall in Mg/Jahr	33 500
2.4	Anlage zur mechanischen Behandlung von Siedlungsabfällen	Genehmigte Behandlungskapazität von Rest- oder gemischtem Gewerbeabfall in Mg/Jahr	79 500
2.5	Anlage zur Sortierung von Siedlungsabfällen	Genehmigte Behandlungskapazität von Rest- oder gemischtem Gewerbeabfall in Mg/Jahr oder	79 500
		genehmigte Behandlungskapazität von LVP- und Kunststoffabfall in Mg/Jahr	18 500

Verordnung über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI-Zertifizierungs- und -Anerkennungsverordnung – BSIZertV)

Eingangsformel

Auf Grund des § 10 Absatz 1 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821) verordnet das Bundesministerium des Innern nach Anhörung der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie:

Abschnitt 1
Allgemeine Bestimmungen

§ 1 Anwendungsbereich

Das Bundesamt für Sicherheit in der Informationstechnik (Bundesamt) erteilt Zertifikate und Anerkennungen gemäß § 9 des BSI-Gesetzes nach dieser Verordnung.

§ 2 Antragsverfahren

Anträge müssen schriftlich eingereicht werden und den Namen und die Anschrift des Antragstellers sowie das Datum des Antrags enthalten.

§ 3 Vorlage und Aufbewahrung von Unterlagen und sonstigen Beweismitteln

(1) Der Antrag, die mit dem Antrag eingereichten Unterlagen und die im Zertifizierungs- oder Anerkennungsverfahren anfallenden Unterlagen werden beim Bundesamt elektronisch oder in Papierform gemäß den geltenden Bestimmungen aufbewahrt.

(2) Soweit der Antragsteller nach dieser Verordnung dazu berechtigt ist, dem Bundesamt Unterlagen oder sonstige Beweismittel nur zeitweise zur Verfügung zu stellen, hat er diese Unterlagen oder sonstigen Beweismittel nach der Inaugenscheinnahme durch das Bundesamt beim Antragsteller während des Antragsverfahrens und des Gültigkeitszeitraums der Zertifizierung oder der Anerkennung aufzubewahren. Nach Ablauf der Geltungsdauer der Zertifizierung oder der Anerkennung sind diese Unterlagen oder sonstigen Beweismittel für mindestens drei weitere Jahre aufzubewahren und dem Bundesamt jederzeit auf Anfrage kostenfrei zur Verfügung zu stellen.

§ 4 Prüfkriterien, Anforderungen, sachliche Geltungsbereiche

(1) Das Bundesamt bestimmt, soweit erforderlich, für Zertifizierungs- und Anerkennungsverfahren nach dieser Verordnung

1. technische Geltungsbereiche,
2. bedarfsgerechte Prüfkriterien (Sicherheitskriterien, Schutzprofile, Technische Richtlinien und BSI-Standards),
3. Anforderungen an die Fachkunde, Ausstattung und Zuverlässigkeit und

4. notwendige Nachweise

und veröffentlicht diese auf seiner Internetseite.

(2) Das Bundesamt bestimmt das Verfahren zur Erteilung von Zertifikaten und Anerkennungen nach dieser Verordnung und veröffentlicht hierzu Verfahrensbeschreibungen auf seiner Internetseite.

(3) Das Bundesamt sieht von der Veröffentlichung nach den Absätzen 1 und 2 ab, wenn durch die Veröffentlichung die öffentliche Sicherheit gefährdet würde. Das Bundesamt kann von der Veröffentlichung absehen, wenn durch die Veröffentlichung öffentliche Interessen oder die Sicherheit bestimmter Produkte, Komponenten, Produktkategorien oder Systeme beeinträchtigt würden oder die Prüfkriterien oder Verfahrensbeschreibungen als Verschlusssache eingestuft sind. Das Bundesamt gibt nicht veröffentlichte Prüfkriterien, Geltungsbereiche und Verfahrensbeschreibungen denjenigen, die als Antragsteller in Betracht kommen, bekannt, wenn diese gegenüber dem Bundesamt ein berechtigtes Interesse nachweisen und sich verpflichten, die notwendigen Sicherheitsvorkehrungen einzuhalten.

§ 5 Form der Entscheidungen; Anhörungspflicht

(1) Entscheidungen, mit denen abschließend über einen nach dieser Verordnung gestellten Antrag entschieden wird, sind schriftlich oder elektronisch zu erlassen.

(2) Vor der Ablehnung eines Antrags sind dem Antragsteller die Gründe der voraussichtlichen Ablehnung mitzuteilen. Innerhalb einer vom Bundesamt festgesetzten angemessenen Frist ist dem Antragsteller Gelegenheit zur Äußerung und zur Nachbesserung zu geben. § 28 Absatz 3 des Verwaltungsverfahrensgesetzes ist anzuwenden.

(3) Vor Erteilung eines Zertifikats oder einer Anerkennung mit Nebenbestimmungen nach § 22 ist der Antragsteller nach § 28 des Verwaltungsverfahrensgesetzes anzuhören.

§ 6 Mitwirkungsobliegenheit des Antragstellers

(1) Das Bundesamt stellt die Tatsachen fest, die notwendig sind, um den für die Zertifizierung oder Anerkennung relevanten Sachverhalt zu ermitteln. Es obliegt dem Antragsteller, die notwendigen Beweismittel zur Ermittlung des Sachverhaltes beizubringen. Das Bundesamt ist nicht verpflichtet, eigene Ermittlungen im Sinne des § 26 Absatz 1 des Verwaltungsverfahrensgesetzes anzustellen, kann aber auf ihm bereits vorliegende Erkenntnisse zurückgreifen.

(2) Dem Antragsteller obliegt es, im Rahmen seiner Mitwirkungsobliegenheiten die notwendige Mitwirkung etwaiger Dritter sicherzustellen.

§ 7 Veröffentlichung von Zertifikaten und Anerkennungen

(1) Das Bundesamt veröffentlicht mindestens vierteljährlich im Internet oder in anderen Medien Gesamtlisten oder seit der letzten Veröffentlichung geänderte oder hinzugefügte Listeneinträge der zertifizierten informationstechnischen Systeme, Standorte, Produkte, Komponenten und Schutzprofile sowie die zugehörigen Sicherheitszertifikate und Zertifizierungsreporte.

(2) Das Bundesamt veröffentlicht mindestens vierteljährlich im Internet oder in anderen Medien Gesamtlisten oder seit der letzten Veröffentlichung geänderte oder hinzugefügte

Listeneinträge der zertifizierten Personen mit deren Adresse, mit den technischen Geltungsbereichen der Zertifizierung und mit der Geltungsdauer der Zertifizierung.

(3) Das Bundesamt veröffentlicht mindestens vierteljährlich im Internet oder in anderen Medien Gesamtlisten oder seit der letzten Veröffentlichung geänderte oder hinzugefügte Listeneinträge der zertifizierten IT-Sicherheitsdienstleister mit deren Adresse, mit den technischen Geltungsbereichen der Zertifizierung und mit der Geltungsdauer der Zertifizierung.

(4) Das Bundesamt veröffentlicht mindestens vierteljährlich im Internet oder in anderen Medien Gesamtlisten oder seit der letzten Veröffentlichung geänderte oder hinzugefügte Listeneinträge der anerkannten sachverständigen Stellen mit deren Adresse, mit den technischen Geltungsbereichen der Anerkennung und mit der Geltungsdauer der Anerkennung.

(5) Der Inhaber eines Zertifikats oder einer Anerkennung kann der Veröffentlichung nach den Absätzen 1 bis 4 widersprechen. Das Bundesamt sieht von der Veröffentlichung nach den Absätzen 1 bis 4 ab, soweit durch die Veröffentlichung die öffentliche Sicherheit beeinträchtigt werden könnte. Das Bundesamt kann von der Veröffentlichung nach den Absätzen 1 bis 4 ganz oder teilweise absehen, wenn durch die Veröffentlichung öffentliche oder private Interessen beeinträchtigt würden.

Abschnitt 2
Zertifizierung von informationstechnischen Produkten oder Komponenten, informationstechnischen Systemen sowie Schutzprofilen

§ 8 Zertifizierung von informationstechnischen Produkten oder Komponenten

(1) Ein Antrag auf Zertifizierung von informationstechnischen Produkten oder Komponenten kann von einer natürlichen oder juristischen Person gestellt werden. Ist der Antragsteller nicht Hersteller des zu zertifizierenden Produkts oder der zu zertifizierenden Komponente oder von Teilen davon, so muss der Antragsteller dem Antrag eine Erklärung aller Hersteller des zu zertifizierenden Produkts oder der zu zertifizierenden Komponente beifügen, in der die Hersteller ihr Einverständnis mit dem Antrag erklären sowie ihre Bereitschaft zur Mitwirkung und ihr Einverständnis, den Antragsteller bei der Erfüllung von Auflagen oder sonstigen Nebenbestimmungen im Antragsverfahren und nach der Erteilung des Zertifikats zu unterstützen. § 13 Absatz 2 des Verwaltungsverfahrensgesetzes bleibt unberührt.

(2) Der Antrag muss neben den nach § 2 erforderlichen Angaben Folgendes enthalten:

1. Angaben über die nach § 4 Absatz 1 anzuwendenden Prüfkriterien und die angestrebte Bewertungsstufe,
2. die genaue Bezeichnung des zu zertifizierenden Produkts oder der zu zertifizierenden Komponente,
3. Angaben über Hersteller und Rechteinhaber des zu zertifizierenden Produkts oder der zu zertifizierenden Komponente,
4. eine Darstellung des Entwicklungs- und Fertigungsstandes,
5. die Angabe der vom Bundesamt anerkannten sachverständigen Stelle, die für die Prüfung und Bewertung vorgesehen ist,

6. soweit vorhanden, Angaben über bereits erfolgte Prüfungen und Bewertungen durch andere sachverständige Stellen sowie
7. die Zustimmung zur Veröffentlichung einer erteilten Zertifizierung nach § 7 Absatz 1 oder den Widerspruch gegen die Veröffentlichung nach § 7 Absatz 5 Satz 1.

§ 9 Zertifizierung von informationstechnischen Systemen

(1) Ein Antrag auf Zertifizierung von informationstechnischen Systemen kann nur von dem Betreiber des zu zertifizierenden Systems gestellt werden.

(2) Der Antrag muss neben den nach § 2 erforderlichen Angaben Folgendes enthalten:

1. Angaben zu den nach § 4 Absatz 1 anzuwendenden Prüfkriterien und die angestrebte Bewertungsstufe,
2. die genaue Bezeichnung des zu zertifizierenden Systems,
3. eine Darstellung des Entwicklungs- und Fertigungsstandes sowie Angaben über Hersteller und Rechteinhaber der verwendeten informationstechnischen Produkte,
4. die Angabe der vom Bundesamt anerkannten sachverständigen Stelle, die für die Prüfung und Bewertung vorgesehen ist,
5. soweit vorhanden, Angaben über Prüfungen und Bewertungen durch andere Personen oder sachverständige Stellen sowie
6. die Zustimmung zur Veröffentlichung einer erteilten Zertifizierung nach § 7 Absatz 1 oder den Widerspruch gegen die Veröffentlichung nach § 7 Absatz 5 Satz 1.

§ 10 Zertifizierung von Schutzprofilen

(1) Ein Antrag auf Zertifizierung von Schutzprofilen kann nur von einer Vereinigung von Herstellern oder Anwendern von informationstechnischen Produkten, von einer Standardisierungsorganisation oder von einer Behörde gestellt werden.

(2) Der Antrag muss neben den nach § 2 erforderlichen Angaben Folgendes enthalten:

1. Angaben zu den nach § 4 Absatz 1 anzuwendenden Prüfkriterien und die angestrebte Bewertungsstufe,
2. die genaue Bezeichnung des zu zertifizierenden Schutzprofils,
3. soweit vorhanden, Angaben über den Autor des Schutzprofils, falls Autor und Antragsteller nicht identisch sind,
4. die Einwilligung des Antragstellers und Rechteinhabers, das Schutzprofil kostenfrei bereitzustellen,
5. die Angabe der vom Bundesamt anerkannten sachverständigen Stelle, die für die Prüfung und Bewertung vorgesehen ist, sowie
6. die Zustimmung zur Veröffentlichung einer erteilten Zertifizierung nach § 7 Absatz 1 oder den Widerspruch gegen die Veröffentlichung nach § 7 Absatz 5 Satz 1.

§ 11 Mitwirkungsobliegenheiten

(1) Zur Zertifizierung von informationstechnischen Produkten oder Komponenten obliegt es dem Antragsteller, kostenfrei dem Bundesamt und der sachverständigen Stelle das zu zertifizierende Produkt oder die zu zertifizierende Komponente, die für dessen oder deren Betrieb notwendigen Einrichtungen und Rechte sowie die nach § 4 Absatz 1 erforderlichen Unterlagen und Beweismittel zur Verfügung zu stellen. Unterlagen und sonstige Beweismittel können beim Antragsteller in Augenschein genommen werden, wenn der Antragsteller glaubhaft macht, dass einer Weitergabe der Unterlagen oder Beweismittel wesentliche Interessen des Antragstellers entgegenstehen.

(2) Zur Zertifizierung von informationstechnischen Systemen obliegt es dem Antragsteller, dem Bundesamt und der sachverständigen Stelle kostenfrei Zugang zum installierten informationstechnischen System und zu den relevanten Standorten zu gewähren und die für die Prüfung notwendigen Rechte sowie die nach § 4 Absatz 1 erforderlichen Unterlagen und Nachweise zur Verfügung zu stellen.

(3) Zur Zertifizierung von Schutzprofilen obliegt es dem Antragsteller, dem Bundesamt und der beauftragten sachverständigen Stelle kostenfrei das zu zertifizierende Schutzprofil zur Verfügung zu stellen.

(4) Zur Durchführung des Zertifizierungsverfahrens obliegt es dem Antragsteller, das Bundesamt und die beauftragte sachverständige Stelle kostenfrei durch fachkompetente Vertreter zu unterstützen. Soweit notwendig, obliegt es dem Antragsteller, kostenfrei das mit der Prüfung, Bewertung und Zertifizierung befasste Personal produkt-, komponenten- oder systembezogen einzuweisen oder Schulungen durchzuführen.

§ 12 Zertifikat

(1) Ein Zertifikat nach § 9 Absatz 4 des BSI-Gesetzes wird erteilt, wenn

1. die Prüfung und die Bewertung ergeben, dass das geprüfte informationstechnische Produkt, die informationstechnische Komponente, das informationstechnische System oder das Schutzprofil die Prüfkriterien nach § 4 Absatz 1 erfüllt, und
2. das Bundesministerium des Innern, für Bau und Heimat nach § 9 Absatz 4 Nummer 2 des BSI-Gesetzes festgestellt hat, dass überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung nicht entgegenstehen.

(2) Das Zertifikat ist vom Bundesamt zu befristen. Das Bundesamt setzt die Geltungsdauer für den jeweiligen technischen Geltungsbereich fest.

(3) Das Zertifikat für informationstechnische Produkte, Systeme, Komponenten sowie für Schutzprofile enthält:

1. die Zertifizierungsnummer,
2. die Angabe der Prüfkriterien, soweit sie bekannt gemacht sind,
3. den Namen der vom Bundesamt anerkannten sachverständigen Stelle, deren Prüfung und Bewertung der Zertifizierung zugrunde gelegt wurde,
4. etwaige Nebenbestimmungen nach § 22,
5. Ausstellungsort und -datum des Sicherheitszertifikats sowie

6. die Geltungsdauer des Sicherheitszertifikats.

Dem Sicherheitszertifikat wird ein Zertifizierungsbericht beigefügt.

(4) Das Zertifikat für informationstechnische Produkte oder Komponenten enthält zusätzlich zu Absatz 3 folgende Angaben:

1. die Bezeichnung, die Beschreibung und die Angabe des Herstellers des geprüften Produkts oder der Komponente,
2. die Angabe der zum geprüften Produkt oder zur Komponente gehörenden Dokumentationen,
3. die Beschreibung der Sicherheitsfunktionen und
4. die erreichte Bewertungsstufe oder den Prüfumfang.

(5) Das Zertifikat für informationstechnische Systeme enthält zusätzlich zu Absatz 3 folgende Angaben:

1. die Bezeichnung und die Beschreibung des geprüften Systems und der relevanten Standorte und
2. soweit erforderlich, die Angabe der zum geprüften System und Standort gehörenden sicherheitsrelevanten Dokumentationen.

(6) Das Zertifikat für Schutzprofile enthält zusätzlich zu Absatz 3 folgende Angaben:

1. die Bezeichnung und die Beschreibung des geprüften Schutzprofils und
2. die erreichte Bewertungsstufe oder den Prüfumfang.

(7) Das Bundesamt kann jederzeit anlassbezogen überprüfen, ob die Voraussetzungen für die Zertifizierung nach Absatz 1 weiterhin vorliegen. Das Bundesamt entwickelt für die Überprüfungen Verfahrensbeschreibungen und veröffentlicht diese auf seiner Internetseite.

§ 13 Rückgabe von informationstechnischen Produkten oder Komponenten

Vom Antragsteller an das Bundesamt übergebene informationstechnische Produkte oder Komponenten werden dem Antragsteller am Ort der Prüfung zurückgegeben. Das Bundesamt kann mit dem Antragsteller vereinbaren, dass das Produkt oder die Komponente beim Bundesamt aufbewahrt wird.

Abschnitt 3
Zertifizierung von Personen

§ 14 Antrag

(1) Ein Antrag auf Zertifizierung einer Person kann nur von der Person gestellt werden, die die Zertifizierung erhalten möchte.

(2) Der Antrag muss neben den nach § 2 erforderlichen Angaben Folgendes enthalten:

1. Angaben über den oder die beantragten technischen Geltungsbereiche,
2. die für diesen technischen Geltungsbereich geforderten Nachweise nach § 4 Absatz 1 und

3. die Zustimmung zur Veröffentlichung einer erteilten Zertifizierung nach § 7 Absatz 2 oder den Widerspruch gegen die Veröffentlichung nach § 7 Absatz 5 Satz 1.

§ 15 Zertifikat

(1) Ein Zertifikat für Personen nach § 9 Absatz 5 des BSI-Gesetzes wird erteilt, wenn

1. die Prüfung und die Bewertung ergeben, dass die zu zertifizierende Person die Prüfkriterien nach § 4 Absatz 1 erfüllt, und
2. das Bundesministerium des Innern, für Bau und Heimat nach § 9 Absatz 4 Nummer 2 des BSI-Gesetzes festgestellt hat, dass überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung nicht entgegenstehen.

(2) Das Zertifikat ist vom Bundesamt zu befristen. Das Bundesamt setzt die Geltungsdauer für den jeweiligen technischen Geltungsbereich fest.

(3) Das Personenzertifikat enthält folgende Angaben:

1. Den Namen und die Adresse der zertifizierten Person,
2. die Zertifizierungsnummer,
3. die Geltungsdauer der Zertifizierung,
4. den technischen Geltungsbereich der Zertifizierung unter Verweis auf die zugrunde gelegten Standardisierungsnormen,
5. die Angabe der Standardisierungsnormen, die der Evaluierung der Person zugrunde lagen,
6. etwaige Nebenbestimmungen nach § 22 sowie
7. Ausstellungsort und -datum des Zertifikats.

(4) Das Bundesamt überprüft regelmäßig, ob die Voraussetzungen für die Zertifizierung nach Absatz 1 weiterhin vorliegen. Daneben kann auch jederzeit eine anlassbezogene Überprüfung stattfinden. Das Bundesamt entwickelt für diese Überprüfungen Verfahrensbeschreibungen und veröffentlicht diese auf seiner Internetseite.

Abschnitt 4
Zertifizierung von IT-Sicherheitsdienstleistern

§ 16 Antrag

(1) Ein Antrag auf Zertifizierung als IT-Sicherheitsdienstleister kann nur von dem IT-Sicherheitsdienstleister gestellt werden, der die Zertifizierung erhalten möchte.

(2) Der Antrag muss neben den nach § 2 erforderlichen Angaben Folgendes enthalten:

1. Angaben zur Rechtsform, Unternehmensstruktur und zu Beteiligungen des Antragstellers,
2. Angaben über die beantragten sachlichen Geltungsbereiche der Zertifizierung,

3. eine Aufstellung der verantwortlichen Mitarbeiter des Antragstellers und ihres jeweiligen Verantwortungsbereiches,
4. Angaben zum Qualitäts- und Informationssicherheitsmanagement sowie, soweit erforderlich, Angaben zur Geheimschutzbetreuung,
5. die Erklärung zur Unabhängigkeit oder Objektivität bezüglich der vorgesehenen Tätigkeiten im Geltungsbereich und
6. die Zustimmung zur Veröffentlichung einer erteilten Zertifizierung nach § 7 Absatz 3 oder den Widerspruch gegen die Veröffentlichung nach § 7 Absatz 5 Satz 1.

§ 17 Mitwirkungsobliegenheiten

(1) Es obliegt dem Antragsteller, im Rahmen des Verfahrens dem Bundesamt oder den vom Bundesamt beauftragten Personen, soweit erforderlich, kostenfrei Zugang zu den Standorten, zu den zur Prüfung vorgesehenen Systemen und zu den Unterlagen nach § 4 zu gewähren.

(2) Während des Verfahrens obliegt es dem Antragsteller, das Bundesamt oder die vom Bundesamt beauftragten Personen kostenfrei durch fachkompetente Vertreter zu unterstützen.

§ 18 Zertifikat

(1) Ein Zertifikat als IT-Sicherheitsdienstleister nach § 9 Absatz 5 des BSI-Gesetzes wird erteilt, wenn

1. die Prüfung und die Bewertung ergeben, dass der IT-Sicherheitsdienstleister die Prüfkriterien nach § 4 Absatz 1 erfüllt, und
2. das Bundesministerium des Innern, für Bau und Heimat nach § 9 Absatz 4 Nummer 2 des BSI-Gesetzes festgestellt hat, dass überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung nicht entgegenstehen.

(2) Die Zertifizierung ist vom Bundesamt zu befristen. Das Bundesamt setzt die Geltungsdauer für den jeweiligen technischen Geltungsbereich fest.

(3) Das Zertifikat enthält folgende Angaben:

1. Den Namen des IT-Sicherheitsdienstleisters und die Adressen aller zertifizierten Standorte,
2. die Zertifizierungsnummer,
3. die Geltungsdauer der Zertifizierung,
4. den technischen Geltungsbereich oder die technischen Geltungsbereiche der Zertifizierung unter Verweis auf die zugrunde gelegten Standardisierungsnormen,
5. die Angabe der Standardisierungsnormen, die der Begutachtung des IT-Sicherheitsdienstleisters zugrunde lagen,
6. etwaige Nebenbestimmungen nach § 22 sowie
7. Ausstellungsort und -datum des Zertifikats.

(4) Das Bundesamt überprüft regelmäßig, ob die Voraussetzungen für die Zertifizierung nach Absatz 1 weiterhin vorliegen. Daneben kann auch jederzeit eine anlassbezogene Überprüfung stattfinden. Das Bundesamt entwickelt für diese Überprüfungen Verfahrensbeschreibungen und veröffentlicht diese auf seiner Internetseite.

Abschnitt 5
Anerkennung von sachverständigen Stellen

§ 19 Antrag

(1) Ein Antrag auf Anerkennung als sachverständige Stelle kann nur von der Stelle gestellt werden, die die Anerkennung erhalten möchte.

(2) Der Antrag muss neben den nach § 2 erforderlichen Angaben Folgendes enthalten:

1. Angaben zur Rechtsform, Unternehmensstruktur und zu Beteiligungen der Stelle,
2. Angaben über die beantragten technischen Geltungsbereiche der Anerkennung,
3. eine Aufstellung der verantwortlichen Mitarbeiter der Stelle und ihres jeweiligen Verantwortungsbereiches,
4. Angaben zum Qualitäts- und Informationssicherheitsmanagement sowie, soweit vorhanden, Angaben zur Geheimschutzbetreuung,
5. eine Erklärung zur Unabhängigkeit oder Objektivität der Stelle bezüglich der vorgesehenen Tätigkeiten im Geltungsbereich und
6. die Zustimmung zur Veröffentlichung einer ausgesprochenen Anerkennung nach § 7 Absatz 4 oder den Widerspruch gegen die Veröffentlichung nach § 7 Absatz 5 Satz 1.

(3) Die Anträge werden in der zeitlichen Reihenfolge ihres Eingangs bearbeitet; hiervon kann abgewichen werden, wenn das Bundesamt wegen der Zahl und des Umfangs anhängiger Prüfungsverfahren eine Prüfung in angemessener Zeit nicht durchführen kann und an einer Anerkennung ein öffentliches Interesse besteht.

§ 20 Mitwirkungsobliegenheiten

(1) Es obliegt dem Antragsteller, im Rahmen des Verfahrens dem Bundesamt oder den vom Bundesamt beauftragten Personen, soweit erforderlich, kostenfrei Zugang zu den Standorten, zu den zur Prüfung vorgesehenen Systemen und zu den Unterlagen nach § 4 zu gewähren.

(2) Während des Verfahrens obliegt es dem Antragsteller, das Bundesamt oder die vom Bundesamt beauftragten Personen kostenfrei durch fachkompetente Vertreter zu unterstützen.

§ 21 Anerkennung

(1) Eine Anerkennung nach § 9 Absatz 6 des BSI-Gesetzes wird erteilt, wenn

1. die Prüfung und die Bewertung ergeben, dass die sachliche und personelle Ausstattung sowie die fachliche Qualifikation und Zuverlässigkeit der Konformitätsbewertungsstelle die Prüfkriterien nach § 4 Absatz 1 erfüllen, und

2. das Bundesministerium des Innern, für Bau und Heimat nach § 9 Absatz 6 Nummer 2 des BSI-Gesetzes festgestellt hat, dass überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung nicht entgegenstehen.

(2) Die Anerkennung ist vom Bundesamt zu befristen. Das Bundesamt setzt die Geltungsdauer für den jeweiligen technischen Geltungsbereich fest.

(3) Die Anerkennung enthält folgende Angaben:

1. den Name und die Adresse der anerkannten sachverständigen Stelle und aller anerkannten Standorte,
2. die Anerkennungsnummer,
3. die Geltungsdauer der Anerkennung,
4. den technischen Geltungsbereich oder die technischen Geltungsbereiche der Anerkennung unter Verweis auf die zugrunde gelegten Standardisierungsnormen,
5. die Angabe der Standardisierungsnormen, die der Begutachtung der Stelle zugrunde lagen,
6. etwaige Nebenbestimmungen nach § 22 sowie
7. Ausstellungsort und -datum der Anerkennungsurkunde.

(4) Das Bundesamt überprüft regelmäßig nach § 9 Absatz 6 Satz 2 des BSI-Gesetzes, ob die Voraussetzungen für die Anerkennung nach Absatz 1 weiterhin vorliegen. Daneben kann auch jederzeit eine anlassbezogene Überprüfung stattfinden. Das Bundesamt entwickelt für diese Überprüfungen Verfahrensbeschreibungen und veröffentlicht diese auf seiner Internetseite.

Abschnitt 6
Nebenbestimmungen

§ 22 Nebenbestimmungen

(1) Ein Zertifikat nach § 12, § 15 und § 18 sowie eine Anerkennung nach § 21 kann unter dem Vorbehalt des Widerrufs erlassen werden.

(2) Ein Zertifikat nach § 12, § 15 und § 18 sowie eine Anerkennung nach § 21 kann mit Nebenbestimmungen, insbesondere mit Auflagen oder Befristungen, erlassen werden. Insbesondere kann bestimmt werden, dass

1. der Inhaber des Zertifikats oder der Anerkennung bei der Nutzung des Zertifikats oder der Anerkennung, insbesondere bei der Verwendung zu Werbezwecken, Vorlage und Nachweisführung, auf näher bestimmte, in Zusammenhang mit der Zertifizierung oder Anerkennung ausgestellte Begleitdokumente hinweisen und diese zur Verfügung stellen muss,
2. der Inhaber des Zertifikats unaufgefordert das Bundesamt informieren muss, wenn sich die Sicherheitseigenschaften des Zertifizierungsgegenstandes ändern,

3. der Inhaber des Zertifikats oder der Anerkennung regelmäßig oder anlassbezogen auf seine Kosten durch das Bundesamt oder durch von diesem beauftragte Personen oder Stellen überprüfen lassen muss, ob die Voraussetzungen zur Zertifizierung von Produkten (zum Beispiel nach Common Criteria) oder Anerkennung weiterhin vorliegen,
4. eine Zertifizierung von der Gültigkeit eines Schutzprofils oder einer technischen Richtlinie abhängig ist,
5. in den Fällen des § 15, § 18 oder § 21 der Antragsteller dem Bundesamt unverzüglich schriftlich mitteilen muss, wenn sich seine Arbeitsweise oder seine Unternehmensform wesentlich ändert oder sich sein Unternehmenssitz ändert,
6. in den Fällen des § 15, § 18 oder § 21 der Antragsteller an vom Bundesamt angebotenen Arbeitstreffen zum technischen Geltungsbereich der Zertifizierung oder Anerkennung teilnehmen muss,
7. in den Fällen des § 18 oder § 21 der Antragsteller eine bestimmte Zahl von nach § 15 zertifizierten Personen für den jeweiligen Geltungsbereich beschäftigen muss.

Abschnitt 7
Schlussbestimmungen

§ 23 Inkrafttreten, Außerkrafttreten

Diese Verordnung tritt am Tag nach der Verkündung in Kraft. Gleichzeitig tritt die BSI-Zertifizierungsverordnung vom 7. Juli 1992 (BGBl. I S. 1230) außer Kraft.

Verordnung zum IT-Sicherheitskennzeichen des Bundesamtes für Sicherheit in der Informationstechnik (BSI-IT-Sicherheitskennzeichenverordnung - BSI-ITSiKV)

Eingangsformel

Auf Grund des § 10 Absatz 3 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821), der durch Artikel 1 Nummer 21 des Gesetzes vom 18. Mai 2021 (BGBl. I S. 1122) eingefügt worden ist, verordnet das Bundesministerium des Innern, für Bau und Heimat im Einvernehmen mit dem Bundesministerium der Justiz und für Verbraucherschutz und dem Bundesministerium für Wirtschaft und Energie:

§ 1 Anwendungsbereich

Diese Verordnung regelt die Gestaltung und Verwendung des IT-Sicherheitskennzeichens im Sinne des § 9c Absatz 1 Satz 1 des BSI-Gesetzes und legt das Verwaltungsverfahren zur Sicherstellung der Anforderungen im Zusammenhang mit der Verwendung des Kennzeichens fest.

§ 2 Begriffsbestimmungen

Im Sinne dieser Verordnung ist oder sind:

1. Hersteller
   jede juristische oder natürliche Person, die einen Dienst anbietet oder ein Produkt herstellt beziehungsweise entwickeln oder herstellen lässt und dieses Produkt oder diesen Dienst unter ihrem eigenen Namen oder ihrer eigenen Marke vermarktet; nicht erfasst sind die Hersteller einzelner Teile oder Komponenten davon;
2. Verkäufer
   jede juristische oder natürliche Person, die gewerblich ein Produkt unmittelbar Verbrauchern und Verbraucherinnen auf dem Markt bereitstellt;
3. Branche
   die Unternehmen und Organisationen und ihre Verbände, die für den jeweiligen Wirtschaftsbereich Produkte oder Dienstleistungen im Geltungsbereich dieses Gesetzes herstellen oder vertreiben;
4. branchenabgestimmte IT-Sicherheitsvorgabe
   ein Anforderungskatalog, der von einer Branche erstellt und gepflegt wird und dessen Geeignetheit das Bundesamt nach § 9c Absatz 3 Satz 1 des BSI-Gesetzes festgestellt hat;
5. geeignete und qualifizierte Dritte
   juristische oder natürliche Personen, die aufgrund ihrer fachlichen Qualifikation eine Aussage darüber treffen können, ob Sicherheitsversprechen eines Produktes eingehalten werden oder bestimmte Eigenschaften nachgewiesen werden können;
6. Plausibilitätsprüfung
   die Sichtung der Herstellererklärung, der Angaben des Herstellers im Antrag und

eventueller Unterlagen zur Ermittlung, ob die Konformität mit den vom Bundesamt festgelegten Sicherheitsanforderungen plausibel und nachvollziehbar zugesichert wird;

7. Produktkategorie
ein durch das Bundesamt festgelegter Oberbegriff für die Erfassung einer Gruppe von vergleichbaren informationstechnischen Produkten in einem eingrenzbaren Bereich;

8. zugehörige Internetseite
der für das einzelne Produkt angepasste Zielbereich auf der Internetseite des Bundesamtes, auf der Informationen zu diesem Produkt vorgehalten werden;

9. Etikett
die physische oder elektronische Kennzeichnung am Produkt oder seiner Umverpackung, welche produktspezifisch mit dem Verweis auf die zugehörige Internetseite angepasst wird.

§ 3 Gestaltung des Etiketts und der Internetseite zum IT-Sicherheitskennzeichen

(1) Das IT-Sicherheitskennzeichen besteht aus der Herstellererklärung und der Sicherheitsinformation nach § 9c Absatz 2 des BSI-Gesetzes, auf die beide auf dem Etikett verwiesen wird. Das Etikett versetzt den Verbraucher in die Lage, sich ohne erhebliche Hürden mittels gängiger technischer Hilfsmittel über die Art und Aussage der Herstellererklärung gegenüber den Vorgaben des Bundesamtes, die eventuell zur Verfügung stehenden aktuellen Sicherheitsinformationen und die Laufzeit des Kennzeichens zu informieren.

(2) Das Etikett hat dafür jedenfalls zwingend zu umfassen:

1. einen Verweis auf die zugehörige Internetseite des Bundesamtes nach Absatz 4;

2. die Nennung des Bundesamtes.

(3) Das Etikett kann durch das Bundesamt mit einer grafischen Darstellung ausgestaltet werden, um mittels dieser bildlich für den Verbraucher einen sofortigen Wiedererkennungswert zu erzeugen.

(4) Auf der Internetseite des Bundesamtes sind die Herstellererklärung und die Sicherheitsinformation in aktueller Fassung mit der Laufzeit des Kennzeichens abrufbar. Der Hersteller stellt dem Bundesamt hierfür in eigener Verantwortung aktuelle Sicherheitsinformationen zur Konformität des Produktes zur Verfügung, die das Bundesamt auf der zugehörigen Internetseite einstellt. Das Bundesamt kann zudem weitere Informationen über sicherheitsrelevante IT-Eigenschaften und darüber, ob und inwieweit die Herstellererklärung nach derzeitiger Kenntnis eingehalten wird, einstellen.

(5) Das Bundesamt kann eine Applikation zur Verfügung stellen, in der die Informationen zum Herstellerversprechen von Produkten bereitgestellt und abgerufen werden können.

§ 4 Antrag

(1) Ein Antrag auf Freigabe des IT-Sicherheitskennzeichens für ein Produkt kann nur innerhalb der vom Bundesamt nach § 11 bekannt gegebenen Produktkategorien gestellt werden. Der Antrag kann vom Hersteller des Produktes gestellt werden.

(2) Der Antrag ist unter Verwendung der dafür geltenden Vorlage einzureichen, wenn das Bundesamt eine solche veröffentlicht hat. Der Hersteller hat dafür Sorge zu tragen, dass die Erklärung und beigefügten Unterlagen ausschließlich zutreffende Angaben enthalten.

(3) Der Eingang des Antrags wird vom Bundesamt bestätigt. Das Bundesamt teilt dabei die geltende Prüfungsfrist für die Freigabeerklärung nach dieser Verordnung mit.

§ 5 Antragsprüfung

(1) Das Bundesamt führt anhand der eingereichten Unterlagen eine Plausibilitätsprüfung durch. Die Prüfung erfolgt innerhalb der nach § 11 Absatz 1 festgelegten Prüfungsfrist und anhand einer Verfahrensbeschreibung zum Ablauf des Prüfverfahrens, die vom Bundesamt veröffentlicht wird.

(2) Das Bundesamt kann die Überprüfung von Herstellerdokumenten auf qualifizierte Dritte im Sinne des § 2 Nummer 5 übertragen.

(3) Ist für ein Produkt eine geeignete branchenabgestimmte IT-Sicherheitsvorgabe nach § 10 einschlägig, sind für die Plausibilitätsprüfung die Vorgaben dieses Standards ausschlaggebend.

(4) Liegen die gesetzlichen Voraussetzungen gemäß § 9c Absatz 5 BSIG vor, erteilt das Bundesamt die Freigabe zur Nutzung des IT-Sicherheitskennzeichens.

(5) Das Bundesamt kann den Antrag ablehnen, wenn Hinweise dafür vorliegen, dass

1. das Produkt oder die mit dem Produkt ausgelieferte Software bekannte Sicherheitslücken enthält oder
2. Produkte des Herstellers bereits Gegenstand einer Warnung oder Information nach den §§ 7 oder 7a des BSI-Gesetzes oder von Maßnahmen nach § 9c Absatz 8 des BSI-Gesetzes betroffen waren.

Das Bundesamt kann die Freigabe der Nutzung auch dann verweigern, wenn der Freigabe unabhängig von den eingereichten Unterlagen ernstliche Zweifel an der Herstellererklärung entgegenstehen.

(6) Entscheidungen, mit denen abschließend über einen nach dieser Verordnung gestellten Antrag entschieden wird, sind schriftlich oder elektronisch zu erlassen.

§ 6 Vereinfachtes Verfahren

(1) Das Bundesamt kann auf die Plausibilitätsprüfung verzichten, wenn das Bundesamt für das Produkt ein Zertifikat nach § 9 des BSI-Gesetzes auf Grundlage des gleichen Prüfstandards erteilt hat.

(2) Ist für ein Produkt bereits ein ausländisches staatliches Kennzeichen auf Grundlage des gleichen oder eines vergleichbaren Prüfstandards und auf Grundlage der gleichen oder vergleichbarer Prüfspezifikationen vergeben worden, kann das Bundesamt den Antrag unter Vorlage dieses Kennzeichens und der zugrunde liegenden Unterlagen in deutscher oder englischer Sprache prüfen. Das Bundesamt legt in einem Kriterienkatalog fest, unter welchen Voraussetzungen ein Prüfstandard eines anderen Kennzeichens mit solchen nach dieser Verordnung vergleichbar ist und veröffentlicht diesen auf seiner Internetseite.

§ 7 Gegenstand der Herstellererklärung

(1) Die Herstellererklärung enthält die Zusicherung, dass das Produkt für die nach § 8 festgelegte Dauer die für die einschlägige Produktkategorie geltenden IT-Sicherheitsanforderungen erfüllt. Der Hersteller verpflichtet sich innerhalb des Zeitraumes nach § 8 Absatz 1 Satz 1, das Bundesamt unaufgefordert zu informieren, wenn sich die vom Hersteller erklärten Eigenschaften des Produktes ändern, sobald sie ihm bekannt werden, einschließlich Störungen der Informationssicherheit des Produktes und Sicherheitslücken. Der Hersteller verpflichtet sich des Weiteren, ihm bekannt werdende Sicherheitslücken unverzüglich zu beheben und den Stand der dafür erfolgten Maßnahmen dem Bundesamt mit den in § 3 Absatz 4 Satz 2 genannten Informationen anzuzeigen.

(2) Das Bundesamt informiert auf seiner Internetseite über die Änderung oder Aufhebung der für die einschlägige Produktkategorie geltenden IT-Sicherheitsanforderungen, Technischen Richtlinien oder die Ungeeignetheit von branchenabgestimmten IT-Sicherheitsvorgaben.

(3) Bedient sich der Antragsteller zur Antragstellung oder zur Erfüllung seiner Pflichten aus § 9c des BSI-Gesetzes oder dieser Rechtsverordnung eines Dritten, werden ihm die Handlungen des Dritten wie eigene zugerechnet.

§ 8 Laufzeit des IT-Sicherheitskennzeichens und Erlöschen

(1) Der Hersteller versichert, dass die Herstellererklärung für die dafür festgelegte Dauer erfüllt wird (Laufzeit). Die Laufzeit beträgt regelmäßig zwei Jahre. Eine abweichende Laufzeit kann durch das Bundesamt für die Produktkategorie festgelegt oder in der zugrunde gelegten Technischen Richtlinie oder branchenabgestimmten IT-Sicherheitsvorgaben bestimmt werden. Das Bundesamt hat bei abweichenden Laufzeiten diese gemeinsam mit der Produktkategorie zu veröffentlichen.

(2) Mit Ablauf der Laufzeit erlischt die Freigabe des Bundesamtes. Das Bundesamt weist in der BSI-Sicherheitsinformation öffentlich auf den Ablauf der Laufzeit hin.

(3) Für ein Produkt, für das ein gültiges IT-Sicherheitskennzeichen besteht, kann derselbe Hersteller frühestens drei Monate und spätestens sechs Wochen vor Ablauf der Gültigkeit des IT-Sicherheitskennzeichens dessen Verlängerung beantragen. Die für die erstmalige Freigabe geltenden Vorschriften gelten entsprechend.

(4) Wird eine für die einschlägige Produktkategorie geltende IT-Sicherheitsvorgabe geändert oder für ungültig erklärt, erlischt die Freigabe nach einer Frist von sechs Wochen, wenn der Hersteller die Herstellererklärung nicht auf einer gültigen Prüfgrundlage aktualisiert. Das Bundesamt weist auf entsprechende Änderungen, Ungeeignetheit oder Aufhebungen in der Veröffentlichung der Produktkategorie nach § 11 hin.

(5) Bei einem Verstoß gegen die Herstellererklärung, die gesetzlichen Herstellerpflichten, bei unzutreffenden oder unvollständigen Angaben, sowie dem sonstigen Wegfall der Erfüllung der gesetzlichen Voraussetzungen oder Anforderungen des Bundesamtes kann das Bundesamt die Freigabe unverzüglich widerrufen. Dem Antragsteller ist eine angemessene Frist zur Stellungnahme zu geben, es sei denn, gewichtige Sicherheitsgründe erfordern eine sofortige Maßnahme.

§ 9 Verwendung des Sicherheitskennzeichens

(1) Das produktspezifische Etikett darf in physischer und elektronischer Ausführung für die Dauer der Freigabe nach den Vorgaben des § 9c des BSI-Gesetzes und dieser Rechtsverordnung verwendet werden. Das Bundesamt legt die grafische Gestaltung des Sicherheitskennzeichens sowie des Etiketts fest und veröffentlicht diese auf seiner Internetseite. Hersteller dürfen gemäß ihrer Freigabe keine von diesen Vorgaben abweichende Gestaltung verwenden.

(2) Mit der Freigabe stellt das Bundesamt dem Hersteller das produktspezifische Etikett zur Verfügung. Das Etikett darf nach der Freigabe auf Produkten oder deren Umverpackungen vom Hersteller angebracht werden.

(3) Hersteller und Verkäufer sind berechtigt, das Kennzeichen für die Dauer der Freigabe zu Werbezwecken für das Produkt zu verwenden. Dabei ist ein Verweis auf die zugehörige Internetseite nach § 3 Absatz 4 gut sichtbar anzuzeigen.

(4) Liegt keine Freigabe mehr vor, erlöschen die Rechte von Hersteller und Verkäufer nach dieser Vorschrift. Der Hersteller hat dafür Sorge zu tragen, dass keine nach dem Erlöschen hergestellten Produkte mehr mit dem Etikett auf den Markt gebracht werden.

§ 10 Anerkennung von Normen, Standards oder branchenabgestimmten IT-Sicherheitsvorgaben

(1) Das Bundesamt kann von Amts wegen feststellen, dass eine bestehende Norm oder ein Standard geeignet ist, die Anforderungen nach § 5 Absatz 3 zu gewährleisten. Ein Anspruch auf diese Feststellung besteht nicht.

(2) Branchenverbände oder Hersteller können branchenabgestimmte IT-Sicherheitsvorgaben zur Gewährleistung der Anforderungen nach § 5 Absatz 3 vorschlagen. Das Bundesamt stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen nach § 5 Absatz 3 zu gewährleisten. Die Feststellung befristet das Bundesamt entsprechend der zu erwartenden Entwicklungen in der Produktkategorie. Ein Anspruch auf diese Feststellung besteht nicht.

(3) Für eine Norm, einen Standard oder eine branchenabgestimmte IT-Sicherheitsvorgabe, der oder die nicht mehr diesen Anforderungen oder dem Stand der Technik entspricht oder in eine Technische Richtlinie überführt wurde, kann die Feststellung nach Absatz 1 vom Bundesamt vor Ablauf der Frist widerrufen werden.

(4) Wird für eine Produktkategorie mehr als ein Antrag nach Absatz 2 gestellt, so gibt das Bundesamt den Standard mit einer angemessenen Frist zur Einigung an die Vorschlagenden zurück; es kann nach Ablauf dieser Frist ohne Einigung einen der Standards zur Prüfung auswählen.

(5) Ein oder mehrere branchenspezifische Sicherheitsstandards oder eine oder mehrere branchenabgestimmte IT-Sicherheitsvorgaben können vom Bundesamt im Benehmen mit der Branche in eine Technische Richtlinie überführt werden.

§ 11 Produktkategorien

(1) Das Bundesamt legt die Produktkategorien fest, für deren Produkte es die Freigabe des IT-Sicherheitskennzeichens erteilt. Es gibt die Produktkategorie und die regelmäßige Prüfungsfrist für die Antragsbearbeitung durch im Bundesanzeiger veröffentlichte Allgemeinverfügung bekannt, bevor es die für die jeweilige Produktkategorie einschlägigen IT-Sicher-

heitsanforderungen veröffentlicht. Legt das Bundesamt keine Prüfungsfrist für die Produktkategorie fest, gilt eine Prüfungsfrist ab vollständigem Antragseingang von sechs Wochen.

(2) Das Bundesamt kann für die konkreten Sicherheitsanforderungen auf bestehende Vorgaben, Standards, Technische Richtlinien, Prüfgrundlagen oder branchenabgestimmte IT-Sicherheitsvorgaben verweisen und bemüht sich um den Gleichlauf mit international etablierten Standards.

(3) Die Produktkategorien veröffentlicht das Bundesamt nach Bekanntgabe mit den aktuellen Anforderungen und der Prüfungsfrist auf seiner Internetseite. Es weist ebenso auf eventuelle Änderungen, Aufhebungen oder eine Feststellung der Ungeeignetheit der Anforderungen hin.

(4) Änderungen der Produktkategorie, welche die Kategorie wesentlich verändern oder ganz entfernen, bedürfen ebenfalls der Bekanntgabe mit einer im Bundesanzeiger veröffentlichten Allgemeinverfügung.

§ 12 Aufsicht

(1) Eine Aufsicht über Produkte und Hersteller, welche die Freigabe zur Nutzung des Sicherheitskennzeichens erhalten haben, erfolgt für die Dauer der Freigabe. Sie erfolgt anlasslos auf der Grundlage eines Überwachungskonzeptes sowie anlassbezogen reaktiv und kann eine Sachprüfung umfassen.

(2) Ein Marktüberwachungskonzept im Sinne des Absatzes 1 wird vom Bundesamt erarbeitet. Die dortigen Regelungen sollen bei der anlasslosen Marktüberwachung zugrunde gelegt werden.

(3) Zur effektiven Marktaufsicht kann das Bundesamt sich Dritter im Sinne des § 2 Nummer 5 bedienen und Testkäufe vornehmen. Es kann öffentlich bekannt gewordene Sicherheitsinformationen und Berichte von Verbraucherorganisationen zur Grundlage seiner Aufsicht machen.

§ 13 Informationen für Verbraucher

Verbraucherinformationen zu Produkten mit der Freigabe zur Nutzung des IT-Sicherheitskennzeichens werden in der Sicherheitsinformation nach § 9c Absatz 2 des BSI-Gesetzes auf der Internetseite des Bundesamtes veröffentlicht. Davon unberührt bleiben die Bestimmungen der §§ 7 und 7a des BSI-Gesetzes.

§ 14 Evaluierung

Drei Jahre nach Inkrafttreten dieser Rechtsverordnung und folgend alle drei Jahre sind unter Beteiligung der in § 10 Absatz 3 Satz 1 des BSI-Gesetzes genannten Ressorts zu evaluieren:

1. die Produktkategorien;
2. die Anerkennung von Branchenstandards;
3. die Freigabekriterien für das Kennzeichen.

§ 15 Inkrafttreten

Diese Verordnung tritt am Tag nach der Verkündung in Kraft.

Telekommunikationsgesetz (TKG)

§ 165 Technische und organisatorische Schutzmaßnahmen

(1) Wer Telekommunikationsdienste erbringt oder daran mitwirkt, hat angemessene technische Vorkehrungen und sonstige Maßnahmen zu treffen

1. zum Schutz des Fernmeldegeheimnisses und
2. gegen die Verletzung des Schutzes personenbezogener Daten.

Dabei ist der Stand der Technik zu berücksichtigen.

(2) Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat bei den hierfür betriebenen Telekommunikations- und Datenverarbeitungssystemen angemessene technische und organisatorische Vorkehrungen und sonstige Maßnahmen zu treffen

1. zum Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und -diensten führen, auch, sofern diese Störungen durch äußere Angriffe und Einwirkungen von Katastrophen bedingt sein können, und
2. zur Beherrschung der Risiken für die Sicherheit von Telekommunikationsnetzen und -diensten.

Insbesondere sind Maßnahmen, einschließlich gegebenenfalls Maßnahmen in Form von Verschlüsselung, zu treffen, um Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu sichern und Auswirkungen von Sicherheitsverletzungen für Nutzer, andere Telekommunikationsnetze und Dienste so gering wie möglich zu halten. Bei diesen Maßnahmen ist der Stand der Technik zu berücksichtigen.

(3) Als eine angemessene Maßnahme im Sinne des Absatzes 2 können Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher Telekommunikationsdienste Systeme zur Angriffserkennung im Sinne des § 2 Absatz 9b des BSI-Gesetzes einsetzen. Betreiber öffentlicher Telekommunikationsnetze und Anbieter öffentlich zugänglicher Telekommunikationsdienste mit erhöhtem Gefährdungspotenzial haben entsprechende Systeme zur Angriffserkennung einzusetzen. Die eingesetzten Systeme zur Angriffserkennung müssen in der Lage sein, durch kontinuierliche und automatische Erfassung und Auswertung Gefahren oder Bedrohungen zu erkennen. Sie sollen zudem in der Lage sein, erkannte Gefahren oder Bedrohungen abzuwenden und für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen. Weitere Einzelheiten kann die Bundesnetzagentur im Katalog von Sicherheitsanforderungen nach § 167 festlegen.

(4) Kritische Komponenten im Sinne von § 2 Absatz 13 des BSI-Gesetzes dürfen von einem Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial nur eingesetzt werden, wenn sie vor dem erstmaligen Einsatz von einer anerkannten Zertifizierungsstelle überprüft und zertifiziert wurden.

(5) Wer ein öffentliches Telekommunikationsnetz betreibt, hat Maßnahmen zu treffen, um den ordnungsgemäßen Betrieb seiner Netze zu gewährleisten und dadurch die fortlaufende Verfügbarkeit der über diese Netze erbrachten Dienste sicherzustellen.

(6) Technische Vorkehrungen und sonstige Schutzmaßnahmen sind angemessen, wenn der dafür erforderliche technische und wirtschaftliche Aufwand nicht außer Verhältnis zur Bedeutung der zu schützenden Telekommunikationsnetze oder -dienste steht. § 62 Absatz 1 des Bundesdatenschutzgesetzes gilt entsprechend.

(7) Bei gemeinsamer Nutzung eines Standortes oder technischer Einrichtungen hat jeder Beteiligte die Verpflichtungen nach den Absätzen 1 bis 5 zu erfüllen, soweit bestimmte Verpflichtungen nicht einem bestimmten Beteiligten zugeordnet werden können.

(8) Im Falle des Eintritts eines Sicherheitsvorfalls oder der Feststellung einer erheblichen Gefahr kann die Bundesnetzagentur Maßnahmen zur Behebung des Sicherheitsvorfalls oder zur Abwendung der Gefahr und deren Umsetzungsfristen anordnen.

(9) Die Bundesnetzagentur kann anordnen, dass sich die Betreiber öffentlicher Telekommunikationsnetze oder die Anbieter öffentlich zugänglicher Telekommunikationsdienste einer Überprüfung durch eine qualifizierte unabhängige Stelle oder eine zuständige nationale Behörde unterziehen, in der festgestellt wird, ob die Anforderungen nach den Absätzen 1 bis 7 erfüllt sind. Unbeschadet von Satz 1 haben sich Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial alle zwei Jahre einer Überprüfung durch eine qualifizierte unabhängige Stelle oder eine zuständige nationale Behörde zu unterziehen, in der festgestellt wird, ob die Anforderungen nach den Absätzen 1 bis 7 erfüllt sind. Die Bundesnetzagentur legt den Zeitpunkt der erstmaligen Überprüfung fest. Der nach den Sätzen 1 und 2 Verpflichtete hat eine Kopie des Überprüfungsberichts unverzüglich an die Bundesnetzagentur und an das Bundesamt für Sicherheit in der Informationstechnik, sofern dieses die Überprüfung nicht vorgenommen hat, zu übermitteln. Er trägt die Kosten dieser Überprüfung. Die Bewertung der Überprüfung sowie eine diesbezügliche Feststellung von Sicherheitsmängeln im Sicherheitskonzept nach § 166 erfolgt durch die Bundesnetzagentur im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik.

(10) Über aufgedeckte Mängel bei der Erfüllung der Sicherheitsanforderungen in der Informationstechnik sowie die in diesem Zusammenhang von der Bundesnetzagentur geforderten Abhilfemaßnahmen unterrichtet die Bundesnetzagentur unverzüglich das Bundesamt für Sicherheit in der Informationstechnik.

(11) Die Bundesnetzagentur kann zur Unterstützung ein Computer-Notfallteam gemäß Artikel 9 der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19.7.2016, S. 1; L 33 vom 7.2.2018, S. 5) im Rahmen der zugewiesenen Aufgaben in Anspruch nehmen. Die Bundesnetzagentur kann ferner das Bundesamt für Sicherheit in der Informationstechnik, die zuständigen nationalen Strafverfolgungsbehörden und die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit konsultieren.

§ 166 Sicherheitsbeauftragter und Sicherheitskonzept

(1) Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat

1. einen Sicherheitsbeauftragten zu bestimmen,
2. einen in der Europäischen Union ansässigen Ansprechpartner zu benennen und
3. ein Sicherheitskonzept zu erstellen, aus dem hervorgeht,

a) welches öffentliche Telekommunikationsnetz betrieben wird und welche öffentlich zugänglichen Telekommunikationsdienste erbracht werden,

b) von welchen Gefährdungen auszugehen ist und

c) welche technischen Vorkehrungen oder sonstigen Schutzmaßnahmen zur Erfüllung der durch die Vorgaben des Katalogs von Sicherheitsanforderungen nach § 167 konkretisierten Verpflichtungen aus § 165 Absatz 1 bis 7 getroffen oder geplant sind; sofern der Katalog lediglich Sicherheitsziele vorgibt, ist darzulegen, dass mit den ergriffenen Maßnahmen das jeweilige Sicherheitsziel vollumfänglich erreicht wird.

(2) Wer ein öffentliches Telekommunikationsnetz betreibt, hat der Bundesnetzagentur das Sicherheitskonzept unverzüglich nach der Aufnahme des Netzbetriebs vorzulegen. Wer öffentlich zugängliche Telekommunikationsdienste erbringt, kann von der Bundesnetzagentur verpflichtet werden, das Sicherheitskonzept vorzulegen.

(3) Mit dem Sicherheitskonzept ist eine Erklärung vorzulegen, dass die in dem Sicherheitskonzept aufgezeigten technischen Vorkehrungen und sonstigen Schutzmaßnahmen umgesetzt sind oder unverzüglich umgesetzt werden.

(4) Stellt die Bundesnetzagentur im Sicherheitskonzept oder bei dessen Umsetzung Sicherheitsmängel fest, so kann sie die unverzügliche Beseitigung dieser Mängel verlangen. Sofern sich die dem Sicherheitskonzept zugrunde liegenden Gegebenheiten ändern, hat der nach Absatz 2 Verpflichtete das Sicherheitskonzept unverzüglich nach der Änderung anzupassen und der Bundesnetzagentur unverzüglich nach erfolgter Anpassung unter Hinweis auf die Änderungen erneut vorzulegen.

(5) Die Bundesnetzagentur überprüft regelmäßig die Umsetzung des Sicherheitskonzepts. Die Überprüfung soll mindestens alle zwei Jahre erfolgen.

§ 167 Katalog von Sicherheitsanforderungen

(1) Die Bundesnetzagentur legt im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit durch Allgemeinverfügung in einem Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten fest:

1. Einzelheiten der nach § 165 Absatz 1 bis 7 zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen unter Beachtung der verschiedenen Gefährdungspotenziale der öffentlichen Telekommunikationsnetze und öffentlich zugänglichen Telekommunikationsdienste,

2. welche Funktionen kritische Funktionen im Sinne von § 2 Absatz 13 Satz 1 Nummer 3 Buchstabe b des BSI-Gesetzes sind, die von kritischen Komponenten im Sinne von § 2 Absatz 13 des BSI-Gesetzes realisiert werden, und

3. wer als Betreiber öffentlicher Telekommunikationsnetze und als Anbieter öffentlich zugänglicher Telekommunikationsdienste mit erhöhtem Gefährdungspotenzial einzustufen ist.

Der Katalog von Sicherheitsanforderungen nach Satz 1 kann auch Anforderungen zur Offenlegung und Interoperabilität von Schnittstellen von Netzkomponenten einschließlich einzuhaltender technischer Standards enthalten. Die Bundesnetzagentur gibt den Herstel-

lern, den Verbänden der Betreiber öffentlicher Telekommunikationsnetze und den Verbänden der Anbieter öffentlich zugänglicher Telekommunikationsdienste Gelegenheit zur Stellungnahme.

(2) Die Verpflichteten haben die Vorgaben des Katalogs spätestens ein Jahr nach dessen Inkrafttreten zu erfüllen, es sei denn, in dem Katalog ist eine davon abweichende Umsetzungsfrist festgelegt worden.

§ 168 Mitteilung eines Sicherheitsvorfalls

(1) Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat der Bundesnetzagentur und dem Bundesamt für Sicherheit in der Informationstechnik einen Sicherheitsvorfall mit beträchtlichen Auswirkungen auf den Betrieb der Netze oder die Erbringung der Dienste unverzüglich mitzuteilen. § 42 Absatz 4 und § 43 Absatz 4 des Bundesdatenschutzgesetzes gelten entsprechend.

(2) Das Ausmaß der Auswirkungen eines Sicherheitsvorfalls ist – sofern verfügbar – insbesondere anhand folgender Kriterien zu bewerten:

1. die Zahl der von dem Sicherheitsvorfall betroffenen Nutzer,
2. die Dauer des Sicherheitsvorfalls,
3. die geographische Ausdehnung des von dem Sicherheitsvorfall betroffenen Gebiets,
4. das Ausmaß der Beeinträchtigung des Telekommunikationsnetzes oder des Dienstes,
5. das Ausmaß der Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten.

(3) Die Mitteilung nach Absatz 1 Satz 1 muss die folgenden Angaben enthalten:

1. Angaben zu dem Sicherheitsvorfall,
2. Angaben zu den Kriterien nach Absatz 2,
3. Angaben zu den betroffenen Systemen sowie
4. Angaben zu der vermuteten oder tatsächlichen Ursache.

(4) Die Bundesnetzagentur legt Einzelheiten des Mitteilungsverfahrens fest. Die Bundesnetzagentur kann einen detaillierten Bericht über den Sicherheitsvorfall und die ergriffenen Abhilfemaßnahmen verlangen.

(5) Erforderlichenfalls unterrichtet die Bundesnetzagentur die nationalen Regulierungsbehörden der anderen Mitgliedstaaten der Europäischen Union und die Agentur der Europäischen Union für Cybersicherheit über den Sicherheitsvorfall. Die Bundesnetzagentur kann die Öffentlichkeit unterrichten oder die nach Absatz 1 Satz 1 Verpflichteten zu dieser Unterrichtung verpflichten, wenn sie zu dem Schluss gelangt, dass die Bekanntgabe des Sicherheitsvorfalls im öffentlichen Interesse liegt.

(6) Im Falle einer besonderen und erheblichen Gefahr eines Sicherheitsvorfalls informieren die nach Absatz 1 Satz 1 Verpflichteten die von dieser Gefahr potenziell betroffenen Nutzer über alle möglichen Schutz- oder Abhilfemaßnahmen, die von den Nutzern ergriffen wer-

den können sowie gegebenenfalls auch über die Gefahr selbst. § 8e des BSI-Gesetzes gilt entsprechend.

(7) Die Bundesnetzagentur legt der Kommission, der Agentur der Europäischen Union für Cybersicherheit und dem Bundesamt für Sicherheit in der Informationstechnik einmal pro Jahr einen zusammenfassenden Bericht über die eingegangenen Meldungen und die ergriffenen Abhilfemaßnahmen vor.

§ 169 Daten- und Informationssicherheit

(1) Wer öffentlich zugängliche Telekommunikationsdienste erbringt, hat im Falle einer Verletzung des Schutzes personenbezogener Daten unverzüglich die Bundesnetzagentur und die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit von der Verletzung zu benachrichtigen. Ist anzunehmen, dass durch die Verletzung des Schutzes personenbezogener Daten Endnutzer oder andere Personen schwerwiegend in ihren Rechten oder schutzwürdigen Interessen beeinträchtigt werden, hat der Anbieter des Telekommunikationsdienstes zusätzlich die Betroffenen unverzüglich von dieser Verletzung zu benachrichtigen. In Fällen, in denen in dem Sicherheitskonzept nachgewiesen wurde, dass die von der Verletzung betroffenen personenbezogenen Daten durch geeignete technische Vorkehrungen gesichert, insbesondere unter Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens gespeichert wurden, ist eine Benachrichtigung nicht erforderlich. Unabhängig von Satz 3 kann die Bundesnetzagentur den Anbieter des Telekommunikationsdienstes unter Berücksichtigung der wahrscheinlichen nachteiligen Auswirkungen der Verletzung des Schutzes personenbezogener Daten zu einer Benachrichtigung der Betroffenen verpflichten. Im Übrigen gelten § 42 Absatz 4 und § 43 Absatz 4 des Bundesdatenschutzgesetzes entsprechend.

(2) Die Benachrichtigung nach Absatz 1 Satz 1 und 2 muss mindestens enthalten:

1. die Art der Verletzung des Schutzes personenbezogener Daten,
2. Angaben zu den Kontaktstellen, bei denen weitere Informationen erhältlich sind, und
3. Empfehlungen zu Maßnahmen, die mögliche nachteilige Auswirkungen der Verletzung des Schutzes personenbezogener Daten begrenzen.

In der Benachrichtigung an die Bundesnetzagentur und die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit hat der Anbieter des Telekommunikationsdienstes zusätzlich die Folgen der Verletzung des Schutzes personenbezogener Daten und die beabsichtigten oder ergriffenen Maßnahmen darzulegen.

(3) Die Anbieter der Telekommunikationsdienste haben ein Verzeichnis der Verletzungen des Schutzes personenbezogener Daten zu führen, das Angaben zu Folgendem enthält:

1. den Umständen der Verletzungen,
2. den Auswirkungen der Verletzungen und
3. den ergriffenen Abhilfemaßnahmen.

Diese Angaben müssen ausreichend sein, um der Bundesnetzagentur und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit die Prüfung zu ermöglichen, ob die Absätze 1 und 2 eingehalten wurden. Das Verzeichnis enthält nur die zu

diesem Zweck erforderlichen Informationen und muss nicht Verletzungen berücksichtigen, die mehr als fünf Jahre zurückliegen.

(4) Werden dem Anbieter des Telekommunikationsdienstes nach Absatz 1 Satz 1 Störungen bekannt, die von Datenverarbeitungssystemen der Nutzer ausgehen, so hat er die Nutzer, soweit ihm diese bereits bekannt sind, unverzüglich darüber zu benachrichtigen. Soweit technisch möglich und zumutbar, hat er die Nutzer auf angemessene, wirksame und zugängliche technische Mittel hinzuweisen, mit denen sie diese Störungen erkennen und beseitigen können. Der Anbieter des Telekommunikationsdienstes darf die Teile des Datenverkehrs von und zu einem Nutzer, von denen eine Störung ausgeht, umleiten, soweit dies erforderlich ist, um den Nutzer über die Störungen benachrichtigen zu können.

(5) Wird der Anbieter des Telekommunikationsdienstes nach Absatz 1 Satz 1 vom Bundesamt für Sicherheit in der Informationstechnik über konkrete erhebliche Gefahren informiert, die von Datenverarbeitungssystemen der Nutzer ausgehen oder diese betreffen, so hat er die betroffenen Nutzer, soweit ihm diese bekannt sind, unverzüglich darüber zu benachrichtigen. Soweit technisch möglich und zumutbar, hat er die Nutzer auf angemessene, wirksame und zugängliche technische Mittel hinzuweisen, mit denen sie diese Gefahren erkennen und ihnen vorbeugen können. Werden dem Anbieter des Telekommunikationsdienstes nach Absatz 1 Satz 1 Gefahren bekannt, die von Datenverarbeitungssystemen der Nutzer ausgehen oder diese betreffen, so kann er die Nutzer, soweit ihm diese bekannt sind, darüber benachrichtigen. Soweit technisch möglich und zumutbar, kann er die Nutzer auf angemessene, wirksame und zugängliche technische Mittel hinweisen, mit denen sie diese Gefahren erkennen und ihnen vorbeugen können.

(6) Der Anbieter des Telekommunikationsdienstes darf im Falle einer Störung die Nutzung des Telekommunikationsdienstes bis zur Beendigung der Störung einschränken, umleiten oder unterbinden, soweit dies erforderlich ist, um die Beeinträchtigung der Telekommunikations- und Datenverarbeitungssysteme des Anbieters des Telekommunikationsdienstes, eines Nutzers im Sinne des Absatzes 4 oder anderer Nutzer zu beseitigen oder zu verhindern und der Nutzer die Störung nicht unverzüglich selbst beseitigt oder zu erwarten ist, dass der Nutzer die Störung selbst nicht unverzüglich beseitigt.

(7) Der Anbieter des Telekommunikationsdienstes darf den Datenverkehr von und zu Störungsquellen einschränken, umleiten oder unterbinden, soweit dies zur Vermeidung von Störungen in den Telekommunikations- und Datenverarbeitungssystemen der Nutzer erforderlich ist.

(8) Vorbehaltlich technischer Durchführungsmaßnahmen der Kommission nach Artikel 4 Absatz 5 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. L 201 vom 31.7.2002, S. 37; L 241 vom 10.9.2013, S. 9; L 162 vom 23.6.2017, S. 56), die zuletzt durch die Richtlinie 2009/136/EG (ABl. L 337 vom 18.12.2009, S. 11) geändert worden ist, kann die Bundesnetzagentur Leitlinien vorgeben bezüglich des Formats, der Verfahrensweise und der Umstände, unter denen eine Benachrichtigung über eine Verletzung des Schutzes personenbezogener Daten erforderlich ist.

Gesetz über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren (Atomgesetz)

§ 6 Genehmigung zur Aufbewahrung von Kernbrennstoffen

(1) Wer Kernbrennstoffe außerhalb der staatlichen Verwahrung aufbewahrt, bedarf der Genehmigung. Einer Genehmigung bedarf ferner, wer eine genehmigte Aufbewahrung wesentlich verändert.

(2) [...]

§ 7 Genehmigung von Anlagen

(1) Wer eine ortsfeste Anlage zur Erzeugung oder zur Bearbeitung oder Verarbeitung oder zur Spaltung von Kernbrennstoffen oder zur Aufarbeitung bestrahlter Kernbrennstoffe errichtet, betreibt oder sonst innehat oder die Anlage oder ihren Betrieb wesentlich verändert, bedarf der Genehmigung. Für die Errichtung und den Betrieb von Anlagen zur Spaltung von Kernbrennstoffen zur gewerblichen Erzeugung von Elektrizität und von Anlagen zur Aufarbeitung bestrahlter Kernbrennstoffe werden keine Genehmigungen erteilt. Dies gilt nicht für wesentliche Veränderungen von Anlagen oder ihres Betriebs.

(1a) [...]

§ 9 Bearbeitung, Verarbeitung und sonstige Verwendung von Kernbrennstoffen außerhalb genehmigungspflichtiger Anlagen

(1) Wer Kernbrennstoffe außerhalb von Anlagen der in § 7 bezeichneten Art bearbeitet, verarbeitet oder sonst verwendet, bedarf der Genehmigung. Einer Genehmigung bedarf ferner, wer von dem in der Genehmigungsurkunde festgelegten Verfahren für die Bearbeitung, Verarbeitung oder sonstige Verwendung wesentlich abweicht oder die in der Genehmigungsurkunde bezeichnete Betriebsstätte oder deren Lage wesentlich verändert.

(2) [...]

§ 44b Meldewesen für die Sicherheit in der Informationstechnik

Genehmigungsinhaber nach den §§ 6, 7 und 9 haben Beeinträchtigungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einer Gefährdung oder Störung der nuklearen Sicherheit der betroffenen kerntechnischen Anlage oder Tätigkeit führen können oder bereits geführt haben, unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik als zentrale Meldestelle zu melden. § 8b Absatz 1, 2 Nummer 1 bis 3, Nummer 4 Buchstabe a bis c und Absatz 7 des BSI-Gesetzes sind entsprechend anzuwenden. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, und der betroffenen Informationstechnik enthalten. Das Bundesamt für Sicherheit in der Informationstechnik leitet diese Meldungen unverzüglich an die für die nukleare Sicherheit und Sicherung zuständigen Genehmigungs- und Aufsichtsbehörden des Bundes und der Länder und an die von diesen bestimmten Sachverständigen nach § 20 weiter.

Gesetz über die Elektrizitäts- und Gasversorgung (Energiewirtschaftsgesetz - EnWG)

§ 11 Betrieb von Energieversorgungsnetzen

(1) Betreiber von Energieversorgungsnetzen sind verpflichtet, ein sicheres, zuverlässiges und leistungsfähiges Energieversorgungsnetz diskriminierungsfrei zu betreiben, zu warten und bedarfsgerecht zu optimieren, zu verstärken und auszubauen, soweit es wirtschaftlich zumutbar ist; dabei sind die Erfordernisse im Verkehrs-, Wärme-, Industrie- und Strombereich zu beachten, die sich ergeben, um Treibhausgasneutralität zu ermöglichen. Betreiber von Energieversorgungsnetzen haben insbesondere die Aufgaben nach den §§ 12 bis 16a zu erfüllen. Sie nehmen diese Aufgaben für ihr Energieversorgungsnetz in eigener Verantwortung wahr. Sie kooperieren und unterstützen sich bei der Wahrnehmung dieser Aufgaben; dies ist insbesondere für Maßnahmen anzuwenden, die sich auf das Netz eines anderen Betreibers von Energieversorgungsnetzen auswirken können. Die Verpflichtungen sind auch anzuwenden im Rahmen der Wahrnehmung der wirtschaftlichen Befugnisse der Leitung des vertikal integrierten Unternehmens und seiner Aufsichtsrechte nach § 7a Absatz 4 Satz 3. Der Ausbau eines L-Gasversorgungsnetzes ist nicht bedarfsgerecht im Sinne von Satz 1, wenn er auf Grund von Netzanschlüssen erfolgen muss, zu deren Einräumung der Betreiber des L-Gasversorgungsnetzes nicht nach den §§ 17 und 18 verpflichtet war.

(1a) Der Betrieb eines sicheren Energieversorgungsnetzes umfasst insbesondere auch einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Netzbetrieb notwendig sind. Die Regulierungsbehörde erstellt hierzu im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik einen Katalog von Sicherheitsanforderungen und veröffentlicht diesen. Der Katalog der Sicherheitsanforderungen enthält auch Regelungen zur regelmäßigen Überprüfung der Erfüllung der Sicherheitsanforderungen. Ein angemessener Schutz des Betriebs eines Energieversorgungsnetzes liegt vor, wenn dieser Katalog der Sicherheitsanforderungen eingehalten und dies vom Betreiber dokumentiert worden ist. Die Einhaltung kann von der Regulierungsbehörde überprüft werden. Zu diesem Zwecke kann die Regulierungsbehörde nähere Bestimmungen zu Format, Inhalt und Gestaltung der Dokumentation nach Satz 4 treffen.

(1b) Betreiber von Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 8 des Gesetzes vom 17. Juli 2015 (BGBl. I S. 1324) geändert worden ist, in der jeweils geltenden Fassung als Kritische Infrastruktur bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind, haben innerhalb einer von der Regulierungsbehörde festzulegenden Frist einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme zu gewährleisten, die für einen sicheren Anlagenbetrieb notwendig sind. Die Regulierungsbehörde erstellt hierzu im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik einen Katalog von Sicherheitsanforderungen, in den auch die Bestimmung der Frist nach Satz 1 aufzunehmen ist, und veröffentlicht diesen. Für Telekommunikations- und elektronische Datenverarbeitungssysteme von Anlagen nach § 7 Absatz 1 des Atomgesetzes haben Vorgaben auf Grund des Atomgesetzes Vorrang. Die für die nukleare Sicherheit zuständigen Genehmigungs- und Aufsichtsbehörden des Bundes und der Länder sind bei der Erarbeitung des Katalogs von Sicherheitsanforderungen zu beteiligen. Der Katalog von Sicherheitsanforderungen enthält auch Regelungen zur regelmäßigen Überprüfung der Erfüllung der Sicherheitsanforderungen. Ein ange-

messener Schutz des Betriebs von Energieanlagen im Sinne von Satz 1 liegt vor, wenn dieser Katalog eingehalten und dies vom Betreiber dokumentiert worden ist. Die Einhaltung kann von der Bundesnetzagentur überprüft werden. Zu diesem Zwecke kann die Regulierungsbehörde nähere Bestimmungen zu Format, Inhalt und Gestaltung der Dokumentation nach Satz 6 treffen.

(1c) Betreiber von Energieversorgungsnetzen und von solchen Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt wurden, haben

1. Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer erheblichen Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage geführt haben,
2. erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer erheblichen Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage führen können,

über die Kontaktstelle unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik zu melden.

Die Meldung muss Angaben zu der Störung, zu möglichen grenzübergreifenden Auswirkungen sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache und der betroffenen Informationstechnik, enthalten. Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat. Das Bundesamt für Sicherheit in der Informationstechnik hat die Meldungen unverzüglich an die Bundesnetzagentur weiterzuleiten. Das Bundesamt für Sicherheit in der Informationstechnik und die Bundesnetzagentur haben sicherzustellen, dass die unbefugte Offenbarung der ihnen nach Satz 1 zur Kenntnis gelangten Angaben ausgeschlossen wird. Zugang zu den Akten des Bundesamtes für Sicherheit in der Informationstechnik sowie zu den Akten der Bundesnetzagentur in Angelegenheiten nach § 11 Absatz 1a bis Absatz 1c wird nicht gewährt. § 29 des Verwaltungsverfahrensgesetzes bleibt unberührt. § 8e Absatz 1 des BSI-Gesetzes ist entsprechend anzuwenden.

(1d) Betreiber von Energieversorgungsnetzen und von solchen Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt wurden, sind verpflichtet, spätestens bis zum 1. April jeden Jahres, die von ihnen betriebene Anlage beim Bundesamt für Sicherheit in der Informationstechnik zu registrieren und eine Kontaktstelle zu benennen. Das Bundesamt für Sicherheit in der Informationstechnik übermittelt die Registrierungen einschließlich der damit verbundenen Kontaktdaten an die Bundesnetzagentur. Die Registrierung eines Betreibers eines Energieversorgungsnetzes oder von solchen Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt wurden, kann das Bundesamt für Sicherheit in der Informationstechnik auch selbst vornehmen, wenn der Betreiber seine Pflicht zur Registrierung nicht erfüllt. Nimmt das Bundesamt für Sicherheit in der Informationstechnik eine solche Registrierung selbst vor, informiert es die Bundesnetzagentur darüber und übermittelt die damit verbundenen Kontaktdaten. Die Betreiber haben sicherzustellen, dass sie über die benannte oder durch das Bundesamt für Sicherheit in der Informationstechnik festgelegte Kontaktstelle jederzeit erreichbar sind. Die

Übermittlung von Informationen durch das Bundesamt für Sicherheit in der Informationstechnik nach § 8b Absatz 2 Nummer 4 Buchstabe a des BSI-Gesetzes erfolgt an diese Kontaktstelle.

(1e) Betreiber von Energieversorgungsnetzen und von solchen Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt wurden, haben spätestens ab dem 1. Mai 2023 in ihren informationstechnischen Systemen, Komponenten oder Prozessen, die für die Funktionsfähigkeit der von ihnen betriebenen Energieversorgungsnetze oder Energieanlagen maßgeblich sind, in angemessener Weise Systeme zur Angriffserkennung einzusetzen. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen. Dabei soll der Stand der Technik eingehalten werden. Der Einsatz von Systemen zur Angriffserkennung ist angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den möglichen Folgen eines Ausfalls oder einer Beeinträchtigung des betroffenen Energieversorgungsnetzes oder der betroffenen Energieanlage steht.

(1f) Betreiber von Energieversorgungsnetzen und von solchen Energieanlagen, die nach der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur gelten, haben dem Bundesamt für Sicherheit in der Informationstechnik erstmalig am 1. Mai 2023 und danach alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1e nachzuweisen. Das Bundesamt für Sicherheit in der Informationstechnik hat die hierfür eingereichten Nachweisdokumente unverzüglich an die Bundesnetzagentur weiterzuleiten. Das Bundesamt für Sicherheit in der Informationstechnik und die Bundesnetzagentur haben sicherzustellen, dass die unbefugte Offenbarung der ihnen nach Satz 1 zur Kenntnis gelangten Angaben ausgeschlossen wird. Das Bundesamt für Sicherheit in der Informationstechnik kann bei Mängeln in der Umsetzung der Anforderungen nach Absatz 1e oder in den Nachweisdokumenten nach Satz 1 im Einvernehmen mit der Bundesnetzagentur die Beseitigung der Mängel verlangen.

(1g) Die Bundesnetzagentur legt bis zum 22. Mai 2023 im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik durch Allgemeinverfügung im Wege einer Festlegung nach § 29 Absatz 1 in einem Katalog von Sicherheitsanforderungen für das Betreiben von Energieversorgungsnetzen und Energieanlagen fest,

1. welche Komponenten kritische Komponenten im Sinne des § 2 Absatz 13 Satz 1 Nummer 3 Buchstabe a des BSI-Gesetzes sind oder
2. welche Funktionen kritisch bestimmte Funktionen im Sinne des § 2 Absatz 13 Satz 1 Nummer 3 Buchstabe b des BSI-Gesetzes sind.

Die Betreiber von Energieversorgungsnetzen und Energieanlagen, die durch Rechtsverordnung gemäß § 10 Absatz 1 Satz 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt wurden, haben die Vorgaben des Katalogs spätestens sechs Monate nach dessen Inkrafttreten zu erfüllen, es sei denn, in dem Katalog ist eine davon abweichende Umsetzungsfrist festgelegt worden. Der Katalog wird mit den Katalogen der Sicherheitsanforderungen nach § 11 Absatz 1a und 1b verbunden.

(2) [...]

Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen

Inhaltsübersicht

Erster Abschnitt
Allgemeine Vorschriften

§ 1 Zweck und Anwendungsbereich des Gesetzes

§ 2 Betroffener Personenkreis

§ 3 Zuständigkeit

§ 3a Geheimschutzbeauftragte, Sabotageschutzbeauftragte

§ 4 Allgemeine Grundsätze zum Schutz von Verschlusssachen, Mitwirkung des Bundesamtes für Sicherheit in der Informationstechnik

§ 5 Sicherheitsrisiken, sicherheitserhebliche Erkenntnisse

§ 6 Rechte der betroffenen Person und der mitbetroffenen Person

Zweiter Abschnitt
Überprüfungsarten und Durchführungsmaßnahmen

§ 7 Arten der Sicherheitsüberprüfung

§ 8 Einfache Sicherheitsüberprüfung

§ 9 Erweiterte Sicherheitsüberprüfung

§ 10 Erweitere Sicherheitsüberprüfung mit Sicherheitsermittlungen

§ 11 Datenerhebung

§ 12 Maßnahmen bei den einzelnen Überprüfungsarten, Überprüfungszeitraum

Dritter Abschnitt
Verfahren

§ 13 Sicherheitserklärung

§ 14 Abschluß der Sicherheitsüberprüfung

§ 15 Vorläufige Zuweisung einer sicherheitsempfindlichen Tätigkeit

§ 15a Unterrichtung durch die personalverwaltende Stelle

§ 16 Sicherheitserhebliche Erkenntnisse nach Abschluß der Sicherheitsüberprüfung

§ 17 Aktualisierung und Wiederholungsüberprüfung

Vierter Abschnitt
Akten über die Sicherheitsüberprüfung; Datenverarbeitung

§ 18 Sicherheitsakte und Sicherheitsüberprüfungsakte
§ 19 Aufbewahrung und Vernichtung der Unterlagen
§ 20 Speichern, Verändern und Nutzen personenbezogener Daten in Dateien
§ 21 Übermittlung und Zweckbindung
§ 22 Berichtigen, Löschen und Einschränken der Verarbeitung personenbezogener Daten
§ 23 Auskunft über gespeicherte personenbezogene Daten

Fünfter Abschnitt
Sonderregelungen für den nichtöffentlichen Bereich

§ 24 Anwendungsbereich
§ 25 Zuständigkeit
§ 26 Sicherheitserklärung
§ 27 Abschluß der Sicherheitsüberprüfung, Weitergabe sicherheitserheblicher Erkenntnisse
§ 28 Aktualisierung
§ 29 Übermittlung von Informationen über persönliche und arbeitsrechtliche Verhältnisse
§ 30 Sicherheitsakte der nicht-öffentlichen Stelle
§ 31 Datenverarbeitung in automatisierten Dateien

Sechster Abschnitt
Reisebeschränkungen, Sicherheitsüberprüfungen auf Antrag ausländischer Dienststellen und Schlußvorschriften

§ 32 Reisebeschränkungen
§ 33 Sicherheitsüberprüfung auf Antrag ausländischer Dienststellen
§ 34 Verordnungsermächtigung
§ 35 Allgemeine Verwaltungsvorschriften
§ 36 Anwendung des Bundesdatenschutzgesetzes, Bundesverfassungsschutzgesetzes, MAD-Gesetzes und BND-Gesetzes
§ 36a Unabhängige Datenschutzkontrolle
§ 37 Strafvorschriften
§ 38 Übergangsregelung
§ 39 Inkrafttreten

Erster Abschnitt
Allgemeine Vorschriften

§ 1 Zweck und Anwendungsbereich des Gesetzes

(1) Dieses Gesetz regelt die Voraussetzungen und das Verfahren zur Überprüfung einer Person, die von der zuständigen Stelle mit einer sicherheitsempfindlichen Tätigkeit betraut werden soll (Sicherheitsüberprüfung) oder bereits betraut worden ist (Wiederholungsüberprüfung), sowie den Schutz von Verschlusssachen.

(2) Eine sicherheitsempfindliche Tätigkeit übt aus, wer

1. Zugang zu Verschlußsachen hat oder ihn sich verschaffen kann, die STRENG GEHEIM, GEHEIM ODER VS-VERTRAULICH eingestuft sind,
2. Zugang zu Verschlußsachen über- oder zwischenstaatlicher Einrichtungen und Stellen hat oder ihn sich verschaffen kann, wenn die Bundesrepublik Deutschland verpflichtet ist, nur sicherheitsüberprüfte Personen hierzu zuzulassen,
3. in einer Behörde oder einer sonstigen öffentlichen Stelle des Bundes oder in einem Teil von ihr tätig ist, die auf Grund des Umfanges und der Bedeutung dort anfallender Verschlußsachen von der jeweils zuständigen obersten Bundesbehörde im Einvernehmen mit dem Bundesministerium des Innern, für Bau und Heimat als Nationale Sicherheitsbehörde zum Sicherheitsbereich erklärt worden ist,
4. nach anderen Vorschriften einer Sicherheitsüberprüfung unterliegt, soweit auf dieses Gesetz verwiesen wird.

(3) Verpflichten sich Stellen der Bundesrepublik Deutschland gegenüber Stellen anderer Staaten durch Übereinkünfte, bei Personen, die Zugang zu Verschlußsachen ausländischer Staaten haben oder sich verschaffen können, zuvor Sicherheitsüberprüfungen nach deutschem Recht durchzuführen, ist in diesen Übereinkünften festzulegen, welche Verschlußsachengrade des Vertragspartners Verschlußsachengraden nach diesem Gesetz vergleichbar sind. Derartige Festlegungen müssen sich im Rahmen der Bewertungen dieses Gesetzes halten und insbesondere den Maßstäben des § 4 entsprechen.

(4) Eine sicherheitsempfindliche Tätigkeit übt auch aus, wer an einer sicherheitsempfindlichen Stelle innerhalb einer lebens- oder verteidigungswichtigen Einrichtung oder wer innerhalb einer besonders sicherheitsempfindlichen Stelle des Geschäftsbereiches des Bundesministeriums der Verteidigung ("Militärischer Sicherheitsbereich") beschäftigt ist oder werden soll (vorbeugender personeller Sabotageschutz). Ziel des vorbeugenden personellen Sabotageschutzes ist es, potenzielle Saboteure (Innentäter) von sicherheitsempfindlichen Stellen fernzuhalten, um den Schutz der in Absatz 5 Satz 1 und 2 genannten Schutzgüter sicherzustellen.

(5) Lebenswichtig sind solche Einrichtungen,

1. deren Beeinträchtigung auf Grund der ihnen anhaftenden betrieblichen Eigengefahr die Gesundheit oder das Leben großer Teile der Bevölkerung erheblich gefährden kann oder
2. die für das Funktionieren des Gemeinwesens unverzichtbar sind und deren Beeinträchtigung erhebliche Unruhe in großen Teilen der Bevölkerung und somit Gefahren für die öffentliche Sicherheit oder Ordnung entstehen lassen würde.

Verteidigungswichtig sind außerhalb des Geschäftsbereiches des Bundesministeriums der Verteidigung solche Einrichtungen, die der Herstellung oder Erhaltung der Verteidigungsbereitschaft dienen und deren Beeinträchtigung auf Grund

1. fehlender kurzfristiger Ersetzbarkeit die Funktionsfähigkeit, insbesondere die Ausrüstung, Führung und Unterstützung der Bundeswehr und verbündeter Streitkräfte sowie der Zivilen Verteidigung, oder
2. der ihnen anhaftenden betrieblichen Eigengefahr die Gesundheit oder das Leben großer Teile der Bevölkerung

erheblich gefährden kann. Sicherheitsempfindliche Stelle ist die kleinste selbständig handelnde Organisationseinheit innerhalb einer lebens- oder verteidigungswichtigen Einrichtung, die vor unberechtigtem Zugang geschützt ist und von der im Falle der Beeinträchtigung eine erhebliche Gefahr für die in den Sätzen 1 und 2 genannten Schutzgüter ausgeht.

§ 2 Betroffener Personenkreis

(1) Eine Person, die mit einer sicherheitsempfindlichen Tätigkeit betraut werden soll (betroffene Person), ist vorher einer Sicherheitsüberprüfung zu unterziehen. Die Sicherheitsüberprüfung bedarf der Zustimmung der betroffenen Person, soweit gesetzlich nichts anderes bestimmt ist. Die Zustimmung ist schriftlich oder nach Maßgabe von § 3a des Verwaltungsverfahrensgesetzes oder unter Verwendung einer fortgeschrittenen elektronischen Signatur im Sinne von Artikel 3 Nummer 11 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73) zu erteilen. Eine sicherheitsempfindliche Tätigkeit darf erst nach Vollendung des 16. Lebensjahres übertragen werden.

(1a) Auf eine Sicherheitsüberprüfung kann verzichtet werden, wenn

1. für die betroffene Person bereits vor weniger als fünf Jahren eine gleich- oder höherwertige Überprüfung abgeschlossen wurde, ohne dass ein Sicherheitsrisiko festgestellt worden ist, oder
2. dies im Einzelfall erforderlich ist zur Abwehr einer gegenwärtigen und erheblichen Gefahr für
   a) eine Einrichtung nach § 1 Absatz 5 Satz 1 oder Satz 2 oder
   b) eine Anlage nach § 4 Absatz 2 oder § 12 Absatz 2 des Satellitendatensicherheitsgesetzes.

Die Entscheidung nach Satz 1 Nummer 2 trifft im öffentlichen Bereich die nach § 3 Absatz 1 zuständige Stelle und im nichtöffentlichen Bereich die nach § 25 Absatz 3 zuständige Stelle. Die nach Satz 2 zuständige Stelle bestimmt die im Fall von Satz 1 Nummer 2 zum Schutz der Verschlusssachen, der sicherheitsempfindlichen Stelle oder der Anlagen nach § 4 Absatz 2 und § 12 Absatz 2 des Satellitendatensicherheitsgesetzes erforderlichen Maßnahmen.

(2) In die Sicherheitsüberprüfung nach § 9 Absatz 1 Nummer 1 oder Nummer 2 oder nach § 10 soll einbezogen werden:

1. die volljährige Ehegattin oder der volljährige Ehegatte der betroffenen Person,
2. die Lebenspartnerin oder der Lebenspartner der betroffenen Person oder

3. die volljährige Partnerin oder der volljährige Partner, mit der oder dem die betroffene Person in einer auf Dauer angelegten Gemeinschaft lebt (Lebensgefährtin oder Lebensgefährte).

Über Ausnahmen entscheidet die zuständige Stelle. Die Einbeziehung bedarf der Zustimmung dieser Person. Die Zustimmung ist schriftlich oder nach Maßgabe von § 3a des Verwaltungsverfahrensgesetzes oder unter Verwendung einer fortgeschrittenen elektronischen Signatur im Sinne von Artikel 3 Nummer 11 der Verordnung (EU) Nr. 910/2014 zu erteilen. Sofern die Person im Sinne des Satzes 1 in die Sicherheitsüberprüfung einbezogen wird, ist sie mitbetroffene Person. Geht die betroffene Person die Ehe während oder nach der Sicherheitsüberprüfung ein oder begründet sie die auf Dauer angelegte Gemeinschaft während oder nach der Sicherheitsüberprüfung, so hat die betroffene Person die zuständige Stelle unverzüglich zu unterrichten. Das gleiche gilt, wenn die Volljährigkeit der Ehegattin, des Ehegatten, der Lebensgefährtin oder des Lebensgefährten während oder nach der Sicherheitsüberprüfung eintritt.

(3) Eine Sicherheitsüberprüfung ist nicht durchzuführen für

1. die Mitglieder der Verfassungsorgane des Bundes,

1a. die in der Bundesrepublik Deutschland gewählten Mitglieder des Europäischen Parlaments,

2. Richterinnen und Richter, soweit sie Aufgaben der Rechtsprechung wahrnehmen,

3. ausländische Staatsangehörige, die in der Bundesrepublik Deutschland im Interesse über- oder zwischenstaatlicher Einrichtungen und Stellen eine sicherheitsempfindliche Tätigkeit nach § 1 Abs. 2 Nr. 2 ausüben sollen; Regelungen über- oder zwischenstaatlicher Einrichtungen und Stellen bleiben unberührt.

Die in Satz 1 Nummer 1 bis 2 genannten Personen erhalten den Zugang zu Verschlusssachen kraft Amtes.

§ 3 Zuständigkeit

(1) Zuständige Stelle für die Sicherheitsüberprüfung ist

1. die Behörde oder sonstige öffentliche Stelle des Bundes, die eine betroffene Person mit einer sicherheitsempfindlichen Tätigkeit betrauen will,

2. das Bundesministerium des Innern, für Bau und Heimat als Nationale Sicherheitsbehörde für deutsche Staatsangehörige, die mit einer sicherheitsempfindlichen Tätigkeit bei über- oder zwischenstaatlichen Einrichtungen und Stellen betraut werden sollen, soweit nichts anderes bestimmt ist,

3. die politische Partei nach Artikel 21 des Grundgesetzes, die eine betroffene Person mit einer sicherheitsempfindlichen Tätigkeit innerhalb der Partei oder ihrer Stiftung betrauen will,

4. die Behörde oder sonstige öffentliche Stelle des Bundes, die eine Verschlusssache an eine nichtöffentliche Stelle weitergeben will, für eine betroffene Person dieser nichtöffentlichen Stelle, sofern sich die Zuständigkeit nicht nach dem Fünften Abschnitt richtet,

5. bei der Durchführung von Bauangelegenheiten des Bundes im Wege der Organleihe

   a) im zivilen Bereich die Bundesanstalt für Immobilienaufgaben,

   b) im Geschäftsbereich des Bundesministeriums der Verteidigung die nutzende Verwaltung,

   für eine betroffene Person einer nichtöffentlichen Stelle, sofern sich die Zuständigkeit nicht nach dem Fünften Abschnitt richtet.

In den Fällen des Satzes 1 Nummer 1 und 4 kann die oberste Bundesbehörde für ihren jeweiligen Geschäftsbereich abweichende Regelungen treffen. Ist eine andere Bundesbehörde als die Bundesbehörde, die die Liegenschaft nutzt oder nutzen soll, nach Satz 1 Nummer 1 oder 5 zuständige Stelle, obliegt es der Bundesbehörde, die die Liegenschaft nutzt oder nutzen soll, die sicherheitsempfindliche Tätigkeit festzustellen und im Bedarfsfall die Art der Sicherheitsüberprüfung festzulegen.

(1a) Die Aufgaben der zuständigen Stelle sind von einer von der Personalverwaltung, der oder dem Beauftragten für den Datenschutz und der Ansprechperson für Korruptionsprävention getrennten Organisationseinheit wahrzunehmen.

(2) Mitwirkende Behörde bei der Sicherheitsüberprüfung ist das Bundesamt für Verfassungsschutz nach § 3 Absatz 2 Satz 1 Nummer 1, 2 und 4 des Bundesverfassungsschutzgesetzes und im Geschäftsbereich des Bundesministeriums der Verteidigung der Militärische Abschirmdienst nach § 1 Absatz 3 Satz 1 Nummer 1 Buchstabe a bis c des MAD-Gesetzes, soweit nicht in Rechtsvorschriften über- oder zwischenstaatlicher Einrichtungen oder in völkerrechtlichen Verträgen, denen die gesetzgebenden Körperschaften gemäß Artikel 59 Abs. 2 des Grundgesetzes zugestimmt haben, etwas anderes bestimmt ist.

(3) Der Bundesnachrichtendienst, das Bundesamt für Verfassungsschutz und der Militärische Abschirmdienst sind

1. für Bewerberinnen und Bewerber sowie für Mitarbeiterinnen und Mitarbeiter des eigenen Nachrichtendienstes und
2. für andere betroffene Personen, wenn diese mit einer sicherheitsempfindlichen Tätigkeit nach § 1 Absatz 2 beim jeweiligen Nachrichtendienst betraut werden sollen,

jeweils zuständige Stelle für die Sicherheitsüberprüfung und mitwirkende Behörde zugleich. Sie wenden hierbei die Vorschriften dieses Gesetzes an. Satz 1 Nummer 2 gilt nicht, sofern der Bundesnachrichtendienst, das Bundesamt für Verfassungsschutz oder der Militärische Abschirmdienst ihre jeweils alleinige Zuständigkeit nach Art oder Dauer der sicherheitsempfindlichen Tätigkeit für entbehrlich halten.

§ 3a Geheimschutzbeauftragte, Sabotageschutzbeauftragte

(1) Die nach § 3 Absatz 1 Satz 1 Nummer 1, 4 und 5 für den Bereich des Geheimschutzes zuständigen Stellen sollen zur Erfüllung ihrer Aufgaben eine Geheimschutzbeauftragte oder einen Geheimschutzbeauftragten sowie eine zur Vertretung berechtigte Person bestellen. Soweit eine Geheimschutzbeauftragte oder ein Geheimschutzbeauftragter nicht bestellt wird, nimmt die Dienststellenleitung die Aufgaben der oder des Geheimschutzbeauftragten wahr. Die oder der Geheimschutzbeauftragte sorgt in ihrer oder seiner Behörde oder sonstigen öf-

fentlichen Stelle des Bundes für die Durchführung dieses Gesetzes und der dazu ergangenen Regelungen.

(2) Die nach § 3 Absatz 1 Satz 1 Nummer 1 und 5 für den Bereich des vorbeugenden personellen Sabotageschutzes zuständigen Stellen sollen zur Erfüllung ihrer Aufgaben eine Sabotageschutzbeauftragte oder einen Sabotageschutzbeauftragten sowie eine zur Vertretung berechtigte Person bestellen. Absatz 1 Satz 2 und 3 gilt entsprechend.

(3) Das Bundesministerium der Verteidigung trifft für seinen Geschäftsbereich die organisatorischen Maßnahmen zur Einrichtung von Geheimschutzbeauftragten und Sabotageschutzbeauftragten.

(4) Die näheren Aufgaben der Geheimschutzbeauftragten und der Sabotageschutzbeauftragten regeln die allgemeinen Verwaltungsvorschriften im Sinne des § 35.

§ 4 Allgemeine Grundsätze zum Schutz von Verschlusssachen, Mitwirkung des Bundesamtes für Sicherheit in der Informationstechnik

(1) Verschlusssachen sind im öffentlichen Interesse, insbesondere zum Schutz des Wohles des Bundes oder eines Landes, geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse, unabhängig von ihrer Darstellungsform. Verschlusssachen können auch Produkte und die dazugehörenden Dokumente sowie zugehörige Schlüsselmittel zur Entschlüsselung, Verschlüsselung und Übertragung von Informationen sein (Kryptomittel). Geheimhaltungsbedürftig im öffentlichen Interesse können auch Geschäfts-, Betriebs-, Erfindungs-, Steuer- oder sonstige private Geheimnisse oder Umstände des persönlichen Lebensbereichs sein.

(1a) Von einer Verschlusssache dürfen nur Personen Kenntnis erhalten, die auf Grund ihrer Aufgabenerfüllung Kenntnis haben müssen. Keine Person darf über eine Verschlusssache umfassender oder eher unterrichtet werden, als dies aus Gründen der Aufgabenerfüllung notwendig ist.

(2) Verschlusssachen werden entsprechend ihrer Schutzbedürftigkeit von einer amtlichen Stelle des Bundes oder auf deren Veranlassung in folgende Geheimhaltungsgrade eingestuft:

1. STRENG GEHEIM, wenn die Kenntnisnahme durch Unbefugte den Bestand oder lebenswichtige Interessen der Bundesrepublik Deutschland oder eines ihrer Länder gefährden kann,
2. GEHEIM, wenn die Kenntnisnahme durch Unbefugte die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährden oder ihren Interessen schweren Schaden zufügen kann,
3. VS-VERTRAULICH, wenn die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder schädlich sein kann,
4. VS-NUR FÜR DEN DIENSTGEBRAUCH, wenn die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein kann.

(3) Wer auf Grund dieses Gesetzes oder sonst in berechtigter Weise Zugang zu einer Verschlusssache erlangt,

1. ist zur Verschwiegenheit über die ihm dadurch zur Kenntnis gelangten Informationen verpflichtet und
2. hat durch Einhaltung der Schutzmaßnahmen, die auf Grund dieses Gesetzes erlassen worden sind, dafür Sorge zu tragen, dass keine unbefugte Person Kenntnis von der Verschlusssache erlangt.

(4) Behörden und sonstige öffentliche Stellen des Bundes sind verpflichtet, Verschlusssachen durch Maßnahmen des materiellen Geheimschutzes nach der jeweils für sie geltenden allgemeinen Verwaltungsvorschrift, die nach § 35 zu erlassen ist, so zu schützen, dass Durchbrechungen ihrer Vertraulichkeit entgegengewirkt wird, und darauf hinzuwirken, dass solche Versuche erkannt und aufgeklärt werden können. Dies gilt auch für die Weitergabe von Verschlusssachen an nichtöffentliche Stellen. Die eine Verschlusssache herausgebende Stelle kann weitere Vorgaben zum Schutz der Verschlusssache treffen.

(5) Bei der Durchführung der nach § 35 Absatz 1 erster Halbsatz zu erlassenden allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz wirkt das Bundesamt für Sicherheit in der Informationstechnik mit. Bei der Durchführung der nach § 35 Absatz 3 zu erlassenden allgemeinen Verwaltungsvorschrift zum materiellen Geheimschutz wirkt der Militärische Abschirmdienst mit. Bei der Betreuung der nichtöffentlichen Stellen im materiellen Geheimschutz sowie bei den Nachrichtendiensten des Bundes wirkt das Bundesamt für Sicherheit in der Informationstechnik auf Ersuchen der jeweils zuständigen Behörde mit.

(6) Das Bundesamt für Verfassungsschutz, der Militärische Abschirmdienst und der Bundesnachrichtendienst teilen dem Bundesamt für Sicherheit in der Informationstechnik nichtpersonenbezogene Erkenntnisse, die für den Schutz von Verschlusssachen oder die Aufrechterhaltung des Geheimschutzes von Bedeutung sein können, unverzüglich mit. Das gilt nicht, soweit die Erkenntnisse einem Weitergabeverbot unterliegen. § 23 des Bundesverfassungsschutzgesetzes gilt entsprechend.

§ 5 Sicherheitsrisiken, sicherheitserhebliche Erkenntnisse

(1) Im Sinne dieses Gesetzes liegt ein Sicherheitsrisiko vor, wenn tatsächliche Anhaltspunkte Folgendes begründen:

1. Zweifel an der Zuverlässigkeit der betroffenen Person bei der Wahrnehmung einer sicherheitsempfindlichen Tätigkeit,
2. eine besondere Gefährdung der betroffenen Person, insbesondere die Besorgnis der Erpressbarkeit, bei möglichen Anbahnungs- oder Werbungsversuchen
   a) ausländischer Nachrichtendienste,
   b) von Vereinigungen im Sinne der §§ 129 bis 129b des Strafgesetzbuches oder
   c) extremistischer Organisationen, die Bestrebungen im Sinne des § 3 Absatz 1 des Bundesverfassungsschutzgesetzes verfolgen,

   oder
3. Zweifel am Bekenntnis der betroffenen Person zur freiheitlichen demokratischen Grundordnung im Sinne des Grundgesetzes oder am jederzeitigen Eintreten für deren Erhaltung.

Ein Sicherheitsrisiko kann auch auf Grund tatsächlicher Anhaltspunkte nach Satz 1 Nummer 1 bis 3 im Hinblick auf die mitbetroffene Person vorliegen.

(2) Eine Erkenntnis ist sicherheitserheblich, wenn sich aus ihr ein Anhaltspunkt für ein Sicherheitsrisiko ergibt.

§ 6 Rechte der betroffenen Person und der mitbetroffenen Person

(1) Vor der Feststellung eines Sicherheitsrisikos ist der betroffenen Person Gelegenheit zu geben, sich persönlich zu den für die Entscheidung erheblichen Tatsachen zu äußern. Die betroffene Person kann im Rahmen der Anhörung eine Rechtsanwältin oder einen Rechtsanwalt beiziehen. Die Anhörung erfolgt in einer Weise, die den Quellenschutz gewährleistet und den schutzwürdigen Interessen von Personen, die im Rahmen einer Sicherheitsüberprüfung befragt wurden, Rechnung trägt. Sie unterbleibt, wenn sie einen erheblichen Nachteil für die Sicherheit des Bundes oder eines Landes zur Folge hätte, insbesondere bei Sicherheitsüberprüfungen der Bewerberinnen und Bewerber bei den Nachrichtendiensten des Bundes.

(2) Liegen im Hinblick auf die mitbetroffene Person tatsächliche Anhaltspunkte im Sinne des § 5 Absatz 1 Satz 1 Nummer 1 bis 3 vor, ist ihr Gelegenheit zu geben, sich vor der Feststellung eines Sicherheitsrisikos persönlich zu den für die Entscheidung erheblichen Tatsachen zu äußern. Absatz 1 Satz 2 bis 4 gilt entsprechend.

(3) Die Absätze 1 und 2 sind auch im Falle der Ablehnung einer Weiterbeschäftigung in einer sicherheitsempfindlichen Tätigkeit anzuwenden.

Zweiter Abschnitt
Überprüfungsarten und Durchführungsmaßnahmen

§ 7 Arten der Sicherheitsüberprüfung

(1) Entsprechend der vorgesehenen sicherheitsempfindlichen Tätigkeit wird entweder eine

1. einfache Sicherheitsüberprüfung oder
2. erweiterte Sicherheitsüberprüfung oder
3. erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen

durchgeführt.

(2) Ergeben sich bei der Sicherheitsüberprüfung sicherheitserhebliche Erkenntnisse, die nur durch Maßnahmen der nächsthöheren Art der Sicherheitsüberprüfung geklärt werden können, kann die zuständige Stelle mit Zustimmung der betroffenen Person die nächsthöhere Art der Sicherheitsüberprüfung anordnen. § 2 Absatz 2 Satz 1 bis 6 gilt entsprechend; § 12 Absatz 5 bleibt unberührt.

§ 8 Einfache Sicherheitsüberprüfung

(1) Die einfache Sicherheitsüberprüfung ist für Personen durchzuführen, die

1. Zugang zu VS-VERTRAULICH eingestuften Verschlußsachen erhalten sollen oder ihn sich verschaffen können,

2. Tätigkeiten in Bereichen nach § 1 Abs. 2 Nr. 3 wahrnehmen sollen.

(2) Die zuständige Stelle kann von der Sicherheitsüberprüfung absehen, wenn

1. in den Fällen des Absatzes 1 Nummer 1
   a) die Zuverlässigkeit der betroffenen Person durch eine Überprüfung nach dem Luftsicherheitsgesetz festgestellt wurde,
   b) die Betrauung mit der sicherheitsempfindlichen Tätigkeit unaufschiebbar ist,
   c) die Einstufung der Verschlusssache voraussichtlich vor Abschluss der Sicherheitsüberprüfung wieder aufgehoben wird und
   d) das Bundesministerium des Innern, für Bau und Heimat dem zugestimmt hat,
2. in den Fällen des Absatzes 1 Nummer 2 Art oder Dauer der Tätigkeit dies zulassen.

§ 2 Absatz 1a bleibt unberührt.

§ 9 Erweiterte Sicherheitsüberprüfung

(1) Eine erweiterte Sicherheitsüberprüfung ist für Personen durchzuführen, die

1. Zugang zu GEHEIM eingestuften Verschlußsachen erhalten sollen oder ihn sich verschaffen können,
2. Zugang zu einer hohen Anzahl VS-VERTRAULICH eingestuften Verschlußsachen erhalten sollen oder ihn sich verschaffen können,
3. Tätigkeiten in Bereichen nach § 1 Absatz 4 wahrnehmen sollen,

soweit nicht die zuständige Stelle in den Fällen der Nummern 1 und 2 im Einzelfall nach Art und Dauer der Tätigkeit eine Sicherheitsüberprüfung nach § 8 für ausreichend hält.

(2) In den Fällen von Absatz 1 Nummer 3 kann die Sicherheitsüberprüfung unterbleiben, wenn

1. eine Person mit einer unaufschiebbaren sicherheitsempfindlichen Tätigkeit betraut werden soll, für die keine überprüften Personen zur Verfügung stehen, oder
2. eine Person nur kurzzeitig, höchstens vier Wochen, eine sicherheitsempfindliche Tätigkeit ausüben soll

und die nicht überprüfte Person durch eine überprüfte Person ständig begleitet wird.

(3) Sofern eine sicherheitsempfindliche Stelle im Sinne des § 1 Absatz 5 Satz 3 neu festgestellt wird, ist die Sicherheitsüberprüfung für eine dort tätige Person nach Absatz 1 Nummer 3 unverzüglich durchzuführen.

§ 10 Erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen

Eine erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen ist für Personen durchzuführen,

1. die Zugang zu STRENG GEHEIM eingestuften Verschlußsachen erhalten sollen oder ihn sich verschaffen können,

2. die Zugang zu einer hohen Anzahl GEHEIM eingestuften Verschlußsachen erhalten sollen oder ihn sich verschaffen können,

3. die bei einem Nachrichtendienst des Bundes oder einer Behörde oder sonstigen öffentlichen Stelle des Bundes tätig werden sollen, die nach Feststellung der Bundesregierung gemäß § 34 Aufgaben von vergleichbarer Sicherheitsempfindlichkeit wahrnimmt,

soweit nicht die zuständige Stelle im Einzelfall nach Art und Dauer der Tätigkeit eine Sicherheitsüberprüfung nach § 8 oder § 9 für ausreichend hält.

§ 11 Datenerhebung

(1) Die zuständige Stelle und die mitwirkende Behörde dürfen die zur Erfüllung ihrer Aufgaben nach diesem Gesetz erforderlichen Daten erheben. Die betroffene Person sowie die sonstigen zu befragenden Personen und nicht-öffentlichen Stellen sind auf den Zweck der Erhebung, die Auskunftspflichten nach diesem Gesetz und auf eine dienst-, arbeitsrechtliche oder sonstige vertragliche Mitwirkungspflicht, ansonsten auf die Freiwilligkeit ihrer Angaben hinzuweisen. Bei Sicherheitsüberprüfungen nach § 3 Absatz 3 Satz 1 kann die Angabe der erhebenden Stelle gegenüber den sonstigen zu befragenden Personen oder öffentlichen und nichtöffentlichen Stellen unterbleiben, wenn dies zum Schutz der betroffenen Person oder des Nachrichtendienstes erforderlich ist.

(2) Die zuständige Stelle erhebt die personenbezogenen Daten bei der betroffenen Person oder bei der mitbetroffenen Person. Reicht diese Erhebung nicht aus oder stehen ihr schutzwürdige Interessen der betroffenen Person oder der mitbetroffenen Person entgegen, können andere geeignete Personen oder Stellen befragt werden.

§ 12 Maßnahmen bei den einzelnen Überprüfungsarten, Überprüfungszeitraum

(1) Bei der Sicherheitsüberprüfung nach § 8 trifft die mitwirkende Behörde folgende Maßnahmen:

1. sicherheitsmäßige Bewertung der Angaben in der Sicherheitserklärung unter Berücksichtigung der Erkenntnisse der Verfassungsschutzbehörden des Bundes und der Länder,

2. Einholung einer unbeschränkten Auskunft aus dem Bundeszentralregister und dem Gewerbezentralregister und Ersuchen um eine Datenübermittlung aus dem Zentralen staatsanwaltschaftlichen Verfahrensregister,

3. soweit im Einzelfall erforderlich, bei ausländischen betroffenen Personen, die keine freizügigkeitsberechtigten Unionsbürger sind, Ersuchen um eine Übermittlung der nach § 3 Absatz 1 und 2 Nummer 5, 6 und 9 des AZR-Gesetzes gespeicherten Daten,

4. Anfragen an das Bundeskriminalamt, die in der Rechtsverordnung nach § 58 Abs. 1 des Bundespolizeigesetzes bestimmte Bundespolizeibehörde und die Nachrichtendienste des Bundes,

5. Anfragen an ausländische Sicherheitsbehörden oder nach dortigem Recht für solche Anfragen zuständige öffentliche Stellen bei Auslandsaufenthalten von ununterbrochen längerer Dauer als sechs Monaten in den vergangenen fünf Jahren.

(1a) Eine Anfrage nach Absatz 1 Nummer 4 bedarf der gesonderten Zustimmung. Bei einer Anfrage dürfen an die ausländischen Sicherheitsbehörden oder an die nach dortigem Recht für eine solche Anfrage zuständigen öffentlichen Stellen nur folgende Daten übermittelt werden:

1. Namen, auch frühere, Vornamen, auch frühere,
2. Geburtsdatum, -ort,
3. Staatsangehörigkeit, auch frühere und weitere Staatsangehörigkeiten,
4. Wohnsitze, Adressen des Aufenthalts in dem Staat, dessen Sicherheitsbehörde oder zuständige öffentliche Stelle angefragt werden soll,
5. aktueller Wohnsitz, sofern erforderlich,
6. Pass- oder Personalausweisnummer oder Kopie des Ausweisdokuments, sofern erforderlich,
7. Angaben zu den Eltern, sofern erforderlich, sowie
8. Anlass der Anfrage.

Die Anfrage unterbleibt, wenn ihr entgegenstehen:

1. auswärtige Belange der Bundesrepublik Deutschland,
2. Sicherheitsinteressen der Bundesrepublik Deutschland oder
3. unter Berücksichtigung des besonderen öffentlichen Interesses der Anfrage überwiegende schutzwürdige Interessen der betroffenen Person oder der mitbetroffenen Person.

Zu den schutzwürdigen Interessen der betroffenen Person oder der mitbetroffenen Person gehört auch das Vorhandensein eines angemessenen Datenschutzniveaus im angefragten Staat. Wird eine Anfrage aus den in Satz 3 genannten Gründen nicht durchgeführt oder wurde sie nicht beantwortet, ist Absatz 5 entsprechend anzuwenden.

(2) Bei der Sicherheitsüberprüfung nach § 9 trifft die mitwirkende Behörde zusätzlich zu Absatz 1 folgende Maßnahmen:

1. Anfragen an die Polizeidienststellen der innegehabten Wohnsitze im Inland der betroffenen Person, in der Regel beschränkt auf die letzten fünf Jahre,
2. Prüfung der Identität der betroffenen Person.

(2a) Für die mitbetroffene Person trifft die mitwirkende Behörde die in den Absätzen 1 bis 2 genannten Maßnahmen.

(3) Bei der Sicherheitsüberprüfung nach § 10 befragt die mitwirkende Behörde zusätzlich von der betroffenen Person in ihrer Sicherheitserklärung angegebene Referenzpersonen und weitere geeignete Auskunftspersonen, um zu prüfen, ob die Angaben der betroffenen Person zutreffen und ob tatsächliche Anhaltspunkte vorliegen, die auf ein Sicherheitsrisiko schließen lassen. In den Fällen des § 10 Nummer 3 sind diese Maßnahmen in der Regel auch im Hinblick auf die mitbetroffene Person durchzuführen. Ist die betroffene Person Bewerberin oder Bewerber oder Mitarbeiterin oder Mitarbeiter eines Nachrichtendienstes, kann sie auch selbst befragt werden.

(3a) Bei der Sicherheitsüberprüfung nach den §§ 8, 9 und 10 kann zu der betroffenen Person in erforderlichem Maße Einsicht in öffentlich sichtbare Internetseiten genommen werden mit Ausnahme des öffentlich sichtbaren Teils sozialer Netzwerke. Bei der Sicherheitsüberprüfung nach den §§ 9 und 10 kann zu der betroffenen Person zusätzlich in erforderlichem Maße in den öffentlich sichtbaren Teil sozialer Netzwerke Einsicht genommen werden. Satz 2 gilt auch bei der Sicherheitsüberprüfung nach § 8, soweit die betroffene Person dem Geschäftsbereich des Bundesministeriums der Verteidigung angehört.

(4) Die zuständige Stelle fragt zur Feststellung einer hauptamtlichen oder inoffiziellen Tätigkeit der betroffenen Person oder der mitbetroffenen Person für den Staatssicherheitsdienst der Deutschen Demokratischen Republik bei dem Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik an, wenn die betroffene Person oder die mitbetroffene Person vor dem 1. Januar 1970 geboren wurde und in dem Gebiet der Deutschen Demokratischen Republik wohnhaft war oder Anhaltspunkte für eine Tätigkeit für den Staatssicherheitsdienst der Deutschen Demokratischen Republik vorliegen. Die Anfrage bezieht sich auch auf Hinweise über frühere Verbindungen zu einem ausländischen Nachrichtendienst. Ergibt die Anfrage sicherheitserhebliche Erkenntnisse, übermittelt sie die zuständige Stelle zur Bewertung an die mitwirkende Behörde. Die Regelung gilt nicht für die Sicherheitsüberprüfung nach § 9 Absatz 1 Nummer 3, es sei denn, die Überprüfung betrifft Angehörige des Geschäftsbereichs des Bundesministeriums der Verteidigung.

(5) Soweit es eine sicherheitserhebliche Erkenntnis erfordert, können die betroffene und die mitbetroffene Person selbst befragt werden. Reicht diese Befragung nicht aus, stehen ihr schutzwürdige Interessen entgegen oder erfordert es die Prüfung der Identität, kann die mitwirkende Behörde neben den Maßnahmen nach den Absätzen 1 bis 3 weitere geeignete Auskunftspersonen oder andere geeignete Stellen befragen oder Einzelmaßnahmen der nächsthöheren Art der Sicherheitsüberprüfung durchführen. Ferner kann die betroffene Person aufgefordert werden, für die Aufklärung der sicherheitserheblichen Erkenntnis geeignete Unterlagen beizubringen. Zusätzlich können von öffentlichen Stellen Akten beigezogen werden, von Gerichten, Staatsanwaltschaften oder Finanzbehörden auch über Strafverfahren wegen einer Steuerstraftat im Sinne des § 369 der Abgabenordnung.

(6) Die Überprüfung erstreckt sich in der Regel auf den Zeitraum der letzten fünf Jahre, bei den in § 3 Absatz 3 Nummer 1 genannten Personen auf den Zeitraum der letzten zehn Jahre. Internationale Vorschriften, die einen anderen Zeitraum vorsehen, bleiben unberührt.

Dritter Abschnitt
Verfahren

§ 13 Sicherheitserklärung

(1) In der Sicherheitserklärung sind von der betroffenen Person anzugeben:

1. Namen, auch frühere, Vornamen, auch frühere,
2. Geburtsdatum-, -ort,
2a. Geschlechtseintrag,
3. Staatsangehörigkeit, auch frühere und weitere Staatsangehörigkeiten,
4. Familienstand und das Bestehen einer auf Dauer angelegten Gemeinschaft,

5. Wohnsitze und Aufenthalte von längerer Dauer als zwei Monate, und zwar im Inland in den vergangenen fünf Jahren, im Ausland grundsätzlich ab dem 18. Lebensjahr, in jedem Fall aber in den vergangenen fünf Jahren,
6. ausgeübter Beruf,
7. Arbeitgeber und dessen Anschrift,
8. telefonische und elektronische Erreichbarkeit,
9. im Haushalt lebende Personen über 18 Jahre (Namen, auch frühere, Vornamen, Geburtsdatum, Geburtsort, Staatsangehörigkeit, Geschlechtseintrag und Verhältnis zu dieser Person),
10. Eltern, Stief- oder Pflegeeltern (Namen, auch frühere, Vornamen, Geburtsdatum, Geburtsort, Staatsangehörigkeit und Wohnsitz),
11. Ausbildungs- und Beschäftigungszeiten, Wehr- oder Zivildienstzeiten mit Angabe der Ausbildungsstätten, Beschäftigungsstellen sowie deren Anschriften, für Zeiten der Nichtbeschäftigung den Aufenthaltsort, sofern der jeweilige Zeitraum ununterbrochen mehr als drei Monate umfasst,
12. Nummer des Personalausweises oder Reisepasses sowie die ausstellende Behörde und das Ausstellungsdatum,
13. laufende oder in den vergangenen fünf Jahren abgeschlossene Insolvenzverfahren, in den vergangenen fünf Jahren gegen sie durchgeführte Zwangsvollstreckungsmaßnahmen und ob zurzeit die finanziellen Verpflichtungen erfüllt werden können,
14. Kontakte zu ausländischen Nachrichtendiensten oder zu Nachrichtendiensten der Deutschen Demokratischen Republik, die auf einen Anbahnungs- und Werbungsversuch hindeuten können,
15. Beziehungen zu verfassungsfeindlichen Organisationen,
16. anhängige Strafverfahren einschließlich Ermittlungsverfahren und Disziplinarverfahren,

16a. strafrechtliche Verurteilungen im Ausland,

17. Wohnsitze, Aufenthalte, Reisen, nahe Angehörige und sonstige Beziehungen in und zu Staaten, in denen nach Feststellung des Bundesministeriums des Innern, für Bau und Heimat besondere Sicherheitsrisiken für die mit sicherheitsempfindlicher Tätigkeit befassten Personen zu besorgen sind,
18. drei Referenzpersonen (Namen, Vornamen, Geburtsdatum, Geburtsort, Geschlechtseintrag, Beruf, berufliche und private Anschrift und telefonische und elektronische Erreichbarkeit sowie zeitlicher Beginn der Bekanntschaft) nur bei einer Sicherheitsüberprüfung nach § 10,
19. frühere Sicherheitsüberprüfungen und Zuverlässigkeitsüberprüfungen,
20. die Adressen eigener Internetseiten und die Mitgliedschaften in sozialen Netzwerken im Internet nur bei einer Sicherheitsüberprüfung nach den §§ 9, 10 und bei ei-

ner Sicherheitsüberprüfung nach § 8 für Angehörige des Geschäftsbereichs des Bundesministeriums der Verteidigung.

Der Sicherheitserklärung sind zwei aktuelle Lichtbilder der betroffenen Person mit der Angabe des Jahres der Aufnahme beizufügen. Die Lichtbilder können in elektronischer Form verlangt werden. Die Lichtbilder dürfen nicht für einen automatisierten Abgleich mit Datenbanken genutzt werden.

(2) Bei der Sicherheitsüberprüfung nach § 8 entfallen die Angaben zu Absatz 1 Nummer 11 und 12; Angaben zu Absatz 1 Nummer 12 dürfen nachträglich erhoben werden, soweit Maßnahmen nach § 12 Absatz 1 Nummer 4 zu treffen sind. Angaben zu Absatz 1 Nummer 10 entfallen, soweit die dort genannten Personen nicht in einem Haushalt mit der betroffenen Person leben. Zur Person der Ehegattin, des Ehegatten, der Lebenspartnerin, des Lebenspartners, der Lebensgefährtin oder des Lebensgefährten sind mit deren Einverständnis die in Absatz 1 Nummer 1 bis 4, 14 und 15 genannten Daten anzugeben.

(2a) Für Angehörige des Geschäftsbereichs des Bundesministeriums der Verteidigung entfallen bei Sicherheitsüberprüfungen nach § 9 Absatz 1 Nummer 3 die Angaben zu Absatz 1 Nummer 4, 9 und 10, bei Sicherheitsüberprüfungen nach § 9 Absatz 1 Nummer 3 im Übrigen entfallen zusätzlich auch die Angaben zu Absatz 1 Nummer 11, 13, 14 und 17.

(3) Zur mitbetroffenen Person sind zusätzlich die in Absatz 1 Nummer 5 bis 7, 12, 13, 16, 16a und 17 genannten Daten anzugeben.

(4) Bei Sicherheitsüberprüfungen der in § 3 Absatz 3 Satz 1 Nummer 1 genannten Personen sind zusätzlich anzugeben:

1. die Wohnsitze seit der Geburt,
2. die Kinder,
3. die Geschwister,
4. abgeschlossene Strafverfahren einschließlich Ermittlungsverfahren und Disziplinarverfahren,
5. alle Kontakte zu ausländischen Nachrichtendiensten oder zu Nachrichtendiensten der Deutschen Demokratischen Republik,
6. zwei Auskunftspersonen (Namen, Vornamen, Geburtsdatum, Geburtsort, Anschrift, telefonische und elektronische Erreichbarkeit und Verhältnis zur Person) zur Identitätsprüfung der betroffenen Person,
7. im Falle des Vorhandenseins einer mitbetroffenen Person zwei Auskunftspersonen (Namen, Vornamen, Geburtsdatum, Geburtsort, Anschrift, telefonische und elektronische Erreichbarkeit und Verhältnis zur Person) zu deren Identitätsprüfung.

(4a) Von Angehörigen des Geschäftsbereichs des Bundesministeriums der Verteidigung sowie von Angehörigen der Behörden des Bundes mit Aufgaben von vergleichbarer Sicherheitsempfindlichkeit wie die der Nachrichtendienste des Bundes sind zusätzlich die Anzahl der Kinder anzugeben.

(5) Die betroffene Person kann Angaben verweigern, die für sie, eine nahe Angehörige oder einen nahen Angehörigen im Sinne des § 52 Absatz 1 der Strafprozessordnung oder die Lebensgefährtin oder den Lebensgefährten die Gefahr strafrechtlicher oder disziplinarischer Verfolgung, der Entlassung oder Kündigung begründen könnten. Dies gilt auch, soweit für

eine nahe Angehörige oder einen nahen Angehörigen der mitbetroffenen Person eine solche Gefahr begründet werden könnte. Über das Verweigerungsrecht ist die betroffene Person zu belehren.

(6) Die Sicherheitserklärung ist von der betroffenen Person der zuständigen Stelle zuzuleiten. Sie prüft die Angaben der betroffenen Person auf ihre Vollständigkeit und Richtigkeit. Zu diesem Zweck kann die Personalakte eingesehen werden. Die zuständige Stelle leitet die Sicherheitserklärung an die mitwirkende Behörde weiter und beauftragt diese, eine Sicherheitsüberprüfung durchzuführen, es sei denn, die zuständige Stelle hat bereits bei der Prüfung der Sicherheitserklärung festgestellt, daß ein Sicherheitsrisiko vorliegt, das einer sicherheitsempfindlichen Tätigkeit entgegensteht. Die mitwirkende Behörde kann mit Zustimmung der zuständigen Stelle und der betroffenen Person in die Personalakte Einsicht nehmen, wenn dies zur Klärung oder Beurteilung sicherheitserheblicher Erkenntnisse unerläßlich ist.

§ 14 Abschluß der Sicherheitsüberprüfung

(1) Kommt die mitwirkende Behörde zu dem Ergebnis, daß kein Sicherheitsrisiko nach § 5 Abs. 1 vorliegt, so teilt sie dies der zuständigen Stelle mit. Fallen Erkenntnisse an, die kein Sicherheitsrisiko begründen, aber weiterhin sicherheitserheblich sind, so werden diese mitgeteilt.

(2) Kommt die mitwirkende Behörde zu dem Ergebnis, daß ein Sicherheitsrisiko vorliegt, unterrichtet sie schriftlich oder elektronisch unter Darlegung der Gründe und ihrer Bewertung die zuständige Stelle. Bei nachgeordneten Stellen erfolgt die Unterrichtung über deren oberste Bundesbehörde.

(2a) Kommt die mitwirkende Behörde zu dem Ergebnis, dass die Sicherheitsüberprüfung nicht abgeschlossen werden kann, unterrichtet sie unter Darlegung der Gründe die zuständige Stelle. Kommt die mitwirkende Behörde zu dem Ergebnis, dass die Sicherheitsüberprüfung nicht abgeschlossen werden kann, weil die betroffene Person in Bezug auf den in § 12 Absatz 6 genannten Zeitraum nicht überprüfbar ist, teilt sie der zuständigen Stelle zusätzlich mit, welche Maßnahmen sie nach § 12 getroffen hat und welche sicherheitserheblichen Erkenntnisse sich hieraus ergeben haben. Die Mitteilungen erfolgen schriftlich oder elektronisch.

(3) Die zuständige Stelle entscheidet, ob ein Sicherheitsrisiko vorliegt, das der sicherheitsempfindlichen Tätigkeit der betroffenen Person entgegensteht. Die Bewertung der übermittelten Erkenntnisse erfolgt auf Grund einer am Zweck der Sicherheitsüberprüfung orientierten Gesamtwürdigung des Einzelfalles, insbesondere im Hinblick auf die vorgesehene Tätigkeit. Im Zweifel hat das Sicherheitsinteresse Vorrang vor anderen Belangen. § 6 Abs. 1 und 2 ist zu beachten.

(4) Die zuständige Stelle unterrichtet die betroffene Person über das Ergebnis der Sicherheitsüberprüfung. Die Unterrichtung unterbleibt für Bewerberinnen und Bewerber bei den Nachrichtendiensten des Bundes sowie für Personen im Sinne des § 3 Absatz 3 Satz 1 Nummer 2.

(5) Die zuständige Stelle stellt die Sicherheitsüberprüfung ein, wenn die betroffene Person oder die mitbetroffene Person

1. der für den Abschluss der Sicherheitsüberprüfung erforderlichen Mitwirkung an der Sicherheitsüberprüfung nicht nachkommt oder

2. in Bezug auf den in § 12 Absatz 6 genannten Zeitraum nicht überprüfbar ist.

Ohne eine abgeschlossene Sicherheitsüberprüfung, die zum Ergebnis hat, dass kein Sicherheitsrisiko vorliegt, darf die betroffene Person nicht mit einer sicherheitsempfindlichen Tätigkeit betraut werden. § 2 Absatz 1a, § 8 Absatz 2, § 9 Absatz 2 und 3 und § 15 bleiben unberührt.

§ 15 Vorläufige Zuweisung einer sicherheitsempfindlichen Tätigkeit

Die zuständige Stelle kann in Ausnahmefällen abweichend von § 2 Absatz 1 die betroffene Person vor Abschluss der Sicherheitsüberprüfung mit einer sicherheitsempfindlichen Tätigkeit betrauen, wenn die mitwirkende Behörde

1. bei der einfachen Sicherheitsüberprüfung die Angaben in der Sicherheitserklärung unter Berücksichtigung der eigenen Erkenntnisse bewertet hat oder
2. bei der erweiterten Sicherheitsüberprüfung und bei der erweiterten Sicherheitsüberprüfung mit Sicherheitsermittlungen die Maßnahmen der nächstniederen Art der Sicherheitsüberprüfung abgeschlossen hat

und sich daraus keine tatsächlichen Anhaltspunkte für ein Sicherheitsrisiko ergeben haben.

§ 15a Unterrichtung durch die personalverwaltende Stelle

Die personalverwaltende Stelle unterrichtet die für die Sicherheitsüberprüfung zuständige Stelle unverzüglich über Veränderungen der persönlichen, dienstlichen und arbeitsrechtlichen Verhältnisse der Personen, die mit einer sicherheitsempfindlichen Tätigkeit betraut werden sollen oder bereits betraut sind. Dazu zählen:

1. Umsetzung, Abordnung, Versetzung und Ausscheiden aus dem Dienst,
2. Änderungen des Familienstandes, des Namens, des Vornamens, des Geschlechtseintrages, eines Wohnsitzes und der Staatsangehörigkeit,
3. Anhaltspunkte für Überschuldung, insbesondere Pfändungs- und Überweisungsbeschlüsse, Mitteilungen über abgeschlossene Insolvenzverfahren sowie Beschlüsse zur Eröffnung eines Insolvenzverfahrens und zur Restschuldbefreiung,
4. Strafverfahren und Disziplinarsachen sowie dienst- und arbeitsrechtliche Maßnahmen,
5. Nebentätigkeiten,
6. sonstige Erkenntnisse, die für die sicherheitsmäßige Beurteilung erheblich sein können.

§ 16 Sicherheitserhebliche Erkenntnisse nach Abschluß der Sicherheitsüberprüfung

(1) Die zuständige Stelle und die mitwirkende Behörde haben sich unverzüglich gegenseitig zu unterrichten, wenn sicherheitserhebliche Erkenntnisse über die betroffene Person oder die mitbetroffene Person bekanntwerden oder sich mitgeteilte Erkenntnisse als unrichtig erweisen.

(2) Die mitwirkende Behörde prüft die sicherheitserheblichen Erkenntnisse und stellt fest, ob ein Sicherheitsrisiko nach § 5 Abs. 1 vorliegt und unterrichtet die zuständige Stelle über das Ergebnis der Prüfung. Im übrigen ist § 14 Abs. 3 und 4 entsprechend anzuwenden.

(3) Liegt eine sicherheitserhebliche Erkenntnis vor, kann die zuständige Stelle die weitere Betrauung der betroffenen Person mit der sicherheitsempfindlichen Tätigkeit bis zu einer endgültigen Entscheidung über das Vorliegen eines Sicherheitsrisikos untersagen, sofern die besondere Bedeutung der Erkenntnis und die Art der sicherheitsempfindlichen Tätigkeit dies erfordern und die Untersagung keinen Aufschub duldet. § 6 Absatz 1 und 2 bleibt unberührt.

§ 17 Aktualisierung und Wiederholungsüberprüfung

(1) Die Sicherheitserklärung ist der betroffenen Person, die eine sicherheitsempfindliche Tätigkeit ausübt, in der Regel nach fünf Jahren erneut zuzuleiten und im Falle eingetretener Veränderungen von der betroffenen Person zu aktualisieren. Die zuständige Stelle prüft die Aktualisierungen auf ihre Vollständigkeit und Richtigkeit; § 13 Absatz 6 Satz 3 gilt entsprechend. Die zuständige Stelle beauftragt die mitwirkende Behörde, die Maßnahmen nach § 12 Absatz 1 im erforderlichen Umfang für die betroffene Person und für die mitbetroffene Person erneut durchzuführen und zu bewerten.

(2) Im Abstand von in der Regel zehn Jahren ist eine Wiederholungsüberprüfung einzuleiten. Im Übrigen kann die zuständige Stelle eine Wiederholungsüberprüfung einleiten, wenn sicherheitserhebliche Erkenntnisse dies nahelegen. Die Maßnahmen bei der Wiederholungsüberprüfung entsprechen denen der Erstüberprüfung; bei der Sicherheitsüberprüfung nach den §§ 9 oder 10 kann die mitwirkende Behörde von einer erneuten Identitätsprüfung absehen. Die Wiederholungsüberprüfung erfolgt nur mit Zustimmung

1. der betroffenen Person, soweit gesetzlich nichts anderes bestimmt ist, und
2. der mitbetroffenen Person.

§ 14 Absatz 4 Satz 2 findet keine Anwendung.

(3) Verweigert die betroffene Person oder die mitbetroffene Person die erforderliche Mitwirkung bei den Maßnahmen nach den Absätzen 1 und 2, ist die weitere Betrauung der betroffenen Person mit einer sicherheitsempfindlichen Tätigkeit unzulässig. § 14 Absatz 5 Satz 2 gilt entsprechend.

Vierter Abschnitt
Akten über die Sicherheitsüberprüfung, Datenverarbeitung

§ 18 Sicherheitsakte und Sicherheitsüberprüfungsakte

(1) Die zuständige Stelle führt über die betroffene Person eine Sicherheitsakte, in die alle die Sicherheitsüberprüfung betreffenden Informationen aufzunehmen sind.

(2) Informationen über die persönlichen, dienstlichen und arbeitsrechtlichen Verhältnisse der Personen, die mit einer sicherheitsempfindlichen Tätigkeit befaßt sind, sind zur Sicherheitsakte zu nehmen, soweit sie für die sicherheitsmäßige Beurteilung erheblich sind. Dazu zählen insbesondere:

1. Zuweisung, Übertragung einer sicherheitsempfindlichen Tätigkeit, die dazu erteilte Ermächtigung sowie deren Änderungen und Beendigung,
2. Umsetzung, Abordnung, Versetzung und Ausscheiden,

3. Änderungen des Namens, des Vornamens, des Geschlechtseintrages, eines Wohnsitzes und der Staatsangehörigkeit,
4. Beginn oder Ende einer Ehe, einer Lebenspartnerschaft oder einer auf Dauer angelegten Gemeinschaft,
5. Anhaltspunkte für Überschuldung, insbesondere Pfändungs- und Überweisungsbeschlüsse, Mitteilungen über abgeschlossene Insolvenzverfahren sowie Beschlüsse zur Eröffnung eines Insolvenzverfahrens und zur Restschuldbefreiung sowie
6. Strafverfahren und Disziplinarsachen sowie dienst- und arbeitsrechtliche Maßnahmen.

(3) Die Sicherheitsakte ist keine Personalakte. Sie ist gesondert zu führen und darf weder der personalverwaltenden Stelle noch der betroffenen Person zugänglich gemacht werden; § 23 Abs. 6 bleibt unberührt. Im Falle des Wechsels der Dienststelle oder des Dienstherrn ist die Sicherheitsakte nach dorthin abzugeben, wenn auch dort eine sicherheitsempfindliche Tätigkeit ausgeübt werden soll. Zum Zwecke der Prüfung nach § 2 Absatz 1a Satz 1 Nummer 1 kann der anfordernden Stelle die Sicherheitsakte zur Einsichtnahme übersandt werden.

(3a) Im Geschäftsbereich des Bundesministeriums der Verteidigung ist im Falle des Wechsels der Dienststelle die Sicherheitsakte stets an die neue Dienststelle abzugeben. Die neue Dienststelle darf den Inhalt der Sicherheitsakte nur dann zur Kenntnis nehmen, wenn die betroffene Person dort mit einer sicherheitsempfindlichen Tätigkeit betraut werden soll. Sofern keine Betrauung mit einer sicherheitsempfindlichen Tätigkeit erfolgen soll, ist die Sicherheitsakte dort bis zur Vernichtung aufzubewahren.

(4) Die mitwirkende Behörde führt über die betroffene Person eine Sicherheitsüberprüfungsakte, in die aufzunehmen sind:

1. Informationen, die die Sicherheitsüberprüfung, die durchgeführten Maßnahmen und das Ergebnis betreffen,
2. das Ausscheiden aus oder die Nichtaufnahme der sicherheitsempfindlichen Tätigkeit,
3. Änderungen des Namens, des Vornamens, des Geschlechtseintrages, eines Wohnsitzes und der Staatsangehörigkeit,
4. Beginn oder Ende einer Ehe, einer Lebenspartnerschaft oder einer auf Dauer angelegten Gemeinschaft.

Die in Absatz 2 Nummer 5 und 6 genannten Daten sind zur Sicherheitsüberprüfungsakte zu nehmen, wenn sie sicherheitserheblich sind. Absatz 3 Satz 1 und 2 gilt entsprechend. Im Falle des Wechsels der Dienststelle oder des Dienstherrn ist die Sicherheitsüberprüfungsakte auf Anforderung an die zuständige mitwirkende Behörde abzugeben, wenn eine sicherheitsempfindliche Tätigkeit nicht nur vorübergehend ausgeübt werden soll.

(5) Die zuständige Stelle ist verpflichtet, die in Absatz 4 Satz 1 Nummer 3 und 4 und Satz 2 genannten Daten mit Ausnahme der Änderung eines Wohnsitzes unverzüglich der mitwirkenden Behörde zu übermitteln. Die Übermittlung der in Absatz 4 Satz 1 Nr. 2 genannten Daten erfolgt nach den in § 22 Abs. 2 Nr. 1 festgelegten Fristen. Die in Absatz 4 Satz 1 Nummer 2 genannten Daten sind unverzüglich der mitwirkenden Behörde zu übermitteln, wenn sicherheitserhebliche Erkenntnisse oder Erkenntnisse, die ein Sicherheitsrisiko begründen, vorliegen.

(6) Die Sicherheitsakte und die Sicherheitsüberprüfungsakte dürfen auch in elektronischer Form geführt werden. Eine Abfrage personenbezogener Daten ist nur zulässig, wenn für die Daten die Voraussetzung der Speicherung nach § 20 vorliegt. Der automatisierte Abgleich personenbezogener Daten ist unzulässig.

(7) Bei jeder Abfrage einer Sicherheitsüberprüfungsakte nach Absatz 6 sind für Zwecke der Datenschutzkontrolle der Zeitpunkt, die Angaben, die die Feststellung der abgefragten Daten ermöglichen, sowie Angaben zur Feststellung des Abfragenden zu protokollieren. Die protokollierten Daten dürfen nur für Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitungsanlage verwendet werden. Die Protokolldaten sind am Ende des Kalenderjahres, das dem Jahr der Protokollierung folgt, zu löschen.

(8) Der Bundesnachrichtendienst, das Bundesamt für Verfassungsschutz und der Militärische Abschirmdienst dürfen bei der Sicherheitsüberprüfung von Personen im Sinne des § 3 Absatz 3 die Sicherheitsakte zusammen mit der Sicherheitsüberprüfungsakte in einem gemeinsamen Aktenvorgang unter Beachtung der für die jeweiligen Akten geltenden unterschiedlichen Verwendungs- und Auskunftsregelungen führen.

§ 19 Aufbewahrung und Vernichtung der Unterlagen

(1) Die Unterlagen über die Sicherheitsüberprüfung sind gesondert aufzubewahren und gegen unbefugten Zugriff zu schützen.

(2) Die Unterlagen über die Sicherheitsüberprüfung sind bei der zuständigen Stelle innerhalb eines Jahres zu vernichten, wenn bekannt wird, dass die betroffene Person keine sicherheitsempfindliche Tätigkeit aufgenommen hat. Im Übrigen sind die Unterlagen über die Sicherheitsüberprüfung bei der zuständigen Stelle fünf Jahre nach dem Ausscheiden der betroffenen Person aus der sicherheitsempfindlichen Tätigkeit zu vernichten. Eine Vernichtung unterbleibt, wenn

1. die betroffene Person in die weitere Aufbewahrung einwilligt,
2. ein Verwaltungsstreitverfahren oder ein Gerichtsverfahren anhängig ist, für das die Unterlagen über die Sicherheitsüberprüfung von Bedeutung sind,
3. beabsichtigt ist, die betroffene Person in absehbarer Zeit mit einer sicherheitsempfindlichen Tätigkeit zu betrauen oder
4. Grund zu der Annahme besteht, dass durch sie schutzwürdige Interessen der betroffenen Person beeinträchtigt würden.

Im Falle des Satzes 3 Nummer 4 ist die Verarbeitung der Daten einzuschränken; die Akte ist mit einem entsprechenden Sperrvermerk zu versehen. Die Daten dürfen nur noch mit Einwilligung der betroffenen Person gespeichert, genutzt, verändert, übermittelt und gelöscht werden.

(3) Die Unterlagen über die Sicherheitsüberprüfung bei der mitwirkenden Behörde sind nach den in § 22 Abs. 2 Nr. 2 genannten Fristen zu vernichten. Gleiches gilt bezüglich der Unterlagen zu den in § 3 Abs. 3 genannten Personen. Absatz 2 Satz 3 bis 5 gilt entsprechend.

(4) Das Bundesarchivgesetz findet auf die Unterlagen der Sicherheitsüberprüfung keine Anwendung.

§ 20 Speichern, Verändern und Nutzen personenbezogener Daten in Dateien

(1) Die zuständige Stelle darf zur Erfüllung ihrer Aufgaben nach diesem Gesetz die in § 13 Absatz 1 Satz 1 Nummer 1 bis 6 und Absatz 4 Nummer 1 genannten personenbezogenen Daten der betroffenen Person und der mitbetroffenen Person, ihre Aktenfundstelle und die der mitwirkenden Behörde sowie die Beschäftigungsstelle, Verfügungen zur Bearbeitung des Vorganges und beteiligte Behörden in Dateien speichern, verändern und nutzen.

(2) Die mitwirkende Behörde darf zur Erfüllung ihrer Aufgaben

1. die in § 13 Absatz 1 Satz 1 Nummer 1 bis 6 und Absatz 4 Nummer 1 genannten personenbezogenen Daten der betroffenen Person und der mitbetroffenen Person und die Aktenfundstelle,
2. Verfügungen zur Bearbeitung des Vorgangs sowie
3. sicherheitserhebliche Erkenntnisse und Erkenntnisse, die ein Sicherheitsrisiko begründen,

in Dateien speichern, verändern und nutzen. Die Daten nach Satz 1 Nummer 1 dürfen auch in die nach § 6 Absatz 2 des Bundesverfassungsschutzgesetzes zulässigen Verbunddateien gespeichert werden.

§ 21 Übermittlung und Zweckbindung

(1) Die im Rahmen der Sicherheitsüberprüfung gespeicherten personenbezogenen Daten dürfen von der zuständigen Stelle oder mitwirkenden Behörde nur für

1. die mit der Sicherheitsüberprüfung verfolgten Zwecke,
2. die mit Zuverlässigkeitsüberprüfungen nach dem Luftsicherheitsgesetz und dem Atomgesetz verfolgten Zwecke,
3. die mit sonstigen gesetzlich geregelten Überprüfungsverfahren zur Feststellung der Zuverlässigkeit verfolgten Zwecke,
4. Zwecke der Verfolgung von Straftaten von erheblicher Bedeutung sowie
5. Zwecke parlamentarischer Untersuchungsausschüsse

genutzt und übermittelt werden. Die Übermittlung und Nutzung nach Satz 1 Nummer 2 und 3 ist auf sicherheitserhebliche Erkenntnisse zu beschränken, die für die Bewertung der Zuverlässigkeit für die vorgesehene Verwendung von Bedeutung sein können. Die Strafverfolgungsbehörden dürfen die ihnen nach Satz 1 Nummer 4 übermittelten Daten für Zwecke eines Strafverfahrens nur verwenden, wenn die Strafverfolgung auf andere Weise erheblich weniger erfolgversprechend oder wesentlich erschwert wäre. Die zuständige Stelle darf die gespeicherten personenbezogenen Daten darüber hinaus für Zwecke der disziplinarrechtlichen Verfolgung sowie dienst- oder arbeitsrechtlicher Maßnahmen nutzen und übermitteln, wenn dies zu dem mit der Überprüfung verfolgten Zweck erforderlich ist. Die mitwirkende Behörde darf die gespeicherten personenbezogenen Daten darüber hinaus im Rahmen des erforderlichen Umfangs nutzen und übermitteln zur Aufklärung von sicherheitsgefährdenden oder geheimdienstlichen Tätigkeiten für eine fremde Macht oder von Bestrebungen, die darauf gerichtet sind, Gewalt anzuwenden oder Gewaltanwendung vorzubereiten oder zur Aufklärung sonstiger Bestrebungen von erheblicher Bedeutung.

(2) Die Übermittlung der nach § 20 in Dateien gespeicherten Daten ist nur zulässig, soweit sie für die Erfüllung der in Absatz 1 genannten Zwecke erforderlich ist. Die nach § 20 Abs. 2 Nr. 1 gespeicherten Daten dürfen zur Erfüllung aller Zwecke des Verfassungsschutzes genutzt und übermittelt werden.

(3) Die mitwirkende Behörde darf personenbezogene Daten nach den Absätzen 1 und 2 nur an öffentliche Stellen übermitteln.

(4) Die Nutzung oder Übermittlung unterbleibt, soweit gesetzliche Verwendungsregelungen entgegenstehen.

(5) Der Empfänger darf die übermittelten Daten nur für den Zweck speichern, nutzen, verändern und übermitteln, zu dessen Erfüllung sie ihm übermittelt werden, und zum Zweck der Strafverfolgung gemäß Absatz 1 Satz 1 Nummer 4. Eine nicht-öffentliche Stelle ist darauf hinzuweisen.

§ 22 Berichtigen, Löschen und Einschränken der Verarbeitung personenbezogener Daten

(1) Die zuständige Stelle und die mitwirkende Behörde haben personenbezogene Daten zu berichtigen, wenn sie unrichtig sind. Wird festgestellt, daß personenbezogene Daten unrichtig sind oder wird ihre Richtigkeit von der betroffenen Person bestritten, so ist dies, soweit sich die personenbezogenen Daten in Akten befinden, dort zu vermerken oder auf sonstige Weise festzuhalten.

(2) In Dateien gespeicherte personenbezogene Daten sind zu löschen

1. von der zuständigen Stelle
   a) innerhalb eines Jahres, wenn bekannt wird, dass die betroffene Person keine sicherheitsempfindliche Tätigkeit aufgenommen hat,
   b) nach Ablauf von fünf Jahren nach dem Ausscheiden der betroffenen Person aus der sicherheitsempfindlichen Tätigkeit,
2. von der mitwirkenden Behörde
   a) bei allen Überprüfungsarten innerhalb eines Jahres, im Geschäftsbereich des Bundesministeriums der Verteidigung innerhalb von fünf Jahren, wenn bekannt wird, dass die betroffene Person keine sicherheitsempfindliche Tätigkeit aufgenommen hat und keine sicherheitserheblichen Erkenntnisse angefallen sind,
   b) bei allen Überprüfungsarten nach Ablauf von fünf Jahren, wenn die betroffene Person keine sicherheitsempfindliche Tätigkeit aufgenommen hat und sicherheitserhebliche Erkenntnisse angefallen sind; in diesem Fall dürfen die personenbezogenen Daten nur nach Maßgabe des § 21 Absatz 1 und 2 genutzt und übermittelt werden,
   c) bei einfachen Sicherheitsüberprüfungen nach Ablauf von fünf Jahren nach dem Ausscheiden der betroffenen Person aus der sicherheitsempfindlichen Tätigkeit,
   d) bei erweiterten Sicherheitsüberprüfungen und erweiterten Sicherheitsüberprüfungen mit Sicherheitsermittlungen nach Ablauf von 15 Jahren, beim

Bundesnachrichtendienst nach Ablauf von 30 Jahren nach dem Ausscheiden der betroffenen Person aus der sicherheitsempfindlichen Tätigkeit.

Die mitwirkende Behörde hat bei allen Überprüfungsarten in Dateien gespeicherte personenbezogene Daten im Sinne des § 20 Absatz 2 Satz 1 Nummer 3 unverzüglich zu löschen, wenn die betroffene Person keine sicherheitsempfindliche Tätigkeit aufnimmt oder aus ihr ausgeschieden ist. Im Übrigen sind in Dateien gespeicherte personenbezogene Daten zu löschen, wenn ihre Speicherung unzulässig ist.

(3) Die Löschung nach Absatz 2 Satz 1 unterbleibt, wenn

1. die betroffene Person in die weitere Speicherung einwilligt,
2. ein Verwaltungsstreitverfahren oder ein Gerichtsverfahren anhängig ist, für das die gespeicherten personenbezogenen Daten von Bedeutung sind,
3. beabsichtigt ist, die betroffene Person in absehbarer Zeit mit einer sicherheitsempfindlichen Tätigkeit zu betrauen oder
4. Grund zu der Annahme besteht, dass durch sie schutzwürdige Interessen der betroffenen Person beeinträchtigt würden.

Im Falle des Satzes 1 Nummer 4 ist die Verarbeitung der Daten einzuschränken. Sie dürfen nur noch mit Einwilligung der betroffenen Person genutzt, verändert, übermittelt und gelöscht werden.

(4) Das Bundesarchivgesetz findet auf in Dateien gespeicherte personenbezogene Daten keine Anwendung.

§ 23 Auskunft über gespeicherte personenbezogene Daten

(1) Auf Antrag ist von der zuständigen Stelle oder mitwirkenden Behörde unentgeltlich Auskunft zu erteilen, welche Daten über die anfragende Person im Rahmen der Sicherheitsüberprüfung gespeichert wurden.

(2) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an die mitwirkenden Behörden, ist sie nur mit deren Zustimmung zulässig. Dies gilt auch für die Auskunftserteilung zu solchen Daten, die von der mitwirkenden Behörde an die zuständige Stelle übermittelt wurden. Die Zustimmung nach den Sätzen 1 und 2 ist zu erteilen, soweit kein Ausschlussgrund nach Absatz 3 vorliegt.

(3) Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben gefährden würde,
2. die Auskunft die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder
3. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheimgehalten werden müssen

und deswegen das Interesse der anfragenden Person an der Auskunftserteilung zurücktreten muß.

(4) Die Ablehnung der Auskunftserteilung bedarf einer Begründung nicht, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Fall sind die Gründe der Auskunftsverweigerung aktenkundig zu machen. Die anfragende Person ist auf die Rechtsgrundlage für das Fehlen der Begründung und darauf hinzuweisen, daß sie sich an die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wenden kann.

(5) Wird der anfragenden Person keine Auskunft erteilt, so ist sie auf ihr Verlangen der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu erteilen, soweit nicht die jeweils zuständige oberste Bundesbehörde im Einzelfall feststellt, daß dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit an die anfragende Person darf keine Rückschlüsse auf den Erkenntnisstand der speichernden Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

(6) Die zuständige Stelle gewährt der anfragenden Person Einsicht in die Sicherheitsakte, soweit eine Auskunft für die Wahrnehmung ihrer rechtlichen Interessen nicht ausreicht und sie hierfür auf die Einsichtnahme angewiesen ist. Die Regelungen der Absätze 2 bis 5 gelten entsprechend.

(7) (weggefallen)

Fünfter Abschnitt
Sonderregelungen für den nichtöffentlichen Bereich

§ 24 Anwendungsbereich

(1) Die Sonderregelungen dieses Abschnitts gelten bei Sicherheitsüberprüfungen von betroffenen Personen, die

1. von der zuständigen Stelle zu einer sicherheitsempfindlichen Tätigkeit nach § 1 Absatz 2 Nummer 1 und 2 in einer nichtöffentlichen Stelle ermächtigt werden sollen oder
2. von einer nichtöffentlichen Stelle mit einer sicherheitsempfindlichen Tätigkeit nach § 1 Absatz 2 Nummer 4 oder Absatz 4 betraut werden sollen.

(2) Sofern sicherheitsempfindliche Tätigkeiten im Sinne von § 1 Absatz 2 Nummer 1 bis 4 durch nichtöffentliche Stellen in öffentlichen Stellen durchgeführt werden, finden diese Sonderregelungen nur mit Zustimmung des Bundesministeriums für Wirtschaft und Energie Anwendung.

§ 25 Zuständigkeit

(1) Zuständige Stelle für sicherheitsempfindliche Tätigkeiten nach § 1 Absatz 2 Nummer 1 bis 4 ist das Bundesministerium für Wirtschaft und Energie, soweit gesetzlich nichts anderes bestimmt ist und nicht im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie eine andere Bundesbehörde die Aufgabe als zuständige Stelle wahrnimmt.

(2) Zuständige Stelle für sicherheitsempfindliche Tätigkeiten nach § 1 Abs. 4 ist dasjenige Bundesministerium, dessen Zuständigkeit für die nichtöffentliche Stelle in einer Rechtsver-

ordnung nach § 34 festgelegt ist. Das zuständige Bundesministerium kann seine Befugnis auf eine von ihm bestimmte sonstige öffentliche Stelle des Bundes übertragen.

(3) Die Aufgaben der nichtöffentlichen Stelle nach diesem Gesetz übernimmt

1. für den Bereich des Geheimschutzes nach § 1 Absatz 2 Nummer 1, 2 und 3 eine Sicherheitsbevollmächtigte oder ein Sicherheitsbevollmächtigter,
2. für den Bereich des vorbeugenden personellen Sabotageschutzes nach § 1 Absatz 4 eine Sabotageschutzbeauftragte oder ein Sabotageschutzbeauftragter und
3. für Bereiche nach § 1 Absatz 2 Nummer 4 eine hierfür Beauftragte oder ein hierfür Beauftragter.

(4) Für die Sicherheitsbevollmächtigte oder den Sicherheitsbevollmächtigten ist eine zur Vertretung berechtigte Person zu bestellen. Für Bereiche außerhalb des Geheimschutzes soll eine zur Vertretung berechtigte Person bestellt werden.

(5) § 3 Absatz 1a gilt für die nichtöffentliche Stelle entsprechend. Die zuständige Stelle kann Ausnahmen von § 3 Absatz 1a zulassen, wenn die nichtöffentliche Stelle sich verpflichtet, Informationen, die ihr im Rahmen der Sicherheitsüberprüfung bekannt werden, nur für solche Zwecke zu gebrauchen, die mit der Sicherheitsüberprüfung verfolgt werden.

§ 26 Sicherheitserklärung

Abweichend von § 13 Absatz 6 Satz 1 leitet die betroffene Person ihre Sicherheitserklärung der nicht-öffentlichen Stelle zu, in der sie beschäftigt ist oder beschäftigt werden soll. Die Sicherheitserklärung kann in den Fällen des Satzes 1 mit Zustimmung der zuständigen Stelle auch der nichtöffentlichen Stelle zugeleitet werden, bei der die betroffene Person tätig werden soll. Die Zustimmung der mitbetroffenen Person ist beizufügen. Die nicht-öffentliche Stelle prüft die Vollständigkeit und Richtigkeit der Angaben und darf, soweit dies erforderlich ist, die Personalunterlagen beiziehen. Sie gibt die Sicherheitserklärung an die zuständige Stelle weiter und teilt dieser vorhandene sicherheitserhebliche Erkenntnisse mit.

§ 27 Abschluß der Sicherheitsüberprüfung, Weitergabe sicherheitserheblicher Erkenntnisse

Die zuständige Stelle unterrichtet die nichtöffentliche Stelle nur darüber, dass die betroffene Person

1. nach § 1 Absatz 2 Nummer 1 bis 3 zur sicherheitsempfindlichen Tätigkeit ermächtigt oder nicht ermächtigt wird oder
2. mit der sicherheitsempfindlichen Tätigkeit nach § 1 Absatz 2 Nummer 4 oder Absatz 4 betraut oder nicht betraut werden darf.

Erkenntnisse, die die Ablehnung oder Aufhebung der Ermächtigung zur sicherheitsempfindlichen Tätigkeit oder der Betrauung mit der sicherheitsempfindlichen Tätigkeit betreffen, dürfen nicht mitgeteilt werden. Sofern es zu dem mit der Überprüfung verfolgten Zweck zwingend erforderlich ist, können abweichend von Satz 2 sicherheitserhebliche Erkenntnisse an die nicht-öffentliche Stelle übermittelt werden und dürfen von ihr ausschließlich zu diesem Zweck genutzt werden. Die nicht-öffentliche Stelle hat die zuständige Stelle unverzüglich zu unterrichten, wenn sicherheitserhebliche Erkenntnisse über die betroffene Person oder die mitbetroffene Person bekanntwerden.

§ 28 Aktualisierung

(1) Die nicht-öffentliche Stelle leitet der betroffenen Person, die eine sicherheitsempfindliche Tätigkeit ausübt, auf Anforderung der zuständigen Stelle die Sicherheitserklärung in der Regel nach fünf Jahren erneut zu.

(2) Die betroffene Person hat die in der Sicherheitserklärung angegebenen Daten im Falle eingetretener Veränderungen zu aktualisieren. Die nichtöffentliche Stelle prüft die Vollständigkeit und Richtigkeit der Aktualisierungen und darf, sofern dies erforderlich ist, die Personalunterlagen beiziehen. Die zuständige Stelle beauftragt die mitwirkende Behörde, die Maßnahmen nach § 12 Absatz 1 im erforderlichen Umfang für die betroffene Person und für die mitbetroffene Person erneut durchzuführen und zu bewerten.

§ 29 Übermittlung von Informationen über persönliche und arbeitsrechtliche Verhältnisse

(1) Die nichtöffentliche Stelle hat der zuständigen Stelle unverzüglich mitzuteilen

1. das Ausscheiden aus oder die Nichtaufnahme der sicherheitsempfindlichen Tätigkeit,
2. Änderungen des Namens, des Vornamens, des Geschlechtseintrages, eines Wohnsitzes oder der Staatsangehörigkeit,
3. Beginn oder Ende einer Ehe, einer Lebenspartnerschaft oder einer auf Dauer angelegten Gemeinschaft und
4. auf Anfrage der zuständigen Stelle weitere bei der nichtöffentlichen Stelle vorhandene Informationen zur Aufklärung sicherheitserheblicher Erkenntnisse.

(2) § 2 Absatz 2 Satz 7 und 8, § 14 Absatz 4 Satz 1 und § 15a gelten mit der Maßgabe, dass an die Stelle der zuständigen Stelle die nichtöffentliche Stelle tritt. Für Sicherheitsüberprüfungen nach § 9 Absatz 1 Nummer 3 gilt die Unterrichtungspflicht nach § 15a nur für Veränderungen nach § 15a Satz 2 Nummer 1, 2, 4 und 6.

§ 30 Sicherheitsakte der nicht-öffentlichen Stelle

Für die Sicherheitsakte in der nicht-öffentlichen Stelle gelten die Vorschriften dieses Gesetzes über die Sicherheitsakte entsprechend mit der Maßgabe, daß die Sicherheitsakte der nichtöffentlichen Stelle bei einem Wechsel des Arbeitgebers nicht abgegeben wird.

§ 31 Datenverarbeitung in automatisierten Dateien

Die nicht-öffentliche Stelle darf die nach diesem Gesetz zur Erfüllung ihrer Aufgaben erforderlichen personenbezogenen Daten der betroffenen Person in automatisierten Dateien speichern, verändern und nutzen. Die für die zuständige Stelle geltenden Vorschriften zur Berichtigung, Löschung und Sperrung finden Anwendung.

Sechster Abschnitt
Reisebeschränkungen, Sicherheitsüberprüfungen auf Antrag ausländischer Dienststellen und Schlußvorschriften

§ 32 Reisebeschränkungen

(1) Personen, die eine sicherheitsempfindliche Tätigkeit ausüben, die eine Sicherheitsüberprüfung nach den § 9 Absatz 1 Nummer 1 und 2 und § 10 erfordert, können verpflichtet werden, Dienst- und Privatreisen in und durch Staaten, für die besondere Sicherheitsregelungen gelten, der zuständigen Stelle oder der nicht-öffentlichen Stelle rechtzeitig vorher anzuzeigen. Die Verpflichtung kann auch für die Zeit nach dem Ausscheiden aus der sicherheitsempfindlichen Tätigkeit angeordnet werden.

(2) Die Reise kann von der zuständigen Stelle untersagt werden, wenn Anhaltspunkte zur Person oder eine besondere sicherheitsempfindliche Tätigkeit vorliegen, die eine erhebliche Gefährdung durch ausländische Nachrichtendienste erwarten lassen.

(3) Ergeben sich bei einer Reise in und durch Staaten, für die besondere Sicherheitsregelungen gelten, Anhaltspunkte, die auf einen Anbahnungs- und Werbungsversuch ausländischer Nachrichtendienste hindeuten können, so ist die zuständige Stelle nach Abschluß der Reise unverzüglich zu unterrichten.

§ 33 Sicherheitsüberprüfung auf Antrag ausländischer Dienststellen

(1) Ersucht eine ausländische Dienststelle die mitwirkenden Behörden um die Mitwirkung bei einer Sicherheitsüberprüfung, so richtet sie sich nach den Bestimmungen dieses Gesetzes, soweit nicht in Rechtsvorschriften über- oder zwischenstaatlicher Einrichtungen oder völkerrechtlichen Verträgen, denen die gesetzgebenden Körperschaften gemäß Artikel 59 Abs. 2 des Grundgesetzes zugestimmt haben, etwas anderes bestimmt ist.

(2) Die Mitwirkung unterbleibt, wenn auswärtige Belange der Bundesrepublik Deutschland oder überwiegende schutzwürdige Interessen der betroffenen Person entgegenstehen. Dies gilt auch bei der Übermittlung personenbezogener Daten an die ausländische Dienststelle.

(3) Die ausländische Dienststelle ist darauf hinzuweisen, daß die im Rahmen der Sicherheitsüberprüfung übermittelten personenbezogenen Daten nur für Zwecke der Sicherheitsüberprüfung verwendet werden dürfen und die mitwirkende Behörde sich vorbehält, um Auskunft über die vorgenommene Verwendung der Daten zu bitten.

§ 34 Verordnungsermächtigung

Die Bundesregierung wird ermächtigt, durch Rechtsverordnung ohne Zustimmung des Bundesrates festzustellen,

1. welche Behörden oder sonstigen öffentlichen Stellen des Bundes oder nichtöffentlichen Stellen oder Teile von ihnen lebens- oder verteidigungswichtige Einrichtungen mit sicherheitsempfindlichen Stellen im Sinne des § 1 Absatz 4 sind,
2. welches Bundesministerium für die nichtöffentliche Stelle zuständig ist und
3. welche Behörden oder sonstigen öffentlichen Stellen des Bundes Aufgaben im Sinne des § 10 Nummer 3 wahrnehmen.

§ 35 Allgemeine Verwaltungsvorschriften

(1) Die allgemeinen Verwaltungsvorschriften zur Ausführung dieses Gesetzes erläßt das Bundesministerium des Innern, für Bau und Heimat, soweit in den Absätzen 2 bis 4 nichts anderes bestimmt ist.

(2) Die allgemeinen Verwaltungsvorschriften zur Ausführung dieses Gesetzes im nichtöffentlichen Bereich erläßt das Bundesministerium für Wirtschaft und Energie im Einvernehmen mit dem Bundesministerium des Innern, für Bau und Heimat.

(3) Die allgemeinen Verwaltungsvorschriften zur Ausführung dieses Gesetzes im Geschäftsbereich des Bundesministeriums der Verteidigung erläßt das Bundesministerium der Verteidigung im Einvernehmen mit dem Bundesministerium des Innern, für Bau und Heimat.

(4) Die allgemeinen Verwaltungsvorschriften zur Ausführung dieses Gesetzes bei den Nachrichtendiensten des Bundes erläßt die jeweils zuständige oberste Bundesbehörde im Einvernehmen mit dem Bundesministerium des Innern, für Bau und Heimat.

§ 36 Anwendung des Bundesdatenschutzgesetzes, Bundesverfassungsschutzgesetzes, MAD-Gesetzes und BND-Gesetzes

(1) Die Vorschriften des Bundesdatenschutzgesetzes finden wie folgt Anwendung:

1. § 1 Absatz 8, § 16 Absatz 1 und 4 und die §§ 17 bis 21 sowie § 85 finden keine Anwendung,
2. die §§ 42, 46, 51 Absatz 1 und 3, die §§ 52, 53, 54 Absatz 1 und 2 sowie die §§ 62, 64, 83 sind entsprechend anzuwenden.

(2) Die Vorschriften des Ersten Abschnitts und die §§ 14 und 23 Absatz 1 Satz 2 des Bundesverfassungsschutzgesetzes auch in Verbindung mit § 12 des MAD-Gesetzes und § 18 des BND-Gesetzes sowie die §§ 1, 8 und § 10 Absatz 2 Satz 2 bis 6 des MAD-Gesetzes und § 8 des BND-Gesetzes finden Anwendung.

§ 36a Unabhängige Datenschutzkontrolle

(1) Jede Person kann sich an die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wenden, wenn sie der Ansicht ist, bei der Verarbeitung ihrer personenbezogenen Daten nach diesem Gesetz durch öffentliche oder nichtöffentliche Stellen in ihren Rechten verletzt worden zu sein.

(2) Die oder der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit kontrolliert bei den öffentlichen und den nichtöffentlichen Stellen die Einhaltung der anzuwendenden Vorschriften über den Datenschutz bei der Erfüllung der Aufgaben dieses Gesetzes. Soweit die Einhaltung von Vorschriften der Kontrolle durch die G 10-Kommission unterliegt, unterliegt sie nicht der Kontrolle durch die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, es sei denn, die G 10-Kommission ersucht die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, sie bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten. Der Kontrolle durch die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unterliegen auch nicht personenbezogene Daten in Akten über die Sicherheitsüberprüfung, wenn der Betroffene der Kontrolle der auf ihn bezogenen Daten im Einzelfall gegenüber der

oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit widerspricht.

(3) Die öffentlichen und nichtöffentlichen Stellen sind verpflichtet, die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und ihre oder seine schriftlich besonders Beauftragten bei der Erfüllung ihrer oder seiner Aufgaben zu unterstützen. Den in Satz 1 genannten Personen ist dabei insbesondere

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Kontrolle nach Absatz 2 stehen,
2. jederzeit Zutritt in alle Diensträume zu gewähren.

Dies gilt nicht, soweit die zuständige oberste Bundesbehörde im Einzelfall feststellt, dass die Auskunft oder Einsicht die Sicherheit des Bundes oder eines Landes gefährden würde.

§ 37 Strafvorschriften

(1) Wer unbefugt von diesem Gesetz geschützte personenbezogene Daten, die nicht offenkundig sind,

1. speichert, verändert oder übermittelt,
2. zum Abruf mittels automatisierten Verfahrens bereithält oder
3. abruft oder sich oder einem anderen aus Dateien verschafft,

wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer

1. die Übermittlung von durch dieses Gesetz geschützten personenbezogenen Daten, die nicht offenkundig sind, durch unrichtige Angaben erschleicht oder
2. entgegen § 21 Abs. 1 oder § 27 Satz 3 Daten für andere Zwecke nutzt, indem er sie innerhalb der Stelle an einen anderen weitergibt.

(3) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

(4) Die Tat wird nur auf Antrag verfolgt.

§ 38 Übergangsregelung

Bei Sicherheitsüberprüfungsverfahren von betroffenen Personen, die vor dem 1. Januar 2007 mit einer sicherheitsempfindlichen Tätigkeit betraut wurden und für die in den vergangenen zehn Jahren vor dem 21. Juni 2017 keine Wiederholungsüberprüfung durchgeführt wurde, gilt bis zum 21. Juni 2022 § 17 Absatz 2 Satz 1 mit der Maßgabe, dass die Wiederholungsüberprüfung an die Stelle der nächsten regulären Aktualisierung tritt.

§ 39 Inkrafttreten

Dieses Gesetz tritt am Tage nach der Verkündung in Kraft.

Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA)

Vom 13. März 2023

Nach Artikel 86 Satz 1 des Grundgesetzes in Verbindung mit § 35 Absatz 1 des Sicherheitsüberprüfungsgesetzes vom 20. April 1994 (BGBl. I S. 867) in Verbindung mit § 1 Absatz 2 des Zuständigkeitsanpassungsgesetzes vom 16. August 2002 (BGBl. I S. 3165) und dem Organisationserlass des Bundeskanzlers vom 8. Dezember 2021 erlässt das Bundesministerium des Innern und für Heimat folgende Allgemeine Verwaltungsvorschrift:

Inhaltsübersicht

Abschnitt I: Allgemeine Bestimmungen

§ 1 Anwendungsbereich

§ 2 Begriff der Verschlusssache und Geheimhaltungsgrade

§ 3 Allgemeine Grundsätze

§ 4 Verpflichtung, Ermächtigung und Zulassung

§ 5 Mitwirkende Behörden

§ 6 Mehrschichtige Sicherheit

Abschnitt II: Geheimschutzorganisation und Geheimschutzdokumentation

§ 7 Dienststellenleitung

§ 8 Geheimschutzbeauftragte

§ 8a Risikomanagement

§ 9 IT-Sicherheitsbeauftragte

§ 10 VS-Registratoren

§ 11 Qualifikation

Abschnitt III aufgelöst

§ 12 Erstellung der Geheimschutzdokumentation

§ 13 gestrichen

§ 14 gestrichen

Abschnitt IV: Einstufung und Befristung

§ 15 Einstufung

§ 16 Befristung

§ 17 Verlängerung der Einstufungsfrist

§ 18 Änderung der Einstufung

§ 19 Aufhebung der Einstufung

Abschnitt V: Handhabung von Verschlusssachen

§ 20 Herstellung und Kennzeichnung

§ 21 Verwaltung und Nachweis von Verschlusssachen

§ 22 Vervielfältigung von Verschlusssachen

§ 23 Aufbewahrung von Verschlusssachen

§ 24 Grundsätze zur Weitergabe von Verschlusssachen

§ 25 Weitergabe an nichtöffentliche Stellen

§ 26 Weitergabe an den Deutschen Bundestag, den Bundesrat, Landesparlamente und -behörden

§ 27 Empfang von Verschlusssachen

§ 28 Mitnahme von Verschlusssachen außerhalb des Dienstgebäudes

§ 29 Erörterung von Verschlusssachen

§ 30 Grundsätze der Aussonderung von Verschlusssachen

§ 31 Archivierung von Verschlusssachen

§ 32 Vernichtung von Verschlusssachen

§ 33 VS-Zwischenmaterial

Abschnitt VI: Zusammenarbeit mit nichtdeutschen Stellen und nichtöffentlichen Stellen mit Sitz im Ausland

§ 34 Weitergabe von deutschen Verschlusssachen an nichtdeutsche Stellen und nichtöffentliche Stellen mit Sitz im Ausland

§ 35 Empfang und Handhabung nichtdeutscher Verschlusssachen

§ 36 Sicherheitsakkreditierung

§ 37 Zentralregistraturen

Abschnitt VII: Materielle und technische Maßnahmen

§ 38 Planung und Durchführung

§ 39 Räumliche Sicherheitsmaßnahmen

§ 40 Technische Sicherung von Verschlusssachen

§ 41 Abhörschutzmaßnahmen

§ 42 Besondere Dienststellen

§ 43 VS-Registraturen

§ 44 VS-Verwahrgelasse
§ 45 VS-IT-Räume und -Bereiche
§ 46 Zutritts- und Zugangsmittel
§ 47 Abnahmen und Wiederholungsprüfungen
§ 48 Lauschabwehrprüfungen

Abschnitt VIII: Einsatz von Informationstechnik

§ 49 Allgemeine Grundsätze
§ 50 Freigabe des Betriebs von VS-IT
§ 51 Zulassung
§ 52 IT-Sicherheitsfunktionen
§ 53 Schutz von VS-Übertragungseinrichtungen, -leitungen und -verteilern
§ 54 Handhabung von Datenträgern und IT-Produkten für unkryptierte Verschlusssachen
§ 55 Übertragung von Verschlusssachen über technische Kommunikationsverbindungen
§ 56 Vernichtung und Aussonderung von Datenträgern und registrierten IT-Produkten
§ 57 Abstrahlschutzmaßnahmen
§ 58 Zusammenschaltung von VS-IT

Abschnitt IX: Kryptopersonal und Handhabung von Kryptomitteln

§ 59 Kryptomittel
§ 60 Nationale Verteilerstellen für Kryptomittel
§ 61 Kryptoverwaltung
§ 62 Kryptopersonal

Abschnitt X: Aufrechterhaltung des Geheimschutzes

§ 63 Kontrollen
§ 64 Behandlung von Geheimschutzvorkommnissen
§ 65 Verhalten in außergewöhnlichen Gefahrenlagen

Abschnitt XI: Abschließende Regelungen

§ 66 Schlussbestimmungen
§ 67 Inkrafttreten

Abschnitt I: Allgemeine Bestimmungen

§ 1 Anwendungsbereich

(1) Die Verschlusssachenanweisung richtet sich an Bundesbehörden und bundesunmittelbare öffentlich-rechtliche Einrichtungen (Dienststellen), die mit Verschlusssachen arbeiten, sowie an dort tätige Personen, die Zugang zu Verschlusssachen haben oder eine Tätigkeit ausüben, bei der sie sich Zugang zu Verschlusssachen verschaffen können. Dienststellen wenden in der Zusammenarbeit mit dem Deutschen Bundestag und dem Bundesrat ausschließlich diese Verschlusssachenanweisung an.

(2) Die allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz bei den Nachrichtendiensten des Bundes erlässt die jeweils zuständige oberste Bundesbehörde im Einvernehmen mit dem Bundesministerium des Innern und für Heimat.

(3) Die allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz im nichtöffentlichen Bereich erlässt das Bundesministerium für Wirtschaft und Klimaschutz im Einvernehmen mit dem Bundesministerium des Innern und für Heimat.

(4) Die allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz im Geschäftsbereich des Bundesministeriums der Verteidigung erlässt das Bundesministerium der Verteidigung als militärische Sicherheitsbehörde im Einvernehmen mit dem Bundesministerium des Innern und für Heimat.

§ 2 Begriff der Verschlusssache und Geheimhaltungsgrade

(1) Verschlusssachen sind im öffentlichen Interesse, insbesondere zum Schutz des Wohles des Bundes oder eines Landes, geheimhaltungsbedürftige Tatsachen, Gegenstände oder Erkenntnisse, unabhängig von ihrer Darstellungsform (zum Beispiel Schriftstücke, Zeichnungen, Karten, Fotokopien, Lichtbildmaterial, elektronische Dateien und Datenträger, elektrische Signale, Geräte, technische Einrichtungen oder das gesprochene Wort). Geheimhaltungsbedürftig im öffentlichen Interesse können auch Geschäfts-, Betriebs-, Erfindungs-, Steuer- oder sonstige private Geheimnisse oder Umstände des persönlichen Lebensbereichs sein.

(2) Verschlusssachen werden entsprechend ihrer Schutzbedürftigkeit von einer Dienststelle oder auf deren Veranlassung nach § 4 Absatz 2 Sicherheitsüberprüfungsgesetz in folgende Geheimhaltungsgrade eingestuft:

1. STRENG GEHEIM, wenn die Kenntnisnahme durch Unbefugte den Bestand oder lebenswichtige Interessen der Bundesrepublik Deutschland oder eines ihrer Länder gefährden kann,
2. GEHEIM, wenn die Kenntnisnahme durch Unbefugte die Sicherheit der Bundesrepublik Deutschland oder eines ihrer Länder gefährden oder ihren Interessen schweren Schaden zufügen kann,
3. VS-VERTRAULICH, wenn die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder schädlich sein kann,

4. VS-NUR FÜR DEN DIENSTGEBRAUCH, wenn die Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein kann.

(3) Der Geheimhaltungsgrad einer Verschlusssache bleibt auch bestehen, wenn sie unrechtmäßig bekannt geworden ist.

§ 3 Allgemeine Grundsätze

(1) Von einer Verschlusssache dürfen nur Personen Kenntnis erhalten, die auf Grund ihrer Aufgabenerfüllung von ihr Kenntnis haben müssen. Keine Person darf über eine Verschlusssache umfassender oder eher unterrichtet werden, als dies aus Gründen der Aufgabenerfüllung notwendig ist. Es gilt der Grundsatz „Kenntnis nur, wenn nötig".

(2) Eine Person, die Zugang zu VS-VERTRAULICH oder höher eingestuften Verschlusssachen erhalten soll oder ihn sich verschaffen kann, ist zuvor einer Sicherheitsüberprüfung nach dem Sicherheitsüberprüfungsgesetz zu unterziehen, es sei denn, sie hat Zugang zu Verschlusssachen kraft Amtes nach § 2 Absatz 3 Satz 1 Nummer 1 oder 2 Sicherheitsüberprüfungsgesetz.

(3) Jeder, dem eine Verschlusssache anvertraut oder zugänglich gemacht worden ist, trägt ohne Rücksicht darauf, wie die Verschlusssache zu seiner Kenntnis oder in seinen Besitz gelangt ist, die persönliche Verantwortung für ihre vorschriftsmäßige Behandlung.

§ 4 Verpflichtung, Ermächtigung und Zulassung

(1) Bevor eine Person Zugang zu Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH erhält, ist sie auf Anlage V zu verpflichten. Dabei ist ihr gegen Empfangsbestätigung ein Exemplar der Anlage V zugänglich zu machen.

(2) Bevor eine Person Zugang zu VS-VERTRAULICH oder höher eingestuften Verschlusssachen erhält, ist sie durch den Geheimschutzbeauftragten zu ermächtigen. Dabei ist sie über die besonderen Bestimmungen des Geheimschutzes zu belehren, in erforderlichem Umfang auf den Geheimschutz zu verpflichten und über Anbahnungs- und Anwerbemethoden ausländischer Nachrichtendienste sowie die Möglichkeit straf- und disziplinarrechtlicher Ahndung oder arbeitsrechtlicher Maßnahmen bei Verstößen gegen die Geheimhaltungsvorschriften zu unterrichten. Die Belehrung und Unterrichtung soll spätestens nach fünf Jahren erneut erfolgen.

(3) Bevor einer Person, die nicht nach Absatz 2 ermächtigt ist, eine Tätigkeit übertragen wird, bei der sie sich Zugang zu VS-VERTRAULICH oder höher eingestuften Verschlusssachen verschaffen kann, ist sie durch den Geheimschutzbeauftragten hierfür zuzulassen. Dabei ist sie über die besonderen Bestimmungen des Geheimschutzes zu belehren, in erforderlichem Umfang auf den Geheimschutz zu verpflichten und über Anbahnungs- und Anwerbemethoden ausländischer Nachrichtendienste sowie die Möglichkeit straf- und disziplinarrechtlicher Ahndung oder arbeitsrechtlicher Maßnahmen bei Verstößen gegen die Geheimhaltungsvorschriften zu unterrichten. Die Belehrung und Unterrichtung soll spätestens nach fünf Jahren erneut erfolgen. Personen, die sich Zugang zu Verschlusssachen verschaffen können, können insbesondere Personen sein, die

1. als Boten oder Kuriere Verschlusssachen befördern (VS-Bote / VS-Kurier),
2. VS-Verwahrgelasse oder Sicherheitsbereiche bewachen,

3. Einbruch- oder Überfallmeldeanlagen zum Schutze von Verschlusssachen installieren, warten oder instandsetzen,
4. Schlüssel oder Zahlenkombinationen zu VS-Verwahrgelassen, VS-Schlüssel-behältern, Einbruch- oder Überfallmeldeanlagen zum Schutze von Verschlusssachen verwalten,
5. als IT-Wartungspersonal oder Administratoren von VS-IT eingesetzt sind.

(4) Ermächtigten und zugelassenen Personen sind gegen Empfangsbestätigung die einschlägigen Strafvorschriften und die für ihre Tätigkeit erforderlichen Vorschriften zum Schutz von Verschlusssachen zugänglich zu machen und gegebenenfalls ein VS-Quittungsbuch auszuhändigen. Ermächtigungen, Zulassungen und ihre Befristung sind nach Muster der Anlage VIII zu dokumentieren.

(5) Ermächtigten Personen ist bei Bedarf eine Konferenzbescheinigung nach Muster der Anlage VIII über ihre Ermächtigung auszustellen.

(6) Entfällt die dienstliche Notwendigkeit für eine Ermächtigung oder Zulassung, ist diese aufzuheben oder auf den notwendigen Umfang einzuschränken. Ermächtigungen und Zulassungen sind aufzuheben, wenn ein Sicherheitsrisiko festgestellt wird. Ermächtigungen und Zulassungen erlöschen spätestens bei Ausscheiden der betroffenen Person aus der Dienststelle. Die VS-Registratur ist über Ermächtigungen und Zulassungen sowie deren Erweiterung, Einschränkung, Aufhebung oder Erlöschen zu unterrichten.

(7) Personen, deren Ermächtigung oder Zulassung aufgehoben wird oder erlischt, sind verpflichtet, Verschlusssachen, die sich in ihrem Besitz befinden, und gegebenenfalls das VS-Quittungsbuch unaufgefordert abzugeben und darüber eine Erklärung nach Muster der Anlage VIII zu unterschreiben. Dies gilt im Falle der Einschränkung der Ermächtigung oder Zulassung entsprechend.

(8) Bei Einschränkung, Aufhebung oder Erlöschen der Ermächtigung oder Zulassung ist die betroffene Person auf das Fortbestehen der Geheimschutzpflichten hinzuweisen.

§ 5 Mitwirkende Behörden

(1) Das Bundesamt für Sicherheit in der Informationstechnik

1. gibt zur Umsetzung dieser Verschlusssachenanweisung Technische Leitlinien heraus, die der Zustimmung des Bundesministeriums des Innern und für Heimat bedürfen, in ihrer jeweils gültigen Fassung zu beachten sind und von denen nur im Ausnahmefall im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik abgewichen werden kann,
2. berät bei der Umsetzung dieser Verschlusssachenanweisung und der Technischen Leitlinien nach Nummer 1,
3. führt technische Prüfungen sowie Fortbildungen durch,
4. macht in Abstimmung mit dem Bundesministerium des Innern und für Heimat Vorgaben, welche technischen Mittel und Dienstleister vor dem Einsatz einer Eignungsprüfung zu unterziehen sind, und stellt Eignungsfeststellungen nach einem vom Bundesamt für Sicherheit in der Informationstechnik im Einvernehmen mit dem Bundesministerium des Innern und für Heimat festgelegten Verfahren aus,

5. erteilt Zulassungen für IT-Sicherheitsprodukte nach einem vom Bundesamt für Sicherheit in der Informationstechnik im Einvernehmen mit dem Bundesministerium des Innern und für Heimat festgelegten Verfahren,
6. berät bei der Auswahl von VS-IT und technischen Komponenten, sofern keine zugelassenen IT-Sicherheitsprodukte nach Nummer 5 verfügbar sind und
7. unterrichtet unverzüglich alle Dienststellen über Erkenntnisse, die für den Schutz von dort befindlichen Verschlusssachen oder die Aufrechterhaltung des dortigen Geheimschutzes von Bedeutung sein können.

(2) Das Bundesamt für Sicherheit in der Informationstechnik kann zu seiner Aufgabenerfüllung andere Stellen einbeziehen. Die Einbeziehung privater Stellen bedarf der vorherigen Billigung des Bundesministeriums des Innern. Bei Einbeziehung öffentlicher Stellen ist das Bundesministerium des Innern und für Heimat über die Einbeziehung unverzüglich zu informieren. Die Verantwortung des Bundesamtes für Sicherheit in der Informationstechnik für die ordnungsgemäße Aufgabenerfüllung bleibt von der Einbeziehung unberührt.

(3) Das Bundesamt für Verfassungsschutz, das Bundesamt für den Militärischen Abschirmdienst und der Bundesnachrichtendienst teilen dem Bundesamt für Sicherheit in der Informationstechnik nichtpersonenbezogene Erkenntnisse, die für den Schutz von Verschlusssachen oder die Aufrechterhaltung des Geheimschutzes von Bedeutung sein können, unverzüglich mit. Das gilt nicht, soweit die Erkenntnisse einem Weitergabeverbot unterliegen. § 23 des Bundesverfassungsschutzgesetzes gilt entsprechend. Sofern sich die Erkenntnisse auf den Geheimschutz in der Wirtschaft beziehen, ist auch das Bundesministerium für Wirtschaft und Klimaschutz unverzüglich zu informieren.

§ 6 Mehrschichtige Sicherheit

Bei der Handhabung von Verschlusssachen werden technische und organisatorische Maßnahmen getroffen, die in ihrem Zusammenwirken die Risiken eines Angriffs reduzieren und im Falle eines erfolgreichen Angriffs die negativen Folgen begrenzen sollen. Die Sicherheitsmaßnahmen berücksichtigen die Aspekte Prävention, Detektion und Reaktion.

Abschnitt II: Geheimschutzorganisation und Geheimschutzdokumentation

§ 7 Dienststellenleitung

Die Dienststellenleitung ist innerhalb ihres Zuständigkeitsbereiches für die Umsetzung dieser Verschlusssachenanweisung verantwortlich und hat die Voraussetzungen zur Gewährleistung des materiellen Geheimschutzes zu schaffen. Sie kann ihre Aufgaben ganz oder teilweise auf Mitarbeiter ihrer Dienststelle übertragen.

§ 8 Geheimschutzbeauftragte

(1) Dienststellen, die VS-VERTRAULICH oder höher eingestufte Verschlusssachen handhaben, sollen Geheimschutzbeauftragte und zur Vertretung berechtigte Personen bestellen. Andernfalls nehmen die Dienststellenleitungen die Aufgaben der Geheimschutzbeauftragten wahr.

(2) Dienststellen, die ausschließlich VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte Verschlusssachen handhaben, können Geheimschutzbeauftragte und zur Vertretung be-

rechtigte Personen bestellen. Andernfalls nehmen die Dienststellenleitungen die Aufgaben der Geheimschutzbeauftragten wahr.

(3) Geheimschutzbeauftragte sorgen für die Umsetzung dieser Verschlusssachenanweisung und beraten die Dienststellenleitungen in allen Fragen des Geheimschutzes. Geheimschutzbeauftragte haben ein unmittelbares Vortragsrecht bei den Dienststellenleitungen. Geheimschutzbeauftragte sind bei allen geheimschutzrelevanten Maßnahmen zu beteiligen. Innerhalb der Dienststellen können besonders beauftragte Mitarbeiter (zum Beispiel Geheimschutzbeamte) zur Unterstützung der Geheimschutzbeauftragten bestellt werden.

(4) Geheimschutzbeauftragte oder besonders beauftragte Mitarbeiter haben die mit der Handhabung von Verschlusssachen betrauten Personen durch geeignete Maßnahmen mit den Vorschriften dieser Verschlusssachenanweisung sowie anderen einschlägigen Vorschriften zum Schutz von Verschlusssachen vertraut zu machen.

§ 8a Risikomanagement

Geheimschutzbeauftragte tragen durch angemessene Sicherheitsmaßnahmen dafür Sorge, Risiken für den Schutz von Verschlusssachen zu reduzieren und Restrisiken zu identifizieren, die mit den getroffenen Maßnahmen nicht abgewehrt werden können. Ein solches Risikomanagement wird als fortlaufender Prozess verstanden, in dem Planung, Umsetzung, Überwachung und Verbesserung von angemessenen Sicherungsmaßnahmen kontinuierlich stattfinden. Eine Sicherheitsmaßnahme ist angemessen, wenn der Aufwand zur Umsetzung der Maßnahme und das verbleibende Restrisiko in einem ausgewogenen Verhältnis stehen. Die Bewertung der Angemessenheit erfolgt auf der Grundlage einer Risikoanalyse.

§ 9 IT-Sicherheitsbeauftragte

IT-Sicherheitsbeauftragte unterstützen und beraten die Geheimschutzbeauftragten in allen Fragen des Einsatzes von Informationstechnik zur Handhabung von Verschlusssachen einschließlich deren Übertragung (VS-IT).

§ 10 VS-Registratoren

Dienststellen, die VS-VERTRAULICH oder höher eingestufte Verschlusssachen handhaben, bestellen VS-Registratoren und zur Vertretung berechtigte Personen, die im Rahmen der Verschlusssachenanweisung für die ordnungsgemäße Verwaltung dieser Verschlusssachen Sorge tragen.

§ 11 Qualifikation

Die in §§ 8 bis 10 genannten Personen müssen über die zur Erfüllung ihrer Aufgaben erforderliche Fachkunde verfügen.

§ 12 Erstellung der Geheimschutzdokumentation

(1) Jede Dienststelle, die nicht nur gelegentlich mit Verschlusssachen arbeitet, führt eine Geheimschutzdokumentation, die

1. Verweise auf alle in diesem Zusammenhang zu beachtenden Vorschriften,
2. eine Auflistung der Dienstposten, auf denen eine sicherheitsempfindliche Tätigkeit im Sinne des Sicherheitsüberprüfungsgesetzes ausgeübt wird,

3. eine Auflistung der ermächtigten und zugelassenen Personen,
4. die VS-Sicherungsdokumentation mit den sich aus Anlage II ergebenden Inhalten,
5. die VS-IT-Dokumentation, mit den sich aus Anlage II ergebenden Inhalten,
6. Nachweise über durchgeführte Kontrollen und Überprüfungen und
7. Berichte über Geheimschutzvorkommnisse

umfasst.

(2) Die Geheimschutzdokumentation ist bei allen geheimschutzrelevanten Änderungen zu aktualisieren, mindestens aber alle drei Jahre auf Aktualität, Vollständigkeit und Erforderlichkeit bestehender und noch zu treffender Geheimschutzmaßnahmen zu überprüfen.

(3) Die Geheimschutzbeauftragten geben den Mitarbeitern ihrer Dienststelle die für die Dienststelle getroffenen, für die Handhabung von Verschlusssachen relevanten Regelungen in geeigneter Weise bekannt.

Weiteres zu diesem Abschnitt ist den Anlagen I und II zu entnehmen.

Abschnitt III (aufgelöst)

§§ 13, 14 (weggefallen)

Abschnitt IV: Einstufung und Befristung

§ 15 Einstufung

(1) Die Dienststelle, die eine Verschlusssache erstellt oder deren Erstellung veranlasst, oder der Rechtsnachfolger dieser Dienststelle ist der Herausgeber der Verschlusssache. Der Herausgeber legt nach Maßgabe von § 4 Absatz 2 Sicherheitsüberprüfungsgesetz den Geheimhaltungsgrad der Verschlusssache fest. Von einer Einstufung als Verschlusssache ist nur Gebrauch zu machen, soweit dies notwendig ist.

(2) Die Dienststelle kann Richtlinien zur Einstufung von Verschlusssachen für häufiger vorkommende Fälle festlegen.

(3) Weiteres ist der Anlage III zu entnehmen.

§ 16 Einstufungsfrist

(1) Die Einstufung einer Verschlusssache des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH ist auf 30 Jahre befristet. Der Herausgeber kann unter Berücksichtigung der Begründung für die Einstufung eine kürzere Einstufungsfrist bestimmen.

(2) Der Herausgeber hat für VS-VERTRAULICH oder höher eingestufte Verschlusssachen den Zeitpunkt des Ablaufs der Einstufung zu bestimmen. Die Einstufungsfrist hat sich hierbei an der aus der Begründung für die Einstufung resultierenden voraussichtlichen Dauer der Schutzbedürftigkeit der Verschlusssache zu orientieren. Die Einstufungsfrist soll 30 Jahre nicht überschreiten. Soweit die Begründung für die Einstufung eine Einstufungsfrist einzelner Verschlusssachen oder pauschal für die in einem bestimmten Bereich entstehenden Ver-

schlusssachen über einen Zeitraum von 30 Jahren hinaus gebietet, ist dies zu begründen und so zu vermerken, dass dies jederzeit erkennbar ist. Eine solche Abweichung bedarf der Zustimmung der zuständigen obersten Bundesbehörde.

(3) Die Einstufung endet mit Ablauf des Jahres, in welches das Fristende fällt.

(4) Die Dienststelle kann Richtlinien zur Bestimmung der Einstufungsfrist von Verschlusssachen für häufiger vorkommende Fälle festlegen.

§ 17 Verlängerung der Einstufungsfrist

(1) Die nach § 16 Absatz 1 festgelegte Einstufungsfrist von Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH kann nicht verlängert werden.

(2) Soweit die Schutzbedürftigkeit einer Verschlusssache des Geheimhaltungsgrades VS-VERTRAULICH oder höher nach den Vorschriften des Sicherheitsüberprüfungsgesetzes über die nach § 16 Absatz 2 festgelegte Einstufungsfrist hinaus fortbesteht, hat der Herausgeber eine Verlängerung der Einstufungsfrist für einzelne Verschlusssachen oder pauschal für die in einem bestimmten Bereich entstandenen Verschlusssachen zu verfügen. Die Verlängerung ist zu begründen und so zu vermerken, dass diese und die verfügende Stelle jederzeit erkennbar sind. Die Verlängerung soll jeweils 30 Jahre nicht überschreiten. Soweit die Begründung für die Einstufung die Verlängerung der Einstufungsfrist einzelner Verschlusssachen oder pauschal für die in einem bestimmten Bereich entstandenen Verschlusssachen über einen Zeitraum von 30 Jahren hinaus gebietet, ist dies zu begründen und so zu vermerken, dass dies und die verfügende Stelle jederzeit erkennbar sind. Eine solche Abweichung bedarf der Zustimmung der zuständigen obersten Bundesbehörde.

(3) Das Bundesarchiv betreibt eine Nachweisdatenbank für Verschlusssachen, deren Einstufungsfristen verlängert wurden. Grundsätzlich ist jedem Empfänger von Verschlusssachen des Bundes lesender Zugriff auf diese Datenbank zu gewähren. Die Verlängerung der Einstufungsfrist ist dem Bundesarchiv rechtzeitig vor Fristablauf zur Erfassung in der Nachweisdatenbank mitzuteilen. Die Empfänger von Verschlusssachen, deren Einstufungsfrist abgelaufen ist, haben dort zu prüfen, ob die Einstufungsfrist verlängert wurde. Verschlusssachen, die nicht in der Nachweisdatenbank erfasst sind, sind nach Ablauf der Einstufungsfrist offenes Schriftgut.

(4) Nichtöffentliche Empfänger amtlich geheim gehaltener Verschlusssachen sind von dem Verfahren nach Absatz 3 Satz 2 bis 5 ausgenommen. Sie sind als Empfänger von Verschlusssachen schriftlich über die Verlängerungen von Einstufungsfristen zu benachrichtigen. Die Benachrichtigungen sind nachzuweisen.

(5) Absatz 3 gilt nicht für die Verlängerung der Einstufungsfrist von auf amtliche Veranlassung geheim gehaltenen Verschlusssachen, für die eine Einstufungsfrist bestimmt ist. Über die Verlängerungen der Einstufungsfristen dieser Verschlusssachen hat der Herausgeber alle Empfänger schriftlich zu benachrichtigen. Die Benachrichtigungen sind nachzuweisen.

§ 18 Änderung der Einstufung

(1) Ändert sich die Schutzbedürftigkeit einer Verschlusssache, hat der Herausgeber den Geheimhaltungsgrad dieser Verschlusssache entsprechend herauf- oder herabzusetzen. Über die Änderung hat der Herausgeber alle Empfänger der Verschlusssache unverzüglich schriftlich zu benachrichtigen.

(2) Eine nachträgliche Einstufung von nicht eingestuften Informationen sowie eine Heraufstufung von VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften Verschlusssachen ist grundsätzlich nicht zulässig. Ausnahmen sind nur im Benehmen mit den Geheimschutzbeauftragten zulässig.

(3) Die Änderung des Geheimhaltungsgrades lässt die Einstufungsfrist nach § 16 unberührt.

(4) Die Änderung des Geheimhaltungsgrades einer Verschlusssache ist so zu vermerken, dass die Änderung bei der Handhabung der Verschlusssache jederzeit erkennbar ist. Sind Verschlusssachen des Geheimhaltungsgrades VS-VERTRAULICH oder höher betroffen, ist die Änderung im VS-Bestandsverzeichnis des Herausgebers und der Empfänger nachzuweisen.

§ 19 Aufhebung der Einstufung

(1) Entfällt die Geheimhaltungsbedürftigkeit einer Verschlusssache vor Ablauf der Einstufungsfrist, hat der Herausgeber die Einstufung aufzuheben. Die Aufhebung der Einstufung ist so zu vermerken, dass diese und die verfügende Stelle jederzeit erkennbar sind. Im Falle von Verschlusssachen des Geheimhaltungsgrades VS-VERTRAULICH oder höher hat der Herausgeber alle Empfänger der Verschlusssache oder deren Rechtsnachfolger schriftlich zu benachrichtigen. Die Aufhebung der Einstufung ist in diesem Falle zusätzlich im VS-Bestandsverzeichnis des Herausgebers und der Empfänger nachzuweisen.

(2) Einstufungen sind aufgehoben, sofern auf der Verschlusssache keine längere oder kürzere Frist bestimmt ist (vergleiche §§ 16 und 17)

1. für die Vorgänge der Jahre 1949 bis 1959 mit Ablauf des 31. Dezember 2012,
2. für die Vorgänge der Jahre 1960 bis 1994 bis zum 1. Januar 2025 - dabei sind beginnend mit dem Ablauf des Jahres 2013 mindestens drei Jahrgänge je Kalenderjahr in chronologischer Reihenfolge auf Offenlegung zu prüfen,
3. für die Vorgänge der Jahre ab 1995 nach 30 Jahren.

Für Empfänger von Verschlusssachen, die nach § 17 Absatz 3 in der VS-Nachweisdatenbank zu prüfen haben, ob es sich bei diesen um offenes Schriftgut handelt, ersetzt diese Prüfung Benachrichtigungen nach Absatz 1 Satz 3.

Für nichtöffentliche Empfänger amtlich geheim gehaltener Verschlusssachen, die nach § 17 Absatz 4 als Empfänger von Verschlusssachen schriftlich über die Verlängerung der Fristen nach Satz 1 zu benachrichtigen sind, entfallen Benachrichtigungen nach Absatz 1 Satz 3.

(3) Ausgenommen von der Fristenregelung nach Absatz 2 sind auf amtliche Veranlassung geheim gehaltene Verschlusssachen.

Abschnitt V: Handhabung von Verschlusssachen

§ 20 Herstellung und Kennzeichnung

(1) Die Herstellung von VS-VERTRAULICH oder höher eingestuften Verschlusssachen ist nur an den hierfür bestimmten Stellen mit den dort vorgesehenen Mitteln zulässig.

(2) Bei der Herstellung ist eine Verschlusssache so zu kennzeichnen, dass bei ihrer Handhabung während der gesamten Dauer ihrer Einstufung jederzeit erkennbar sind:

1. der Geheimhaltungsgrad,
2. der Herausgeber,
3. das Datum der Verschlusssache,
4. bei VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften Verschlusssachen das bei der Herstellung festgelegte Ende der Einstufungsfrist, sofern dieses die Regelfrist von 30 Jahren nach § 16 Absatz 1 unterschreitet,
5. bei VS-VERTRAULICH oder höher eingestuften Verschlusssachen das bei der Herstellung festgelegte Ende der Einstufungsfrist mit dem Zusatz „Die Einstufung endet mit Ablauf des Jahres...“,
6. bei VS-VERTRAULICH oder höher eingestuften Verschlusssachen ein geeignetes individuelles Merkmal (zum Beispiel Geschäftszeichen und Tagebuchnummer), ergänzt um das Kürzel des Geheimhaltungsgrades nach Absatz 4, anhand dessen sich in Verbindung mit dem VS-Bestandsverzeichnis die Handhabung der Verschlusssache jederzeit lückenlos ermitteln lässt,
7. bei jeder Ausfertigung einer als VS-VERTRAULICH oder höher eingestuften Verschlusssache eine fortlaufende Nummer und der jeweilige Empfänger und
8. die Seiten- und Gesamtseitenzahl.

(3) Der Herausgeber kann weitere Vorgaben zum Schutz und zur Handhabung von Verschlusssachen durch Warn- und Sperrvermerke nach Anlage IV festlegen.

(4) Geheimhaltungsgrade sind auszuschreiben, soweit in dieser Vorschrift nichts anderes bestimmt ist oder die Beschaffenheit einer Verschlusssache das nicht zulässt. In diesen Fällen sind folgende Abkürzungen zu verwenden:

VS-NUR FÜR DEN DIENSTGEBRAUCH	VS-NfD
VS-VERTRAULICH	VS-Vertr.
GEHEIM	Geh.
STRENG GEHEIM	Str. Geh.

(5) Der Betreff einer Verschlusssache soll so formuliert werden, dass er für sich genommen nicht geheimhaltungsbedürftig ist.

(6) Besteht eine Verschlusssache aus mehreren, unterschiedlich eingestuften Teilen (zum Beispiel Anlagen oder Komponenten), sind alle Teile mit ihrem jeweiligen Geheimhaltungsgrad und die Verschlusssache in ihrer Gesamtheit nach dem höchsten Geheimhaltungsgrad zu kennzeichnen. Anfang und Ende der einzelnen Teile müssen erkennbar sein.

(7) Datenträger, auf denen Verschlusssachen unverschlüsselt gespeichert sind, sind mit dem Geheimhaltungsgrad der höchsten Einstufung der darauf gespeicherten Verschlusssachen zu

kennzeichnen. Datenträger, auf denen Verschlusssachen ausschließlich vorschriftsgemäß verschlüsselt gespeichert sind, müssen nicht gekennzeichnet werden.

(8)Die verbindliche Gestaltung der Kennzeichnung von Verschlusssachen, VS-Bestandsverzeichnissen sowie VS-Schriftgutbehältern und Behältern von VS-Datenträgern ist der Anlage IV sowie den Mustern der Anlage VIII zu entnehmen. Die Kennzeichnung gilt auch für elektronische Verschlusssachen. Von der Kennzeichnung sind VS-Transportbehälter ausgenommen. Lässt die Beschaffenheit einer Verschlusssache eine solche Kennzeichnung nicht zu, ist sinngemäß zu verfahren. Näheres zur zusätzlichen Kennzeichnung von elektronischen Verschlusssachen (zum Beispiel anhand von Metadaten) regelt eine Technische Leitlinie des Bundesamtes für Sicherheit in der Informationstechnik.

§ 21 Verwaltung und Nachweis von Verschlusssachen

(1) VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte Verschlusssachen können, soweit sie nicht Bestandteil höher eingestufter Verschlusssachen sind, unter Beachtung des Grundsatzes „Kenntnis nur, wenn nötig“ in offenen Registraturen verwaltet werden.

(2) VS-VERTRAULICH oder höher eingestufte Verschlusssachen sind in VS-Registraturen mittels geeigneter Verfahren so zu verwalten, dass ihre Existenz, ihre Einstufung einschließlich der Einstufungsfrist, ihr Verbleib, die Kenntnisnahmen, ihre Vervielfältigung und deren Verbleib sowie ihre Vernichtung nachvollziehbar sind (Nachweisführung). Für Verschlusssachen ausländischer Staaten und über- oder zwischenstaatlicher Organisationen können andere Regelungen nach Anlage VII dieser Verschlusssachenanweisung gelten.

(3) Die Nachweisführung von VS-VERTRAULICH oder höher eingestufter Verschlusssachen kann in Papier- oder in elektronischer Form erfolgen. Sie muss Schutz vor unbemerkter Veränderung, Verlust und Verfälschung bieten. Die papiergestützte Nachweisführung von Verschlusssachen erfolgt anhand von VS-Bestandsverzeichnissen, VS-Quittungsbüchern, VS-Begleitzetteln, VS-Empfangsscheinen, VS-Übergabeprotokollen und VS-Vernichtungsprotokollen. Verbindliche Muster für diese Nachweise sind der Anlage VIII zu entnehmen. Die elektronische Nachweisführung von Verschlusssachen erfolgt anhand von VS-Registratursystemen. Diese unterliegen als VS-IT im Sinne des Abschnitts VIII den dortigen Bestimmungen.

(4) VS-Datenträger, ihr Verbleib und ihre Vernichtung sind in einem gesonderten VS-Bestandsverzeichnis nachzuweisen. Für die eindeutige Identifizierbarkeit genügt die Angabe eines Ordnungskriteriums (zum Beispiel laufende Nummer).

(5) VS-Bestandsverzeichnisse sind gemäß dem höchsten Geheimhaltungsgrad der in ihnen nachgewiesenen Verschlusssachen einzustufen. Der Zugriff auf das VS-Bestandsverzeichnis ist nur den Geheimschutzbeauftragten, den besonders beauftragten Mitarbeitern und den VS-Registratoren gestattet.

(6) Bei Wechsel eines VS-Registrators ist der Bestand zu überprüfen und ein Bestandsbericht (Übergabeprotokoll) zu fertigen.

(7) VS-Nachweise sind mindestens fünf Jahre aufzubewahren. Für VS-Quittungsbücher beginnt die Frist mit der letzten Eintragung, für VS-Empfangsscheine, VS-Begleitzettel, VS-Übergabeprotokolle und VS-Vernichtungsprotokolle mit der Ausstellung. Für VS-Bestandsverzeichnisse beginnt die Frist, wenn alle in ihnen nachgewiesenen Verschlusssachen

1. auf den Geheimhaltungsgrad VS-NUR FÜR DEN DIENSTGEBRAUCH herabgestuft,
2. offengelegt (Aufhebung der Einstufung) oder
3. vernichtet

worden sind.

Wenn in einem VS-Bestandsverzeichnis nur noch wenige Verschlusssachen nachgewiesen werden, können die Einträge unter Beibehaltung ihrer Tagebuchnummer in ein anderes VS-Bestandsverzeichnis übertragen werden und sind nur dort nachzuweisen. In diesem Fall beginnt die Aufbewahrungsfrist für das abgeschlossene VS-Bestandsverzeichnis mit der Übertragung der Einträge. Nach Ablauf der Frist sind VS-Nachweise zu vernichten.

(8) Weiteres ist der Anlage IV zu entnehmen.

§ 22 Vervielfältigung von Verschlusssachen

(1) Vervielfältigung von Verschlusssachen ist die absichtliche Herstellung von weiteren Exemplaren einer Ausfertigung einer Verschlusssache, unabhängig von der Darstellungsform (insbesondere durch fotomechanische Kopie, Scan, Abdruck einer elektronisch dargestellten Verschlusssache, elektronische Kopie von Dateien, elektronischer Versand, Auszug und Nachbau).

(2) Jede Vervielfältigung von VS-VERTRAULICH oder höher eingestuften Verschlusssachen ist mit einer fortlaufenden Nummer und dem jeweiligen Empfänger so zu kennzeichnen, dass sie als weiteres Exemplar einer Verschlusssache (Kopie) eindeutig erkennbar ist und der Original-Verschlusssache zugeordnet werden kann. Jede Vervielfältigung von VS-VERTRAULICH oder höher eingestuften Verschlusssachen ist als weiteres Exemplar zudem nach § 21 unverzüglich zu registrieren.

(3) In Dienststellen, in denen VS-VERTRAULICH oder höher eingestufte Verschlusssachen hergestellt oder vervielfältigt werden, sollen hierfür bestimmte Stellen mit ermächtigtem Bedienungspersonal festgelegt werden. Soweit dies nicht geschieht, sind Vervielfältigungen dieser Verschlusssachen durch die VS-Registratoren zu fertigen.

(4) Die Vervielfältigung von STRENG GEHEIM eingestuften Verschlusssachen bedarf zusätzlich der schriftlichen Zustimmung des Herausgebers. Die Zustimmung ist im VS-Bestandsverzeichnis zu vermerken.

(5) Werden in VS-IT Kopien von den dort registrierten Verschlusssachen als Backup-Daten zur Sicherung der Verfügbarkeit benötigt, sind diese in einem gesonderten Bestandsverzeichnis in der Art nachzuweisen, dass jederzeit feststellbar ist, welche Verschlusssachen als Kopie darin gespeichert sind.

§ 23 Aufbewahrung von Verschlusssachen

(1) Die dauerhafte Aufbewahrung von VS-VERTRAULICH oder höher eingestuften Verschlusssachen hat in VS-Registraturen zu erfolgen. Die Aufbewahrung außerhalb der VS-Registratur ist nur für den Zeitraum zulässig, für den ein fortgesetzter Zugriff des Bearbeiters auf die Verschlusssache notwendig ist. Die VS-Registratoren erkundigen sich in angemessenen Zeitabständen, ob diese Voraussetzung weiterbesteht. VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte Verschlusssachen können, soweit sie nicht Bestandteil

höher eingestufter Verschlusssachen sind, unter Beachtung des Grundsatzes „Kenntnis nur, wenn nötig“ in einer offenen Registratur dauerhaft aufbewahrt werden.

(2) VS-VERTRAULICH oder höher eingestufte Verschlusssachen sind bei Nichtgebrauch in einem VS-Verwahrgelass einzuschließen. Dies gilt für STRENG GEHEIM eingestufte Verschlusssachen bereits bei kurzer Abwesenheit der die Verschlusssache bearbeitenden oder verwaltenden Personen. VS-VERTRAULICH oder GEHEIM eingestufte Verschlusssachen können bei einer kurzen Abwesenheit der die Verschlusssache bearbeitenden oder verwaltenden Personen während der Arbeitszeit im VS-Arbeitsbereich verbleiben, sofern die Zimmertür mit einem Sicherheitsschloss verschlossen ist. VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte Verschlusssachen sind bei Nichtgebrauch in verschlossenen Behältern oder abgeschlossenen Räumen aufzubewahren.

(3) Außerhalb der Arbeitszeit sind VS-Verwahrgelasse zu bewachen oder durch eine Alarmanlage technisch zu überwachen. In beiden Fällen ist sicherzustellen, dass Unbefugte am Zugriff auf die darin gelagerten Verschlusssachen gehindert werden und dass ein Zugriff Unbefugter erkannt und hilfeleistenden Stellen gemeldet wird. Bei GEHEIM oder VS-VERTRAULICH eingestuften Verschlusssachen kann eine Bewachung beziehungsweise technische Überwachung des VS-Verwahrgelasses unterbleiben, wenn das Gebäude oder der Gebäudeteil, in dem sich das Verwahrgelass befindet, bewacht oder technisch überwacht ist. Näheres über Art und Umfang der Bewachung und technischen Überwachung legen die Geheimschutzbeauftragten unter Berücksichtigung des Schutzziels für die jeweiligen VS-Verwahrgelasse und Gebäude fest.

§ 24 Grundsätze zur Weitergabe von Verschlusssachen

(1) Weitergabe ist

1. die Weitergabe von Hand zu Hand,
2. die Beförderung durch Boten,
3. der Versand durch Kuriere,
4. der Versand durch private Zustelldienste,
5. die mündliche Mitteilung,
6. die Übertragung über technische Kommunikationsverbindungen oder
7. die Bereitstellung in einem Kommunikationsnetzwerk.

(2) Jeder hat sich vor der Weitergabe von Verschlusssachen zu vergewissern, dass der vorgesehene Empfänger zur Annahme oder Kenntnisnahme berechtigt ist.

(3) Die Weitergabe von VS-VERTRAULICH oder höher eingestuften Verschlusssachen soll über die VS-Registraturen erfolgen und ist nachzuweisen. Die Weitergabe von STRENG GEHEIM eingestuften Verschlusssachen bedarf der schriftlichen Zustimmung des Herausgebers.

(4) Zwischen zwei getrennt liegenden Gebäuden, die nicht zu einer geschlossenen Gebäudegruppe gehören, sollen Verschlusssachen grundsätzlich mittels technischer Kommunikationsverbindungen nach § 55 übertragen werden. Ist dies nicht möglich, sollen sie durch Kuriere versandt werden. Ist auch dies nicht möglich können Verschlusssachen bis zum Geheimhaltungsgrad GEHEIM durch private Zustelldienste versandt werden.

(5) Die Geheimschutzbeauftragten können besondere Regelungen zur Weitergabe von Verschlusssachen innerhalb einer Gemeinschaft von Geheimnisträgern festlegen.

(6) Weiteres ist der Anlage IV zu entnehmen.

§ 25 Weitergabe an nichtöffentliche Stellen

Die Weitergabe von Verschlusssachen an nichtöffentliche Stellen ist nur zulässig, wenn sie im staatlichen Interesse erforderlich ist (zum Beispiel zur Durchführung eines staatlichen Auftrages oder zur Analyse oder Abwehr von Gefahren für die Sicherheit in der Informationstechnik von Kritischen Infrastrukturen, von sonstigen Unternehmen im staatlichen Interesse oder einer Stelle des Bundes). Für die Weitergabe von Verschlusssachen an nichtöffentliche Stellen gilt unter Beachtung von § 1 Absatz 3 Folgendes:

1. Vor Weitergabe von VS-VERTRAULICH oder höher eingestuften Verschlusssachen sind beim Bundesministerium für Wirtschaft und Klimaschutz Sicherheitsbescheide (Facility Security Clearance, FSC) über die beteiligten nichtöffentlichen Stellen anzufordern. Haben Beschäftigte dieser nichtöffentlichen Stellen ausschließlich in Dienststellen Zugang zu solchen Verschlusssachen gilt dies nur, wenn die Zustimmung des Bundesministeriums für Wirtschaft und Klimaschutz nach § 24 Absatz 2 Sicherheitsüberprüfungsgesetz vorliegt.
2. Bei der Weitergabe von VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften Verschlusssachen ist Anlage V (VS-NfD-Merkblatt) zu beachten.

§ 26 Weitergabe an den Deutschen Bundestag, den Bundesrat, Landesparlamente und -behörden

(1) Die Weitergabe von VS-VERTRAULICH oder höher eingestuften Verschlusssachen an den Deutschen Bundestag, den Bundesrat oder Landesparlamente erfolgt über die zuständige oberste Bundesbehörde grundsätzlich an die VS-Registratur des Empfängers.

(2)Die Weitergabe von Verschlusssachen an ein Land sowie der Zugriff eines Landes auf VS-IT des Bundes und die Teilnahme eines Landes an einem VS-IT-System des Bundes sind nur zulässig, sofern in diesem Land Regelungen zum Schutz von Verschlusssachen entsprechend dieser Verschlusssachenanweisung gelten oder sich das Land zum Schutz von Verschlusssachen entsprechend dieser Verschlusssachenanweisung verpflichtet. Bei VS-IT-Systemen des Bundes ist vor der ersten Nutzung zudem eine Zusicherung des Landes an die für den Betrieb verantwortlichen Dienststelle des Bundes erforderlich, dass deren Anforderungen des Geheimschutzes erfüllt werden.

§ 27 Empfang von Verschlusssachen

(1)Bei Empfang von Verschlusssachen des Geheimhaltungsgrades VS-VERTRAULICH oder höher sind

1. die Sendungen umgehend der VS-Registratur zuzuleiten und nach § 21 zu registrieren,
2. die Integrität, Authentizität und Vollständigkeit der Sendungen zu prüfen und
3. der Empfang mit dem Ergebnis der Prüfung gegenüber der VS-Verwaltung des Absenders unverzüglich zu bestätigen.

(2) Zeigen sich Hinweise auf unbefugte Kenntnisnahme, Unvollständigkeit oder Veränderung, so sind die Geheimschutzbeauftragten und die Absender unverzüglich zu benachrichtigen.

§ 28 Mitnahme von Verschlusssachen außerhalb des Dienstgebäudes

(1) Innerhalb des Bundesgebiets sollen VS-VERTRAULICH oder höher eingestufte Verschlusssachen grundsätzlich im Voraus an eine Dienststelle am Zielort, die selbst Verschlusssachen verwaltet und aufbewahrt, mittels technischer Kommunikationsverbindungen nach § 55 übertragen werden. Ist dies nicht möglich sind die folgenden Absätze bei der persönlichen Mitnahme zu beachten.

(2) Verschlusssachen können außerhalb des Dienstgebäudes oder einer Liegenschaft nur auf Dienstreisen und zu Dienstbesprechungen mitgenommen werden, soweit dies dienstlich notwendig ist und sie angemessen gegen unbefugte Kenntnisnahme und unbefugten Zugriff gesichert werden. Die Mitnahme von VS-VERTRAULICH oder höher eingestuften Verschlusssachen aus anderem Anlass (zum Beispiel zur Bearbeitung in der Privatwohnung) ist unzulässig. In besonderen Fällen können die Geheimschutzbeauftragten Ausnahmen zulassen. Die Mitnahme von VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften Verschlusssachen richtet sich nach Ziffer 7 der Anlage V.

(3) Die Mitnahme von STRENG GEHEIM eingestuften Verschlusssachen bedarf der vorherigen Zustimmung durch die Geheimschutzbeauftragten. Dies gilt ebenso bei der Mitnahme von VS-VERTRAULICH und GEHEIM eingestuften Verschlusssachen in das Ausland.

(4) VS-VERTRAULICH oder höher eingestufte Verschlusssachen sind in einem äußerlich neutralen und verschlossenen VS-Transportbehälter mitzunehmen. An verdeckter Stelle ist die Anschrift der Dienststelle anzubringen. Werden STRENG GEHEIM oder GEHEIM eingestufte Verschlusssachen mitgenommen, soll ein Dienstwagen genutzt werden. Ist dies nicht möglich, sind STRENG GEHEIM eingestufte Verschlusssachen mit mindestens zwei ausreichend ermächtigten oder zugelassenen Personen zu befördern. Verschlusssachen in elektronischer Form sind auf hierfür zugelassener VS-IT oder mit einem zugelassenen Verfahren verschlüsselten Datenträgern mitzunehmen.

(5) Nach außerhalb des Bundesgebiets sind VS-VERTRAULICH oder höher eingestufte Verschlusssachen nach Möglichkeit durch den Kurierdienst des Auswärtigen Amtes an die zuständige Auslandsvertretung voraus zu senden oder mittels technischer Kommunikationsverbindungen nach § 55 zu übertragen und nach Erledigung des Dienstgeschäftes auf demselben Weg zurückzusenden. Ist dies nicht möglich, so versiegelt das Auswärtige Amt beziehungsweise die zuständige Auslandsvertretung die verpackten Verschlusssachen und stellt eine Bescheinigung aus, nach der ihr Inhaber zur Mitnahme des versiegelten Stückes als „Kuriergepäck“ berechtigt ist. Die persönliche Mitnahme von VS-VERTRAULICH oder GEHEIM eingestuften Verschlusssachen ist ohne Mitwirkung des Auswärtigen Amtes gestattet, wenn sich diese in elektronischer Form auf hierfür zugelassener VS-IT oder mit einem zugelassenen Verfahren verschlüsselt auf einem Datenträger befinden. Die persönliche Mitnahme von STRENG GEHEIM eingestuften Verschlusssachen im grenzüberschreitenden Verkehr ist unzulässig.

(6) Bei Mitnahme von Verschlusssachen sind diese ständig in persönlichem Gewahrsam zu halten oder nach § 23 aufzubewahren. Die Aufbewahrung in Hotelzimmern bei persönlicher Abwesenheit, Hotelsafes, Gepäckschließfächern oder in unbesetzten Fahrzeugen ist grundsätzlich unzulässig.

§ 29 Erörterung von Verschlusssachen

(1) Bei der Erörterung von geheimhaltungsbedürftigen Sachverhalten ist der Grundsatz „Kenntnis nur, wenn nötig" zu beachten. Die Erörterung in der Öffentlichkeit ist zu unterlassen.

(2) Sollen Verschlusssachen in Dienstbesprechungen erörtert werden, so ist darauf bei der Einladung unter Angabe des Geheimhaltungsgrades hinzuweisen.

(3) Die entsendenden Dienststellen gewährleisten, dass nur ausreichend ermächtigte Teilnehmer entsandt werden und stellen bei VS-VERTRAULICH oder höher eingestuften Verschlusssachen über die Ermächtigung eine Konferenzbescheinigung nach Muster der Anlage VIII aus, soweit die einladende Stelle dies aus besonderen Gründen für erforderlich hält.

(4) Vor Beginn der Dienstbesprechung hat der Leiter der Veranstaltung auf die Geheimhaltungsbedürftigkeit der Erörterungen hinzuweisen und sich zu vergewissern, dass alle teilnehmenden Personen ausreichend ermächtigt sind.

(5) Aufzeichnungen bedürfen der Zustimmung und sind als Verschlusssachen zu behandeln. Über das Mitführen von Bild- und Tonaufzeichnungsgeräten, mobilen Telekommunikationsgeräten und sonstiger Informationstechnik soll der Leiter der Veranstaltung vor deren Beginn entscheiden.

(6) Bei Erörterung von STRENG GEHEIM oder GEHEIM eingestuften Verschlusssachen, sollen abhörsichere oder abhörgeschützte Räume benutzt werden. Vor Konferenzen auf hoher Ebene oder von besonderer Bedeutung ist bezüglich der notwendigen Abhörschutzmaßnahmen das Bundesamt für Sicherheit in der Informationstechnik rechtzeitig beratend hinzuzuziehen.

§ 30 Grundsätze der Aussonderung von Verschlusssachen

(1) Als VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte Verschlusssachen werden wie nicht eingestuftes Material entsprechend dem Bundesarchivgesetz ausgesondert. Die Vernichtung erfolgt nach § 32.

(2) Nicht mehr benötigte VS-VERTRAULICH oder höher eingestufte Verschlusssachen sind aus dem Bestand der Dienststelle zur Archivierung oder Vernichtung nach den §§ 31 und 32 auszusondern.

§ 31 Archivierung von Verschlusssachen

(1) Dienststellen bieten, soweit gesetzlich nichts anderes bestimmt, ihre nicht mehr benötigten Verschlusssachen der Geheimhaltungsgrade VS-VERTRAULICH oder höher dem Bundesarchiv (Geheimarchiv) nach der VS-Archivrichtlinie (Anlage VI) zur Archivierung an.

(2) Dienststellen, die das Zwischenarchiv des Bundesarchivs nach § 20 der Richtlinie für das Bearbeiten und Verwalten von Schriftgut (Akten und Dokumenten) in Bundesministerien nutzen, sollen ihre nicht mehr laufend benötigten Verschlusssachen dem Bundesarchiv (Geheimarchiv) zur weiteren Aufbewahrung nach der VS-Archivrichtlinie übergeben.

(3) Nachgeordnete Dienststellen mit regionaler Zuständigkeit, für deren Unterlagen nach § 7 des Bundesarchivgesetzes ein Landesarchiv zuständig ist, bieten ihre nicht mehr benötigten Verschlusssachen dem Landesarchiv (Geheimarchiv) zur Archivierung an. Die VS-Archivrichtlinie ist sinngemäß anzuwenden. Soweit kein Geheimarchiv besteht, sind die Ver-

schlusssachen bis zur Aufhebung der Einstufung bei der jeweiligen Dienststelle zu verwahren.

(4) Elektronisch vorliegende Verschlusssachen sind dem zuständigen Archiv in entsprechender Anwendung der VS-Archivrichtlinie zur Übernahme anzubieten. Das technische Verfahren der Übergabe ist zuvor mit dem Archiv abzusprechen. Das Bundesarchiv stellt für die Aussonderung digitaler Unterlagen und deren Archivierung einen Leitfaden zur Verfügung.

§ 32 Vernichtung von Verschlusssachen

(1) Verschlusssachen, die das zuständige Archiv nicht übernimmt, sind zu vernichten. Verschlusssachen sind so zu vernichten, dass der Inhalt weder erkennbar ist, noch erkennbar gemacht werden kann.

(2) Für die Vernichtung dürfen nur Produkte oder Verfahren eingesetzt oder Dienstleister beauftragt werden, die die Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik erfüllen.

(3) VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte Verschlusssachen können vom Bearbeiter an den dafür vorgesehenen Orten selbst vernichtet werden.

(4) VS-VERTRAULICH oder höher eingestufte Verschlusssachen dürfen nur auf Weisung eines zeichnungsbefugten VS-Bearbeiters durch die VS-Registratoren vernichtet werden. Die VS-Registratoren prüfen die Verschlusssachen vor der Vernichtung auf ihre Vollständigkeit. Die Vernichtung wird mittels Vernichtungsprotokoll und Vermerk der Vernichtungsprotokollnummer im VS-Bestandsverzeichnis nachgewiesen. Dabei ist zu vermerken, an welchem Tag welche Verschlusssachen oder welche Teile davon vernichtet wurden (mit Angabe der Ausfertigungsnummer und Seitenzahl) und wer die Weisung zur Vernichtung erteilt hat. Das Vernichtungsprotokoll ist vom ausführenden VS-Registrator und von einem Zeugen zu unterschreiben.

(5) Ist die Vernichtung von Verschlusssachen technisch nur für eine Zusammenstellung von Verschlusssachen möglich (zum Beispiel im Falle von Verschlusssachen, die auf einem Datenträger gespeichert sind), ist die Vernichtung grundsätzlich so lange auszusetzen, bis alle Verschlusssachen der Zusammenstellung vernichtet werden können. Ist die vorherige Vernichtung einzelner Dokumente unabdingbar, können die noch benötigten Dateien vor Vernichtung der Zusammenstellung nach den Bestimmungen dieser Verschlusssachenanweisung vervielfältigt werden.

§ 33 VS-Zwischenmaterial

(1) VS-Zwischenmaterial, das im Zusammenhang mit einer Verschlusssache anfällt (zum Beispiel Dateien, Vorentwürfe, Stenogramme, Tonträger, Folien oder Fehldrucke), gilt als Verschlusssache. Für die Behandlung von VS-Zwischenmaterial sind Abweichungen bei der Kennzeichnung und beim Nachweis sowie bei der Vernichtung zugelassen.

(2) VS-Zwischenmaterial, das nicht an Dritte weitergegeben und das unverzüglich vernichtet wird, braucht nicht als Verschlusssache gekennzeichnet und nicht nachgewiesen zu werden.

(3) VS-Zwischenmaterial, das nicht unverzüglich vernichtet wird, ist mit dem entsprechenden Geheimhaltungsgrad und dem Zusatz "VS-Zwischenmaterial" zu kennzeichnen. Bei Weitergabe von VS-Zwischenmaterial von VS-VERTRAULICH oder höher eingestuften

Verschlusssachen an Dritte ist ein Nachweis erforderlich; dies gilt nicht bei Weitergabe an die VS-Registratur.

(4) Die Vernichtung von VS-Zwischenmaterial richtet sich nach § 32 mit Ausnahme des Absatzes 4 Satz 2 bis 5, der keine Anwendung findet.

Abschnitt VI: Zusammenarbeit mit nichtdeutschen Stellen und nichtöffentlichen Stellen mit Sitz im Ausland

§ 34 Weitergabe von deutschen Verschlusssachen an nichtdeutsche Stellen und nichtöffentliche Stellen mit Sitz im Ausland

(1) Die Weitergabe von deutschen Verschlusssachen an Dienststellen ausländischer Staaten sowie über- oder zwischenstaatlicher Organisationen (nichtdeutsche Stellen) setzt ein Regierungs- oder Ressortgeheimschutzabkommen oder ein entsprechendes internationales Abkommen voraus, welches die Bedingungen für die Weitergabe und weitere Handhabung regelt. Die Weitergabe von Verschlusssachen an nichtöffentliche Stellen mit Sitz im Ausland setzt entsprechende Regelungen in einem solchen Abkommen voraus.

(2) Ein Regierungsgeheimschutzabkommen ermöglicht allen öffentlichen Stellen des Bundes den Verschlusssachenaustausch, ein Ressortgeheimschutzabkommen lediglich dem jeweiligen Ressort mit der weiteren Vertragspartei.

(3) Wird die Notwendigkeit eines regelmäßigen VS-Austausches mit einem ausländischen Staat oder einer über- oder zwischenstaatlichen Organisation erkennbar, mit dem oder der kein Geheimschutzabkommen oder ein entsprechendes internationales Abkommen besteht, ist dem Bundesministerium des Innern und für Heimat in seiner Eigenschaft als Nationale Sicherheitsbehörde für den Geheimschutz die Notwendigkeit eines Regierungsgeheimschutzabkommens anzuzeigen. Nur für den Fall, dass der Abschluss eines solchen aus politischen, rechtlichen oder anderen Gründen nicht möglich sein sollte, ist der Abschluss eines Ressortgeheimschutzabkommens anzustreben. Die Erteilung einer Verhandlungsgenehmigung des Auswärtigen Amtes für ein Ressortgeheimschutzabkommen bedarf der Zustimmung des Bundesministeriums des Innern, für Bau und Heimat.

(4) Liegt kein Regierungs- oder Ressortgeheimschutzabkommen oder ein entsprechendes internationales Abkommen vor, können deutsche Verschlusssachen nur dann an nichtdeutsche Stellen oder nichtöffentliche Stellen nach Absatz 1 weitergegeben werden, wenn

1. dies zur Erfüllung der Aufgaben der deutschen Stelle erforderlich ist,
2. der Empfänger über die Geheimhaltungspflicht informiert wurde,
3. die nichtdeutsche Stelle der deutschen Stelle nach dem Muster der Anlage VIII schriftlich zusichert, die Verschlusssachen entsprechend der eigenen Geheimschutzvorschriften zu schützen,
4. im Falle von VS-VERTRAULICH oder höher eingestuften Verschlusssachen der Empfänger schriftlich erklärt, dass nur sicherheitsüberprüftes Personal Zugang zu den Verschlusssachen erhält und
5. die deutsche Stelle die Weitergabe dokumentiert.

(5) Soweit die Weitergabe zur Wahrung wesentlicher Sicherheitsinteressen dringend erforderlich ist, können die Voraussetzungen des Absatzes 4 Nummer 1 bis 5 nachgeholt werden.

(6) Soweit deutsche Stellen deutsche Verschlusssachen an nichtdeutsche Stellen nach Absatz 1 oder Absatz 4 weitergeben, teilt der Geheimschutzbeauftragte dies unter Nennung der Anzahl, des Geheimhaltungsgrades und des Empfängers dem Bundesministerium des Innern und für Heimat als Nationale Sicherheitsbehörde für den Geheimschutz jährlich mit.

(7) Deutsche Verschlusssachen sind vor der Weitergabe nach § 20 Absatz 2 hinsichtlich des Empfängers zu kennzeichnen.

(8) Vor der Weitergabe von Verschlusssachen an nichtdeutsche Stellen oder nichtöffentliche Stellen mit Sitz im Ausland ist die Zustimmung des Herausgebers einzuholen.

§ 35 Empfang und Handhabung nichtdeutscher Verschlusssachen

(1) Nichtdeutsche Verschlusssachen, zu deren Schutz deutsche Dienststellen verpflichtet sind, sind nach dem deutschen Geheimhaltungsgrad, der dem Geheimhaltungsgrad der empfangenen Verschlusssache entspricht, und den getroffenen Vereinbarungen oder der Zusicherung nach Absatz 2 zu behandeln. Über- oder zwischenstaatliche Regelungen bleiben unberührt.

(2) Soweit kein Regierungs- oder Ressortgeheimschutzabkommen oder ein entsprechendes internationales Abkommen vorliegt, dürfen deutsche Stellen zum Empfang nichtdeutscher Verschlusssachen Zusicherungen entsprechend § 34 Absatz 4 gegenüber nichtdeutschen Stellen abgeben. Das Bundesministerium des Innern und für Heimat als Nationale Sicherheitsbehörde für den Geheimschutz kann im Ausnahmefall abweichende Regelungen treffen.

(3) Alle Rechte des nichtdeutschen Herausgebers bleiben unberührt.

§ 36 Sicherheitsakkreditierung

(1) IT-Systeme zur Handhabung von Verschlusssachen über- oder zwischenstaatlicher Organisationen (beispielsweise der EU oder der NATO) müssen einem Sicherheitsakkreditierungsverfahren unterzogen werden. Dieses Verfahren dient dem Zweck, Gewissheit darüber zu erlangen, dass alle angemessenen Sicherheitsmaßnahmen durchgeführt worden sind und dass ein ausreichender Schutz der Verschlusssachen und des IT-Systems nach den anzuwendenden Regelungen der über- oder zwischenstaatlichen Organisationen erreicht wird.

(2) Das Bundesministerium des Innern und für Heimat als Nationale Sicherheitsbehörde für den Geheimschutz ist im Sinne der nationalen Zuständigkeit Sicherheitsakkreditierungsstelle (SAA) für IT-Systeme zur Handhabung von Verschlusssachen über- oder zwischenstaatlicher Organisationen. Es kann diese Rolle oder die damit verbundenen Aufgaben ganz oder teilweise an andere Stellen delegieren.

(3) Die Erarbeitung und fortlaufende Aktualisierung der anzuwendenden Akkreditierungsstrategie obliegt dem Bundesamt für Sicherheit in der Informationstechnik im Einvernehmen mit dem Bundesministerium des Innern und für Heimat. Letzteres kann in Einzelfällen von der Akkreditierungsstrategie abweichen oder Abweichungen genehmigen.

§ 37 Zentralregistraturen

(1) Für nichtdeutsche Verschlusssachen der NATO des Geheimhaltungsgrades COSMIC TOP SECRET oder mit dem Warnvermerk ATOMAL oder höher richtet die Nationale Sicherheitsbehörde für den Geheimschutz beim Bundesministerium der Verteidigung eine Zentralregistratur als zentrale Ein- und Ausgangsstelle für den Empfang und die Weitergabe der Verschlusssachen ein.

(2) Für nichtdeutsche Verschlusssachen der EU des Geheimhaltungsgrades TRES SECRET UE/EU TOP SECRET richtet das Auswärtige Amt eine Zentralregistratur als zentrale Ein- und Ausgangsstelle für den Empfang und die Weitergabe der Verschlusssachen ein.

Weiteres zu diesem Abschnitt ist der Anlage VII zu entnehmen.

Abschnitt VII: Materielle und technische Maßnahmen

§ 38 Planung und Durchführung

(1) Bei der Planung und Durchführung von Baumaßnahmen sind rechtzeitig die notwendigen Geheimschutzvorkehrungen zu treffen. Näheres bestimmen die Richtlinien für Sicherheitsmaßnahmen bei der Durchführung von Bauaufgaben.

(2) Bei der Planung von VS-Aktensicherungsräumen, VS-Arbeitsbereichen, VS-IT-Räumen und -Bereichen, Sicherheitsbereichen, Alarmanlagen zum Schutz von Verschlusssachen, Telekommunikationsanlagen und abhörsicheren oder abhörgeschützten Räumen ist das Bundesamt für Sicherheit in der Informationstechnik beratend hinzuzuziehen.

§ 39 Räumliche Sicherheitsmaßnahmen

(1) VS-IT-Räume und alle anderen Räume, in denen VS-VERTRAULICH oder höher eingestufte Verschlusssachen gehandhabt werden (VS-Arbeitsbereiche) sind so zu schützen, dass Unbefugte am Zutritt gehindert werden. Unberechtigte Zutrittsversuche sollen automatisiert aufgezeichnet werden.

(2) Mit der Handhabung von Verschlusssachen befasste Organisationseinheiten und Personen sind nach Möglichkeit räumlich zusammenzufassen.

(3) Sofern Umfang und Bedeutung der dort anfallenden Verschlusssachen es erfordern, sind in einer Behörde oder sonstigen öffentlichen Stelle des Bundes oder in einem Teil von ihr von der jeweils zuständigen obersten Bundesbehörde im Einvernehmen mit dem Bundesministerium des Innern und für Heimat Sicherheitsbereiche zu bilden. Diese sind durch personelle, organisatorische und technische Maßnahmen gegen den Zutritt durch Unbefugte zu schützen. Zutritt zu diesen Bereichen darf nur an Stellen möglich sein, an denen eine zuverlässige Prüfung der Zutrittsberechtigung stattfindet. Als Sicherheitsbereiche kommen sowohl einzelne oder mehrere Räume als auch Gebäude oder Gebäudegruppen in Betracht.

(4) Die in einem Sicherheitsbereich tätigen Personen sind beim Betreten des Sicherheitsbereiches anhand des Dienstausweises oder auf andere geeignete Weise zu identifizieren. Besucher und Fremdpersonal sind nach Identitätsfeststellung während des Aufenthalts im Sicherheitsbereich zu beaufsichtigen. Bei Besuchern und Fremdpersonal, die/das nachweislich (zum Beispiel durch eine Konferenzbescheinigung nach Muster der Anlage VIII) nach dem Sicherheitsüberprüfungsgesetz und der Allgemeinen Verwaltungsvorschrift zum personel-

len Geheimschutz und zum vorbeugenden personellen Sabotageschutz überprüft sind/ist, kann die Beaufsichtigung entfallen.

(5) Das Kontrollpersonal ist über alle Arten von Ausweisen, die zum Betreten des Sicherheitsbereichs berechtigen, zu unterrichten. Die Aufgaben des Kontrollpersonals sind in einer Dienstanweisung festzulegen.

(6) Personen, die zum Zugang zu Verschlusssachen ermächtigt sind oder die eine Tätigkeit ausüben, bei der sie sich Zugang zu Verschlusssachen des Geheimhaltungsgrades VS-VERTRAULICH oder höher verschaffen können, ist der Betrieb von privaten Bild- und Tonaufzeichnungsgeräten, privater Informationstechnik und mobilen Telekommunikations-Endgeräten (dies sind zum Beispiel Mobiltelefone, Datenträger, PDA usw.) am Arbeitsplatz grundsätzlich untersagt. Die Geheimschutzbeauftragten - bei Konferenzen, Sitzungen und Besprechungen die verantwortlichen Leiter - können spezielle Regelungen festlegen, um den Betrieb zu erlauben oder das Mitbringen zu untersagen.

§ 40 Technische Sicherung von Verschlusssachen

(1) Technische Mittel zur Sicherung von Verschlusssachen müssen die vom Bundesamt für Sicherheit in der Informationstechnik festgelegten Anforderungen erfüllen. Dies gilt insbesondere für:

1. VS-Verwahrgelasse,
2. VS-Schlüsselbehälter,
3. Einbruch- und Überfallmeldeanlagen,
4. Zutrittskontrollanlagen,
5. VS-Transportbehälter,
6. VS-Verpackungen,
7. VS-Sicherheitstüren und -schlösser und
8. technische Mittel zur Vernichtung von Verschlusssachen.

(2) Das Bundesamt für Sicherheit in der Informationstechnik führt Prüfungen technischer Mittel und Eignungsfeststellungen entweder auf der Grundlage eines festgestellten Bedarfs in der Bundesverwaltung oder auf Antrag einer Dienststelle durch. Die abschließende Produktabnahme beinhaltet die Prüfung und Bewertung der technischen Mittel zur Sicherung von Verschlusssachen nach Maßgabe der besonderen Belange des Geheimschutzes. Die entsprechend einzuhaltenden Normen und ergänzenden Anforderungen legt das Bundesamt für Sicherheit in der Informationstechnik in Technischen Leitlinien fest.

(3) Das Bundesamt für Sicherheit in der Informationstechnik gibt eine auf der Eignungsfeststellung basierende aktuelle Liste der geeigneten technischen Mittel als Technische Leitlinie heraus.

(4) Stehen keine technischen Mittel mit Eignungsfeststellung zur Verfügung, kann das Bundesamt für Sicherheit in der Informationstechnik im Einzelfall auch dem Einsatz anderer technischer Mittel zustimmen, soweit diese einen vergleichbaren Schutz bieten.

VSA (Anhang zu § 35 SÜG)

§ 41 Abhörschutzmaßnahmen

(1) Dienststellen haben Vorkehrungen zu treffen, damit ihre Telekommunikations- und Informationstechnik nicht dazu missbraucht werden kann, um Raum- und Telefongespräche abzuhören.

(2) Dienststellen richten Räume, in denen häufig oder regelmäßig Gespräche mit VS-VERTRAULICH oder höher eingestuftem Inhalt geführt werden, abhörgeschützt oder abhörsicher wie folgt ein:

1. VS-VERTRAULICH Abhörgeschützter Raum,
2. GEHEIM Abhörgeschützter Raum und
3. STRENG GEHEIM Abhörsicherer Raum.

(3) Für Räume nach Absatz 2 gelten die folgenden grundsätzlichen Anforderungen:

1. Verfügt die Dienststelle über einen Sicherheitsbereich, sollen sie grundsätzlich innerhalb dieses Sicherheitsbereichs eingerichtet werden.
2. Sie sind gegen den unbemerkten Zutritt Unbefugter zu schützen. Art und Umfang des Schutzes legen die Geheimschutzbeauftragten unter Berücksichtigung der Lage und des bestehenden Umgebungsschutzes fest.
3. Sie müssen mindestens eine akustische Dämpfung aufweisen, die ein Mithören von außen hinreichend ausschließt.
4. Sie sind so ausgeführt und ausgestattet, dass Versteckmöglichkeiten für Abhöreinrichtungen nach Möglichkeit beschränkt sind und Manipulationsprüfungen wirksam und in angemessener Zeit durchgeführt werden können.
5. Abhörsichere Besprechungsräume sind so zu gestalten, dass auch eine unbefugte Übertragung von Gesprächen mittels technischer Hilfsmittel (Abhörgeräten) nach außen verhindert wird.

Näheres regelt eine Technische Leitlinie des Bundesamtes für Sicherheit in der Informationstechnik.

(4) Geräte, die geeignet sind Bild- und/oder Tonaufnahmen zu erstellen, zu speichern oder zu übertragen (zum Beispiel Mobiltelefone, Smartphones, Notebooks, Kameras, Diktiergeräte), dürfen in abhörgeschützten oder abhörsicheren Räumen nicht mitgeführt werden, wenn diese für Gespräche mit VS-VERTRAULICH oder höher eingestuftem Inhalt genutzt werden. Ausnahmen bedürfen im Einzelfall der Zustimmung der Geheimschutzbeauftragten.

§ 42 Besondere Dienststellen

(1) Sofern Dienststellen in besonderem Maße Ziel von Angriffen auf Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität von Verschlusssachen sind, legt das Bundesministerium des Innern und für Heimat diese als Dienststellen mit besonderem Geheimschutzbedarf fest.

(2) Dienststellen nach Absatz 1 treffen in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik weitere Sicherheitsvorkehrungen. Insbesondere sind min-

destens alle vier Jahre umfassende Beratungen und Prüfungen durch das Bundesamt für Sicherheit in der Informationstechnik in Anspruch zu nehmen.

§ 43 VS-Registraturen

(1) VS-Registraturen werden, sofern vorhanden, in Sicherheitsbereichen eingerichtet.

(2) Außerhalb der Arbeitszeit sind sie zu bewachen oder durch eine Alarmanlage technisch zu überwachen. In beiden Fällen ist sicherzustellen, dass Unbefugte am Zutritt gehindert werden und dass ein Eindringen Unbefugter erkannt und hilfeleistenden Stellen gemeldet wird.

(3) Der Zutritt zu VS-Registraturen wird grundsätzlich nur den von den Geheimschutzbeauftragten festgelegten Mitarbeitern gewährt. Alle anderen Personen sind, soweit ihnen ebenfalls Zutritt gewährt werden muss, von Mitarbeitern der VS-Verwaltung zu begleiten.

§ 44 VS-Verwahrgelasse

(1) VS-Verwahrgelasse sind besonders gesicherte Räume, Schränke oder sonstige Behältnisse zur Aufbewahrung von Verschlusssachen.

(2) Jede VS-Registratur verfügt über mindestens ein VS-Verwahrgelass.

(3) Ein VS-Verwahrgelass kann von mehreren Personen genutzt werden, soweit dem Grundsatz „Kenntnis nur, wenn nötig“ durch geeignete technische Maßnahmen Rechnung getragen wird, die die Geheimschutzbeauftragten in Abhängigkeit von den dort aufbewahrten Verschlusssachen und den zum Zugang berechtigten Personen festlegen und in der Geheimschutzdokumentation beschreiben.

(4) Unberechtigte Zugangsversuche zu VS-Verwahrgelassen sind, soweit technisch möglich, zu protokollieren.

§ 45 VS-IT-Räume und -Bereiche

(1) VS-IT-Räume und -Bereiche sind Räume und Bereiche, in denen VS-VERTRAULICH oder höher eingestufte Verschlusssachen mit IT be- oder verarbeitet werden.

(2) Sie sollen, sofern vorhanden, in Sicherheitsbereichen eingerichtet oder zu Sicherheitsbereichen im Sinne von § 39 Absatz 3 erklärt und entsprechend gegen unbefugten Zutritt geschützt werden.

(3) Die Sicherungsmaßnahmen für Räume und Bereiche, in denen VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte Verschlusssachen mit IT be- und verarbeitet werden, sind von den Geheimschutzbeauftragten festzulegen.

§ 46 Zutritts- und Zugangsmittel

(1) Zutritts- und Zugangsmittel zu VS-Arbeitsbereichen, Sicherheitsbereichen, VS-Verwahrgelassen, abhörgeschützten und abhörsicheren Räumen, VS-IT, mit der VS-VERTRAULICH oder höher eingestufte Verschlusssachen gehandhabt werden oder Systemen zur technischen Überwachung von Verschlusssachen sind so zu schützen, dass Unbefugte keinen Zugriff auf Verschlusssachen erhalten.

(2) Gegenständliche Zutritts- und Zugangsmittel sind grundsätzlich während der Dienstzeit in persönlichem Gewahrsam zu halten. Vor Verlassen des Dienstgebäudes sind sie grund-

sätzlich in einem VS-Verwahrgelass oder VS-Schlüsselbehälter zu verschließen. VS-Schlüsselbehälter sind möglichst zu beaufsichtigen. Der Verschluss von Zutritts- und Zugangsmitteln unterschiedlicher Nutzer erfolgt grundsätzlich getrennt. Die Schlüssel zu den VS-Schlüsselbehältern verbleiben im persönlichen Gewahrsam des Nutzers des VS-Schlüsselbehälters.

(3) Wissensbasierte Zutritts- und Zugangsmittel dürfen nur den Berechtigten bekannt sein. Sie sind zu ändern:

1. vor der erstmaligen Nutzung,
2. bei einem Wechsel der Berechtigten,
3. nach deren Nutzung in Abwesenheit des Berechtigten,
4. bei einem Verdacht, dass sie bekannt geworden sind und
5. mindestens alle zwölf Monate.

(4) Zutritts- und Zugangsmittel nach Absatz 1 sind zentral zu verwalten und deren Ausgabe zu dokumentieren.

(5) Für Notfälle sollen gegenständliche und wissensbasierte Reservezutritts- und -zugangsmittel in beschrifteten und versiegelten Umschlägen voneinander und von den Originalzutritts- und -zugangsmitteln getrennt in VS-Verwahrgelassen aufbewahrt werden.

§ 47 Abnahmen und Wiederholungsprüfungen

(1) Dienststellen weisen die ordnungsgemäße Funktion und Ausführung von technischen Mitteln zur Sicherung von Verschlusssachen, von abhörgeschützten und abhörsicheren Räumen sowie die Einhaltung der Anforderungen der jeweiligen Technischen Leitlinien durch Abnahmeprüfungen des Bundesamtes für Sicherheit in der Informationstechnik und entsprechende Prüfprotokolle nach.

(2) Das Bundesamt für Sicherheit in der Informationstechnik ist über anstehende Prüfungen nach Absatz 1 rechtzeitig zu unterrichten.

(3) Nach wesentlichen Änderungen oder wenn eine Beeinträchtigung der Wirksamkeit (zum Beispiel durch Abnutzung oder Verschleiß) zu erwarten ist, sind die Überprüfungen zu wiederholen.

(4) Bei Auslandsvertretungen der Bundesrepublik Deutschland tritt der Bundesnachrichtendienst an die Stelle des Bundesamtes für Sicherheit in der Informationstechnik.

§ 48 Lauschabwehrprüfungen

(1) Lauschabwehrprüfungen werden vom Bundesamt für Sicherheit in der Informationstechnik durchgeführt.

(2) Abhörgeschützte und abhörsichere Räume sind auf Veranlassung der Geheimschutzbeauftragten vor der erstmaligen Nutzung für Verschlusssachen und danach stichprobenweise sowie anlassbezogen auf Manipulationen zu untersuchen, die die Sicherheit der Verschlusssachen gefährden können.

(3) Die Geheimschutzbeauftragten legen die Häufigkeit der Stichproben in Abstimmung mit dem Bundesamt für Sicherheit in der Informationstechnik fest. In Dienststellen nach § 42 soll die Prüfung ausgewählter Räume mindestens alle vier Jahre durchgeführt werden.

(4) Andere Räume sind bei Vorliegen eines Manipulationsverdachts oder aus Anlass von Konferenzen von besonderer Bedeutung zu prüfen.

(5) Die Dienststellen unterstützen das Bundesamt für Sicherheit in der Informationstechnik bei der Durchführung der Überprüfungen.

(6) Bei Auslandsvertretungen der Bundesrepublik Deutschland tritt der Bundesnachrichtendienst an die Stelle des Bundesamtes für Sicherheit in der Informationstechnik.

Abschnitt VIII: Einsatz von Informationstechnik

§ 49 Allgemeine Grundsätze

(1) Die Sicherheit von VS-IT ist während des gesamten Lebenszyklus ab dem Zeitpunkt, zu dem feststeht, dass sie zur VS-Verarbeitung eingesetzt werden soll, bis zur Aussonderung kontinuierlich zu gewährleisten.

(2) Werden mit VS-IT VS-VERTRAULICH oder höher eingestufte Verschlusssachen verarbeitet, ist eine Risikoanalyse nach den Standards des Bundesamtes für Sicherheit in der Informationstechnik in der jeweils gültigen Fassung durchzuführen.

§ 50 Freigabe des Betriebs von VS-IT

(1) Die Verarbeitung von Verschlusssachen ist nur mit VS-IT zulässig, die hierfür freigegeben ist. Die Freigabe kann mit Auflagen erteilt werden.

(2) Voraussetzung für die Freigabe ist die Einhaltung der Standards zur Informationssicherheit des Bundesamtes für Sicherheit in der Informationstechnik in der jeweils geltenden Fassung. Dies ist dem Bundesamt nach dessen Vorgaben nachzuweisen; es überprüft die Umsetzung turnusmäßig nach den Vorgaben des Bundesministeriums des Innern und für Heimat risikobasiert gemäß § 4a BSIG.

(3) Für eine Freigabe ist zudem erforderlich, dass die Anforderungen des Geheimschutzes erfüllt sind; das sind regelmäßig:

1. Die Erfüllung des Grundsatzes „Kenntnis nur, wenn nötig“ (§§ 3 Absatz 1, 24 Absatz 2 und 58 Absatz 1 Nummer 2)
2. die Beachtung der Grundsätze zu Einstufung und Kennzeichnung von Verschlusssachen (§§ 15 Absatz 1, 17 Absatz 1, 18 Absatz 2, 19 und 20 Absatz 2)
3. die Verwaltung und der Nachweis der Verschlusssachen (§ 21)
4. die Einhaltung der Regeln zur (zeitweiligen) Aufbewahrung von Verschlusssachen (§ 23)
5. die Gewährleistung der Sicherheit von VS-IT über deren gesamten Lebenszyklus (§ 49 Absatz 1)
6. die Aussonderung und Vernichtung von Verschlusssachen (§§ 30 fortfolgende, 56)
7. die Beachtung der Vorgaben zur Übertragung von Verschlusssachen über technische Kommunikationsverbindungen (§ 55)

8. die Beachtung der einschlägigen Bestimmungen über- oder zwischenstaatlicher Organisationen sowie bilateraler Geheimschutzabkommen (§§ 34 und 35)

9. die Sicherheitsakkreditierung (§ 36).

Die Anforderungen werden in dem vom Bundesamt für Sicherheit in der Informationstechnik herausgegebenen Geheimschutzbaustein des IT-Grundschutzes konkretisiert. Im Einzelfall und insbesondere infolge weiterer Geheimschutzanforderungen aufgrund nationaler und internationaler Bestimmungen mit Bezug auf die Handhabung und Verarbeitung von Verschlusssachen der Geheimhaltungsgrade VS-VERTRAULICH oder höher können die Geheimschutzbeauftragten weitere Anforderungen vorsehen. Vor der Freigabe veranlassen die Geheimschutzbeauftragten eine Überprüfung der wirksamen Umsetzung der Geheimschutzanforderungen, beispielsweise durch einrichtungsexterne Prüfer. Das Ergebnis der Überprüfung ist in der Geheimschutzdokumentation festzuhalten.

(4) Die Dienststellenleitung erteilt die Freigabe, sofern die in den Absätzen 2 und 3 genannten Voraussetzungen vorliegen. Bei Freigaben von VS-IT-Systemen für den Geheimhaltungsgrad VS-NUR FÜR DEN DIENSTGEBRAUCH ist dies insbesondere der Fall, soweit hierfür eine ISO 2 7001-Zertifizierung auf Basis des IT-Grundschutzes inklusive der im Geheimschutzbaustein aufgeführten Anforderungen vorliegt. Sollen Verschlusssachen der Geheimhaltungsgrade VS-VERTRAULICH oder höher verarbeitet werden, tritt als weitere Voraussetzung ein Freigabevotum des Bundesamtes für Sicherheit in der Informationstechnik hinzu. Das Freigabevotum und die Freigabe sind in der Geheimschutzdokumentation festzuhalten.

(5) Sind an einem VS-IT-System mehrere Dienststellen des Bundes beteiligt, handelt es sich um einen VS-IT-Verbund. In diesem Fall obliegt die Gesamtfreigabe der für den Betrieb verantwortlichen Dienststelle (Betreiber). Die Gesamtfreigabe erfolgt auf Grundlage der in Absatz 4 genannten Voraussetzungen. Im Zweifel bestimmt bei ressortinternen VS-IT-Verbünden die zuständige oberste Bundesbehörde und bei ressortübergreifenden VS-IT-Verbünden das Bundesministerium des Innern und für Heimat als Nationale Sicherheitsbehörde für den Geheimschutz den Betreiber des VS-IT-Verbundes. Der Betreiber ist für die Koordinierung der Erfüllung der in Absatz 4 genannten Voraussetzungen zuständig. Das Freigabevotum und die Freigabe sind in der Geheimschutzdokumentation des Betreibers festzuhalten.

(6) Wird ein VS-IT-System im Auftrag des Bundes privatrechtlich betrieben, so bestimmt die jeweils zuständige oberste Bundesbehörde, welche Stelle als Betreiber für die Umsetzung der sich aus der VSA ergebenden Aufgaben Sorge trägt. Bei ressortübergreifenden VS-IT-Systemen bestimmt im Zweifel das Bundesministerium des Innern und für Heimat als Nationale Sicherheitsbehörde für den Geheimschutz die hierfür zuständige Dienststelle.

(7) Das Bundesamt für Sicherheit in der Informationstechnik unterstützt die Dienststellen im Prozess der VS-IT-Freigabe einschließlich der Erfüllung seiner Vorgaben. Dies erfolgt etwa auch anhand von Handreichungen und Praxisbeispielen.

(8) Die Geheimschutzbeauftragten veranlassen eine Wiederholung der Überprüfung nach Absatz 3 in regelmäßigen Abständen sowie anlassbezogen. Ergibt die Überprüfung, dass eine Freigabe nicht erneut erteilt werden könnte, haben die Geheimschutzbeauftragten auf die unverzügliche Herstellung eines vorschriftenkonformen Zustandes hinzuwirken. Die Freigabe ist zu widerrufen, wenn auch mit Maßnahmen des Risikomanagements ein vorschriftenkonformer Zustand nicht hergestellt werden kann. Die Ergebnisse der Folgeüber-

prüfungen sowie ein Widerruf der Freigabe sind in der Geheimschutzdokumentation festzuhalten.

(9) Geheimschutzrelevante Änderungen bei freigegebener VS-IT bedürfen der vorherigen Zustimmung der Geheimschutzbeauftragten.

(10) Dem Bundesamt für Sicherheit in der Informationstechnik ist die erfolgte Freigabe sowie ihr Widerruf mitzuteilen. Das Bundesamt für Sicherheit in der Informationstechnik führt eine Liste über die in den Dienststellen freigegebene VS-IT sowie der freigegebenen VS-IT-Verbünde und erteilt allen Dienststellen auf berechtigtes Verlangen darüber Auskunft.

(11) Näheres regelt eine Technische Leitlinie des Bundesamtes für Sicherheit in der Informationstechnik.

§ 51 Zulassung

(1) Das Bundesamt für Sicherheit in der Informationstechnik legt fest, welche IT-Sicherheitsprodukte oder -komponenten über eine Zulassung verfügen müssen. Diese IT-Sicherheitsprodukte und -komponenten übernehmen innerhalb von VS-IT IT-Sicherheitsfunktionen zum Schutz elektronischer Verschlusssachen.

(2) Grundlage für die Zulassung ist das Zulassungskonzept des Bundesamtes für Sicherheit in der Informationstechnik. Dieses wird im Einvernehmen zwischen dem Bundesministerium des Innern und für Heimat und dem Bundesamt für Sicherheit in der Informationstechnik festgelegt.

(3) Die Zulassung wird durch einen Zulassungsnachweis des Bundesamtes für Sicherheit in der Informationstechnik bestätigt. Dieser enthält auch Bestimmungen für den Einsatz und den Betrieb.

(4) Das Bundesamt für Sicherheit in der Informationstechnik führt Zulassungsverfahren entweder auf der Grundlage eines festgestellten Bedarfs in der Bundesverwaltung oder auf Antrag einer Dienststelle durch.

(5) Sofern für bestimmte VS-IT keine zugelassenen IT-Sicherheitsprodukte oder -komponenten zur Verfügung stehen oder eine Bereitstellung nicht oder nicht zeitgerecht veranlasst werden kann, ist beim Bundesamt für Sicherheit in der Informationstechnik eine Einsatzerlaubnis für andere IT-Sicherheitsprodukte oder -komponenten zu beantragen. Das Bundesamt kann diese Einsatzerlaubnis zeitlich befristen sowie besondere Auflagen und Einschränkungen hinsichtlich der Einsatz- und Betriebsbedingungen erteilen. Nähere Einzelheiten regelt das Zulassungskonzept des Bundesamtes für Sicherheit in der Informationstechnik.

§ 52 IT-Sicherheitsfunktionen

(1) IT-Sicherheitsfunktionen innerhalb von VS-IT, die Gegenstand einer Zulassungsaussage nach § 51 sein können, sind Funktionen, die sich den folgenden Kategorien zuordnen lassen:

1. zur Zugangs- und Zugriffskontrolle,
2. zur Identifikation und Authentisierung,
3. zur kryptographischen Unterstützung,
4. für das Sicherheitsmanagement,

5. zur Informationsflusskontrolle,
6. zum internen Schutz der Benutzerdaten,
7. zum Selbstschutz der Sicherheitsfunktionen und ihrer Daten,
8. zur Netzwerktrennung,
9. zum Schutz der Unversehrtheit,
10. zur Verfügbarkeitsüberwachung oder
11. zur Sicherheitsprotokollierung und Nachweisführung.

Einzelheiten dazu und zum Zulassungskonzept werden in den Technischen Leitlinien des Bundesamtes für Sicherheit in der Informationstechnik geregelt. Diese regeln auch die Mitwirkungspflichten der an einem Zulassungsverfahren beteiligten Parteien.

(2) Das Bundesamt für Sicherheit in der Informationstechnik gibt einen auf diesen IT-Sicherheitsfunktionen und den sich hieraus ableitenden Produktklassen und -typen basierenden Katalog sowie eine aktuelle Liste zugelassener IT-Sicherheitsprodukte und -komponenten heraus. Der Katalog der Produktklassen und -typen definiert insbesondere,

1. ob eine Zulassungsaussage für einen Produkttyp erforderlich ist und
2. welche Sicherheitsfunktionen in einem Zulassungsverfahren für einzelne Produkttypen gelten.

§ 53 Schutz von VS-Übertragungseinrichtungen, -leitungen und -verteilern

(1) VS-Übertragungseinrichtungen, -leitungen und -verteiler, die Verschlusssachen unkryptiert führen, sind gegen unbefugten Zugriff zu schützen.

(2) Für VS-IT, die für VS-NUR FÜR DEN DIENSTGEBRAUCH eingestufte Verschlusssachen eingesetzt wird, gilt dieser Schutz innerhalb von Räumen und Bereichen, die gegen unkontrollierten Zutritt geschützt sind, grundsätzlich als gegeben.

(3) Für VS-IT, die für VS-VERTRAULICH oder höher eingestufte Verschlusssachen eingesetzt wird, gilt dieser Schutz innerhalb von VS-IT-Räumen und -Bereichen grundsätzlich als gegeben.

(4) Außerhalb von Räumen und Bereichen nach den Absätzen 2 und 3 sind durch die Geheimschutzbeauftragten festzulegende zusätzliche Maßnahmen zu treffen. Näheres regelt eine Technische Leitlinie des Bundesamtes für Sicherheit in der Informationstechnik.

§ 54 Handhabung von Datenträgern und IT-Produkten für unkryptierte Verschlusssachen

IT-Produkte, die keiner Zulassung bedürfen, Datenträger und mobile IT, auf denen jeweils elektronische Verschlusssachen unkryptiert gespeichert sind, sind so zu schützen wie es die Einstufung der darauf gespeicherten Information erfordert.

§ 55 Übertragung von Verschlusssachen über technische Kommunikationsverbindungen

(1) Verschlusssachen müssen bei der Weitergabe über technische Kommunikationsverbindungen (elektronische Übertragung) grundsätzlich durch IT-Sicherheitsprodukte nach Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik verschlüsselt werden. § 57 bleibt unberührt.

(2) Abweichend von Absatz 1 ist die unverschlüsselte Weitergabe von Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH grundsätzlich erlaubt, wenn sie unter Einsatz von VS-IT erfolgt, die gemäß den Vorschriften des § 50 dazu freigegeben worden ist. Vor der Weitergabe hat sich jede Nutzerin und jeder Nutzer zu vergewissern, dass nicht nur die Bedingungen des § 24 Absatz 2 und 3 erfüllt sind, sondern die Empfängerinnen und Empfänger die Verschlusssachen ausschließlich über das dafür freigegebene Netz erhalten. Sind diese Bedingungen erfüllt, ist auch die Weitergabe von Verschlusssachen über- und zwischenstaatlicher Organisationen sowie anderer Staaten erlaubt, es sei denn, höherrangige Rechtsvorschriften stehen dem ausdrücklich entgegen.

(3) Abweichend von Absatz 1 dürfen Verschlusssachen ausnahmsweise über andere technische Kommunikationsverbindungen übermittelt werden, wenn die Übermittlung über eine Kommunikationsverbindung nach Absatz 1 einen unvertretbaren Zeitverlust bedeuten würde. In diesem Fall darf

1. für die Kommunikation von VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften Informationen eine nicht nach Absatz 1 geschützte Verbindung genutzt werden. Es sind Verbindungen auszuwählen, bei denen das Risiko des Mithörens durch Unbefugte weitestgehend reduziert wird.
2. für die Kommunikation von VS-VERTRAULICH eingestuften Informationen eine für VS-NUR FÜR DEN DIENSTGEBRAUCH freigegebene Verbindung genutzt werden.

(4) Abweichend von Absatz 1 dürfen Verschlusssachen über andere technische Kommunikationsverbindungen übermittelt werden, wenn eine Verzögerung zu einem Schaden führen würde, der den mit einer Preisgabe der Verschlusssache verbundenen Schaden deutlich überwiegen würde. In jedem Einzelfall ist die Einwilligung der Dienststellenleitung einzuholen und zu dokumentieren.

(5) In den Ausnahmefällen nach den Absätzen 3 und 4 sind folgende Vorsichtsmaßnahmen, die den Mitarbeitern zur Kenntnis zu geben sind, zu beachten, damit das Risiko eines Informationsabflusses weitgehend reduziert wird:

Die Identität des Kommunikationspartners soll vor Beginn der Kommunikation festgestellt werden,

die Kommunikation ist so zu führen, dass der Sachverhalt Dritten nicht verständlich wird und ein unmittelbarer Rückschluss auf den VS-Charakter nicht möglich ist,

die übermittelten Verschlusssachen dürfen keine Kennzeichnungen oder Hinweise aufweisen, die sie von einer nicht eingestuften Information unterscheiden. Die Kennzeichnungspflicht nach § 20 ist in diesem Fall aufgehoben und

die Kommunikationspartner sind auf anderem Wege (zum Beispiel über andere technische Kommunikationsverbindungen, durch Post oder Kurier) unverzüglich über die Einstufung der Verschlusssachen zu unterrichten, außer, dies ist im Einzelfall nicht möglich oder nicht zweckmäßig.

§ 56 Vernichtung und Aussonderung von Datenträgern und registrierten IT-Produkten

(1) Bevor IT-Produkte, Datenträger und mobile IT im Sinne von § 54 ihre gesicherte Einsatzumgebung dauerhaft verlassen, ist sicherzustellen, dass alle auf ihnen gespeicherten Verschlusssachen gelöscht werden. Die Löschung muss mittels vom Bundesamt für Sicherheit

in der Informationstechnik nach § 51 dafür zugelassener beziehungsweise zur Freigabe empfohlener IT-Sicherheitsprodukte erfolgen.

(2) Ist eine Löschung nicht möglich, sind die Speichermedien physisch zu vernichten.

(3) Die Löschung beziehungsweise Vernichtung ist in der Geheimschutzdokumentation zu dokumentieren.

(4) Näheres regelt eine Technische Leitlinie des Bundesamtes für Sicherheit in der Informationstechnik.

§ 57 Abstrahlschutzmaßnahmen

Bei VS-IT, die für VS-VERTRAULICH oder höher eingestufte Verschlusssachen eingesetzt wird, sind Abstrahlschutzmaßnahmen (zum Beispiel nach dem Zonenmodell) zu treffen und zu dokumentieren. Einzelheiten sind einer Technischen Leitlinie des Bundesamtes für Sicherheit in der Informationstechnik zu entnehmen.

§ 58 Zusammenschaltung von VS-IT

(1) Vor der Zusammenschaltung von VS-IT mit anderer VS-IT ist zu prüfen, ob und inwieweit Informationen zwischen diesen Systemen unter Berücksichtigung

1. des jeweiligen Schutzniveaus und
2. des Prinzips „Kenntnis nur, wenn nötig“

ausgetauscht werden dürfen. In Abhängigkeit zum Ergebnis der Prüfung sind IT-Sicherheitsfunktionen nach § 52 zum Schutz der Systemübergänge zu implementieren.

(2) Die direkte oder kaskadierte Zusammenschaltung von bis zum Geheimhaltungsgrad STRENG GEHEIM freigegebener VS-IT mit offener oder ungeschützter IT ist nicht zulässig.

Abschnitt IX: Kryptopersonal und Handhabung von Kryptomitteln

§ 59 Kryptomittel

(1) Nationale Kryptomittel im Sinne dieser Vorschrift sind Produkte, Geräte und die dazugehörigen Dokumente sowie zugehörige Schlüsselmittel zur Entschlüsselung, Verschlüsselung und Übertragung von Informationen, die vom Bundesamt für Sicherheit in der Informationstechnik oder für den Geschäftsbereich des Bundesministeriums der Verteidigung vom Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr als solche festgelegt werden. Internationale Kryptomittel werden nach den einschlägigen über- oder zwischenstaatlichen Vorschriften sowie den jeweiligen nationalen Vorschriften anderer Staaten festgelegt.

(2) Eingestufte Kryptomittel erhalten einen der Warnvermerke „KRYPTO“ (für „KRYPTOSICHERHEIT“) oder „CRYPTO“ (für „CRYPTOSECURITY“). Nicht eingestufte Kryptogeräte sowie zugehörige kryptographische Komponenten und andere zugehörige Bauteile, die sicherheitsempfindliche Funktionen ausführen, erhalten den Warnvermerk „CCI“ (für „Controlled COMSEC Item“).

(3) Alle Kryptomittel unterliegen einer Nachweisführung. Die Nachweisführung erfolgt entsprechend der Nachweisführung für Verschlusssachen der Einstufung VS-VERTRAULICH oder höher. Dazu sind eigene Bestandsverzeichnisse anzulegen.

§ 60 Nationale Verteilerstellen für Kryptomittel

(1) Das Bundesamt für Sicherheit in der Informationstechnik nimmt die Aufgaben der zentralen Nachweisführung, Verwaltung und Verteilung von Kryptomitteln als zivile nationale Verteilerstelle für Kryptomittel (Civil National Distribution Authority) wahr.

(2) Das Zentrum für Informationstechnik der Bundeswehr nimmt die Aufgaben der militärischen nationalen Verteilerstelle für Kryptomittel (Military National Distribution Authority) wahr.

§ 61 Kryptoverwaltung

(1) Dienststellen, die Kryptomittel handhaben, bestellen mindestens einen Kryptoverwalter und eine zur Vertretung berechtigte Person (Kryptoverwaltung). Große Kryptoverwaltungen, die mehrere Kryptoverwalter benötigen, bestimmen einen leitenden Kryptoverwalter. Kryptoverwalter und die zur Vertretung berechtigten Personen müssen die zur Erfüllung ihrer Aufgaben erforderliche Fachkunde erwerben.

(2) Der Name des (leitenden) Kryptoverwalters, der zur Vertretung berechtigten Person und die Behördenanschrift sowie Änderungen sind der jeweils zuständigen nationalen Verteilerstelle für Kryptomittel mitzuteilen.

(3) Haben sich während der Abwesenheit des Kryptoverwalters Veränderungen im Kryptobestand ergeben, so führt dieser unmittelbar nach Rückkehr eine Bestandsprüfung durch. Beim Wechsel des Kryptoverwalters ist der Bestand zu überprüfen und ein Bestandsbericht (Übergabeprotokoll) zu fertigen.

(4) Weitere Aufgaben der Kryptoverwaltung sind der Anlage I zu entnehmen. Näheres zur Handhabung von Kryptomitteln regelt eine Technische Leitlinie des Bundesamtes für Sicherheit in der Informationstechnik.

§ 62 Kryptopersonal

Personen, die Zugang zu Kryptomitteln erhalten (Kryptopersonal), sind vom Geheimschutzbeauftragten nach Muster der Anlage VIII zu belehren und zu berechtigen (Kryptoberechtigung). Die Belehrung und die Berechtigung sind zu dokumentieren.

Abschnitt X: Aufrechterhaltung des Geheimschutzes

§ 63 Kontrollen

(1) Die Geheimschutzbeauftragten sollen in ihrer Dienststelle in angemessenen Zeitabständen kontrollieren, ob die Einstufung, die Befristung und die Handhabung der Verschlusssachen den Vorschriften der Verschlusssachenanweisung entsprechen. Die Kontrollen können auch durch besonders beauftragte Mitarbeiter durchgeführt werden. Soweit die Bearbeitung von Verschlusssachen mit IT betroffen ist, werden die Geheimschutzbeauftragten hierbei von den IT-Sicherheitsbeauftragten unterstützt.

(2) Alle Bediensteten haben die Durchführung von Kontrollen zu unterstützen und hierfür auf Verlangen Zugang zu allen Verschlusssachen zu gewähren.

(3) Die obersten Bundesbehörden können in angemessenen Abständen bei den Behörden ihres jeweiligen Geschäftsbereichs kontrollieren, ob die dortigen Regelungen, Maßnahmen und Verfahren der Verschlusssachenanweisung entsprechen.

(4) Die Durchführung der Kontrollen und deren Ergebnisse sind in angemessener Weise zu dokumentieren.

§ 64 Behandlung von Geheimschutzvorkommnissen

(1) Wird bekannt oder besteht der Verdacht, dass Geheimschutzvorschriften verletzt wurden oder Sicherheitsvorkehrungen den Geheimschutz nicht gewährleisten, sind die betroffenen Geheimschutzbeauftragten unverzüglich zu unterrichten. Die Geheimschutzbeauftragten stellen in diesen Fällen den Sachverhalt fest und treffen die erforderlichen Maßnahmen.

(2) Werden Dienststellen geheimschutzbezogene Vorkommnisse mit Bezug zu VS-VERTRAULICH oder höher eingestuften nationalen Verschlusssachen von wesentlicher Bedeutung bekannt, unterrichten sie unverzüglich das Bundesministerium des Innern und für Heimat, wenn die Besorgnis einer Bekanntgabe an Dritte besteht. Gleiches gilt für nichtdeutsche Verschlusssachen, unabhängig von deren Geheimhaltungsgrad.

(3) Ist ein nachrichtendienstlicher Hintergrund oder eine Verratstätigkeit anderer Art nicht auszuschließen, so ist das Bundesamt für Verfassungsschutz, im Geschäftsbereich des Bundesministeriums der Verteidigung das Bundesamt für den Militärischen Abschirmdienst zu beteiligen.

(4) Dienststellen, denen geheimschutzbezogene Vorkommnisse bekannt werden, die für die technische Sicherung von Verschlusssachen oder für die Sicherheit der Informations- und Kommunikationstechnik des Bundes von Bedeutung sind, unterrichten unverzüglich das Bundesamt für Sicherheit in der Informationstechnik. Das Bundesamt für Sicherheit in der Informationstechnik unterrichtet im Anschluss unverzüglich das Bundesministerium des Innern und für Heimat.

§ 65 Verhalten in außergewöhnlichen Gefahrenlagen

Sofern im Katastrophen-, Alarm- oder Verteidigungsfall oder in vergleichbaren außergewöhnlichen Gefahrenlagen die Möglichkeit besteht, dass Unbefugte sich Zugang zu VS-VERTRAULICH oder höher eingestuften Verschlusssachen verschaffen können, und eine Aufbewahrung nach § 23 nicht möglich ist, sind die Verschlusssachen zu vernichten. Die Dienststellen treffen in ihren Geheimschutzdokumentationen Handlungsanweisungen für die Vernichtung in diesen Fällen.

Abschnitt XI: Abschließende Regelungen

§ 66 Schlussbestimmungen

(1) Das Bundesministerium des Innern und für Heimat kann in besonderen Ausnahmefällen Abweichungen von dieser Verschlusssachenanweisung unter der Voraussetzung zulassen, dass der mit der Verschlusssachenanweisung beabsichtigte Schutz durch andere Sicherheitsvorkehrungen erreicht wird.

(2) Jede Dienststelle kann über die Verschlusssachenanweisung hinaus verschärfte Sicherheitsvorkehrungen treffen, soweit sie die notwendige einheitliche Behandlung der Verschlusssachen im gesamten VS-Verkehr nicht stören.

§ 67 Inkrafttreten

Diese Allgemeine Verwaltungsvorschrift tritt am 1. April 2023 in Kraft. Gleichzeitig tritt die Allgemeine Verwaltungsvorschrift zum materiellen Geheimschutz (Verschlusssachenanweisung - VSA) vom 10. August 2018 (GMBl. 2018, 826) außer Kraft.

Es gelten folgende Anlagen zu dieser Vorschrift

Anlage I:	Hinweise zur Geheimschutzorganisation
Anlage II:	Hinweise zur Geheimschutzdokumentation
Anlage III:	Hinweise zur Einstufung
Anlage IV:	Hinweise zur Handhabung von Verschlusssachen
Anlage V:	Merkblatt zur Behandlung von Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD-Merkblatt)
Anlage VI:	Richtlinie für die Abgabe von Verschlusssachen an das Geheimarchiv des Bundesarchivs (VS-Archivrichtlinie)
Anlage VII:	Hinweise zur Handhabung von Verschlusssachen ausländischer Staaten sowie über- oder zwischenstaatlicher Organisationen
Anlage VIII:	Muster

Anlage I
Verschlusssachenanweisung
Hinweise zur Geheimschutzorganisation

1 Geheimschutzbeauftragte

Geheimschutzbeauftragte oder besonders beauftragte Mitarbeiter (zum Beispiel Geheimschutzbeamte) nehmen insbesondere die nachfolgend beschriebenen Aufgaben wahr:

1.1 Geheimschutzorganisation

- die Einrichtung und den Betrieb einer VS-Registratur,
- die Einrichtung und den Betrieb einer Kryptoverwaltung,

- die Veranlassung der Bestellung von besonders beauftragten Mitarbeitern, VS-Registratoren und Kryptoverwaltern,
- die Gewährleistung der erforderlichen Fachkunde aller Mitarbeiter in der Geheimschutzorganisation und
- die Erstellung und Fortschreibung der Geheimschutzdokumentation.

1.2 Personeller Geheimschutz

- die Erfassung der Dienstposten, auf denen eine sicherheitsempfindliche Tätigkeit im Sinne des Sicherheitsüberprüfungsgesetzes ausgeübt wird,
- die Veranlassung von Sicherheitsüberprüfungen nach dem Sicherheitsüberprüfungsgesetz,
- die Durchführung des Sicherheitsüberprüfungsgesetzes als zuständige Stelle,
- die Verpflichtung, Ermächtigung und Zulassung von Personen zu sicherheitsempfindlichen Tätigkeiten sowie die Erweiterung, Einschränkung oder Aufhebung der Ermächtigung und Zulassung,
- die Unterrichtung der VS-Registratur über Ermächtigungen und Zulassungen sowie deren Erweiterung, Einschränkung, Aufhebung oder Erlöschen und
- die Sicherstellung der Begleitung von Fremdpersonal in Sicherheitsbereichen.

1.3 Materieller Geheimschutz

- die Festlegung und Einrichtung von Sicherheitsbereichen innerhalb der Dienststelle,
- die Festlegung und Einrichtung von abhörsicheren, abhörgeschützten und abstrahlsicheren Räumen,
- die Festlegung und Einrichtung von Räumen für die Handhabung von VS-VERTRAULICH und höher eingestuften Verschlusssachen, insbesondere
    - unter Abstrahlgesichtspunkten vermessene Räume (entsprechend dem BSI-Zonenmodell),
    - Räume zur Aufbewahrung von Verschlusssachen und
    - VS-IT-Räume und -Bereiche
- die Errichtung von Einbruch- und Überfallmeldeanlagen,
- die Errichtung von Zutrittskontrollen,
- die technischen Überprüfungen zur Abnahme und Revision von abhörgeschützten, abhörsicheren und abstrahlsicheren Räumen,
- die technischen Überprüfungen zur Abnahme von technischen Sicherungseinrichtungen,
- die Festlegung und Bereitstellung von Arbeitsmitteln für die Handhabung von Verschlusssachen,
- die Vorkehrungen gegen ein unbefugtes Vervielfältigen von VS-VERTRAULICH oder höher eingestuften Verschlusssachen,
- die Festlegung von Verfahren zur Vernichtung von Verschlusssachen,
- die Lauschabwehr- und sonstigen Manipulationsprüfungen.
- die Festlegung der Anforderungen des Geheimschutzes an VS-IT,

- die Durchführung von Kontrollen und
- die Behandlung von Geheimschutzvorkommnissen.

2 IT-Sicherheitsbeauftragte

IT-Sicherheitsbeauftragte nehmen insbesondere die nachfolgend beschriebenen Aufgaben wahr:

- Zuständigkeit für das Informationssicherheitskonzept,
- Unterstützung des Geheimschutzbeauftragten bei Kontrollen und der Behandlung von Geheimschutzvorkommnissen, soweit die Verarbeitung von Verschlusssachen mit IT betroffen ist,
- Unterstützung des Geheimschutzbeauftragten bei der Überprüfung der Umsetzung der Geheimschutzmaßnahmen, soweit die Verarbeitung von Verschlusssachen mit IT betroffen ist und
- Planung neuer und Änderung bestehender VS-IT-Verfahren.

3 VS-Registratur

Die Aufgaben der VS-Registratur umfassen insbesondere:

- den Empfang und Versand von Verschlusssachen einschließlich ihrer Überprüfung auf vorschriftsmäßige Verpackung, Beschädigungen und Vollständigkeit,
- die Registrierung von Verschlusssachen im VS-Bestandsverzeichnis sowie die Führung aller weiteren erforderlichen Nachweise,
- die Ausgabe von Verschlusssachen nur an entsprechend ermächtigtes oder zu deren Beförderung zugelassenes Personal,
- die Nachfrage, ob Verschlusssachen weiterhin beim Nutzer verbleiben müssen,
- als VS-Registratur der herausgebenden Dienststelle: die notwendigen Benachrichtigungen im Falle einer Verlängerung, Änderung oder Aufhebung der Einstufung einer Verschlusssache,
- als VS-Registratur der empfangenden Dienststelle: die Nachvollziehung entsprechend eingehender Benachrichtigungen,
- die Prüfung, ob die Einstufung von Verschlusssachen, deren Befristung abgelaufen ist, verlängert wurde durch Abfrage in der VS-Nachweisdatenbank und gegebenenfalls die Nachvollziehung von Verlängerungen oder Aufhebungen der entsprechenden VS-Einstufungen,
- die Sicherstellung der vollständigen Rückgabe von Verschlusssachen im Fall des Aufgabenwechsels von Mitarbeitern innerhalb der Dienststelle, der Aufhebung ihrer Ermächtigung sowie ihres Ausscheidens aus der Dienststelle,
- die jährliche Durchführung von Bestandsprüfungen und schriftliche Berichterstattung an den Geheimschutzbeauftragten,
- die Aussonderung von Verschlusssachen (Abgabe an das zuständige Archiv beziehungsweise Vernichtung) und
- die unverzügliche Mitteilung von Geheimschutzvorkommnissen an den Geheimschutzbeauftragten.

Die Muster für die vorgenannten Tätigkeiten befinden sich in Anlage VIII.

4 Kryptoverwaltung

Die Aufgaben der Kryptoverwaltung umfassen insbesondere

- den Empfang von Kryptomittelsendungen einschließlich ihrer Überprüfung auf vorschriftsmäßige Verpackung, Beschädigungen und Vollständigkeit,
- die Registrierung von Kryptomitteln sowie die Führung aller weiteren erforderlichen Nachweise,
- die Ausgabe von Kryptomitteln nur an Kryptopersonal,
- die Überprüfung der Notwendigkeit von Kryptomitteln beim Kryptopersonal und gegebenenfalls deren Abmeldung bei der zuständigen Kryptoverteilerstelle,
- die Sicherstellung der Rückgabe von Kryptomitteln im Fall des Aufgabenwechsels des zuständigen Kryptopersonals innerhalb der Dienststelle sowie dessen Ausscheiden aus der Dienststelle,
- die jährliche Durchführung von Bestandsprüfungen und schriftliche Berichterstattung an die Geheimschutzbeauftragten,
- die jährliche Durchführung der Seitenkontrollen bei Vorschriften und Dokumentationen,
- die Einarbeitung von Änderungen in Vorschriften,
- die Vernichtung von Kryptomitteln und
- die unverzügliche Mitteilung von Bloßstellungen oder vermutlichen Bloßstellungen von Kryptomitteln sowie von Verstößen gegen Bestimmungen zum Umgang mit Kryptomitteln an die Geheimschutzbeauftragten.

Anlage II
Verschlusssachenanweisung

Hinweise zur Geheimschutzdokumentation

1 Zuständigkeit

Die Geheimschutzdokumentationen werden von den Geheimschutzbeauftragten oder besonders beauftragten Mitarbeitern (zum Beispiel Geheimschutzbeamten) erstellt und fortgeschrieben. Bei der Erstellung der VS-IT-Dokumentationen, die Teil der Geheimschutzdokumentationen sind, werden sie von den IT-Sicherheitsbeauftragten unterstützt.

2 Inhalt der Geheimschutzdokumentation

Die Geheimschutzdokumentation umfasst

- alle Vorschriften, die in der jeweiligen Dienststelle bei der Handhabung von Verschlusssachen zu beachten sind. Dazu zählen insbesondere Dienstanweisungen, Erlasse und Rundschreiben, die den Umgang mit Verschlusssachen regeln,
- eine Auflistung aller sicherheitsempfindlichen Dienstposten der jeweiligen Dienststelle. Die Auflistung soll erkennen lassen, welche Art der Sicherheitsüberprüfung für den jeweiligen Dienstposten erforderlich ist,
- eine Auflistung der nach § 4 Absatz 2 ermächtigten und nach § 4 Absatz 3 zugelassenen Personen der jeweiligen Dienststelle. Die Auflistung soll erkennen lassen, wann und bis zu welchem Geheimhaltungsgrad die jeweiligen Personen ermächtigt beziehungsweise zugelassen sowie belehrt wurden,

- die VS-Sicherungsdokumentation (siehe 2.1),
- die VS-IT-Dokumentation (siehe 2.2),
- alle Prüfprotokolle über Abnahmen und Wiederholungsüberprüfungen nach § 47. Werden bei den Abnahmen und Wiederholungsüberprüfungen Mängel an der ordnungsgemäßen Funktion und Ausführung von technischen Mitteln zur Sicherung von Verschlusssachen oder von abhörgeschützten und abhörsicheren Räumen oder Mängel bei der Einhaltung der Anforderungen der jeweiligen Technischen Leitlinien des Bundesamtes für die Sicherheit in der Informationstechnik festgestellt, sind diese und die diesbezüglich ergriffenen Maßnahmen in der Geheimschutzdokumentation darzulegen,
- alle Nachweise über durchgeführte Lauschabwehrprüfungen nach § 48. Die Ergebnisse der durchgeführten Lauschabwehrprüfungen sind festzuhalten und zur Geheimschutzdokumentation zu nehmen. Werden bei den Lauschabwehrprüfungen Manipulationen festgestellt, sind auch diese und die diesbezüglich ergriffenen Maßnahmen in der Geheimschutzdokumentation darzulegen.
- das Ergebnis der Überprüfung der Geheimschutzanforderungen nach § 50 Absatz 3, Freigaben und Freigabevoten nach § 50 Absatz 4 und 5 sowie Wiederholungsüberprüfungen und ggf. Widerruf der Freigaben nach § 50 Absatz 8,
- alle Nachweise über durchgeführte Kontrollen nach § 63. Die Ergebnisse der durchgeführten Kontrollen sind festzuhalten und zur Geheimschutzdokumentation zu nehmen. Werden bei den Kontrollen Verstöße gegen die Verschlusssachenanweisung festgestellt, sind auch diese und die diesbezüglich ergriffenen Maßnahmen in der Geheimschutzdokumentation darzulegen,
- alle Berichte über Geheimschutzvorkommnisse nach § 64. Auch die Berichte über die diesbezüglich ergriffenen Maßnahmen und über gegebenenfalls erfolgte Unterrichtungen und Beteiligungen nach § 64 Absatz 2 bis 4 sind zur Geheimschutzdokumentation zu nehmen,
- Handlungsanweisungen (Notfallpläne) für die Vernichtung von Verschlusssachen in außergewöhnlichen Gefahrenlagen nach § 65
- die Empfangsbestätigungen zu ausgegebenen VS-Bestandsverzeichnissen.

2.1 Inhalt der VS-Sicherungsdokumentation

Die VS-Sicherungsdokumentation umfasst

- eine Auflistung der Anzahl und Standorte
  - der VS-Aktensicherungsräume nach § 38 Absatz 2,
  - der VS-Arbeitsbereiche nach § 39 Absatz 1,
  - der Sicherheitsbereiche nach § 39 Absatz 3 sowie der hierzu Zutrittsberechtigten,
  - der abhörgeschützten und abhörsicheren Räume nach § 41 Absatz 2,
  - der VS-Registratur nach § 43 sowie der VS-Registratoren,
  - der VS-Verwahrgelasse nach § 44 sowie deren Nutzer,
  - der VS-IT-Räume und -Bereiche nach § 45,
  - der VS-Schlüsselbehälter nach § 46 Absatz 2 sowie deren Nutzer und
  - der Reservezutritts- und -zugangsmittel nach § 46 Absatz 5 sowie deren Verwalter.

- eine Beschreibung der Geheimschutzmaßnahmen für die bei der Dienststelle vorhandenen vorgenannten Bereiche, Räume, Behälter und Mittel, einschließlich der Regelungen zu deren Nutzung, Bewachung und technischen Überwachung unter Berücksichtigung der mehrschichtigen Sicherheit nach § 6.

2.2 Inhalt der VS-IT-Dokumentation

Die VS-IT-Dokumentation umfasst

- Nachweise zur Einhaltung der Standards zur Informationssicherheit des Bundesamtes für Sicherheit in der Informationstechnik,
- Nachweise der Prüfung der wirksamen Umsetzung von Geheimschutzanforderungen und (bei VS-VERTRAULICH und höher) das Freigabevotum des BSI,
- eine Dokumentation der Freigabe des Betriebs von VS-IT nach § 50 (bzw. der Fortgeltung oder des Widerrufs einer Freigabe) einschließlich eventueller Auflagen,
- die Zulassungsnachweise nach § 51 Absatz 3 und Einsatzerlaubnisse nach § 51 Absatz 5 für die eingesetzte VS-IT und
- eine Auflistung der Art, Anzahl und Standorte der genutzten VS-IT und deren IT-Sicherheitsfunktionen nach § 52.

Anlage III
Verschlusssachenanweisung

Hinweise zur Einstufung

Tragen Sie durch eine sachgerechte Einstufung dazu bei, dass

- **tatsächlich geheimhaltungsbedürftige Informationen effektiv geschützt und**
- **Aufwand für unnötige Sicherheitsmaßnahmen vermieden wird.**

Beachten Sie deshalb Folgendes:

1 Prüfen Sie kritisch, ob eine Einstufung tatsächlich notwendig ist.

Eine Einstufung kommt nur im öffentlichen Interesse, insbesondere zum Schutz des Wohles des Bundes oder eines Landes in Betracht. Geschäfts-, Betriebs-, Erfindungs-, Steuer- oder sonstige private Geheimnisse oder Umstände des persönlichen Lebensbereichs sind nur dann einzustufen, wenn die Einstufung zumindest auch im öffentlichen Interesse liegt.

Ein öffentliches Interesse an einer Einstufung kann insbesondere bei Informationen vorliegen, die

- die innere Sicherheit,
- die äußere Sicherheit oder
- die auswärtigen Beziehungen

des Bundes oder eines Landes betreffen.

Im Falle einer Einstufung muss vom Herausgeber der Verschlusssache schlüssig darzulegen sein, welche Schäden, Gefährdungen oder Nachteile für den Bestand, die Sicherheit oder die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder bei Kenntnisnahme der Verschlusssache durch Unbefugte entstehen können.

Für Informationen, die die oben beschriebenen Anforderungen nicht erfüllen, kann eine Einstufung nicht erfolgen. Für diese Informationen bestehen möglicherweise andere (Spezial-)Regelungen, die zu beachten sind und den Schutz dieser Informationen sicherstellen (zum Beispiel das Datenschutzrecht oder das Bundesarchivgesetz).

2 Im Falle einer Einstufung müssen der gewählte Geheimhaltungsgrad und die damit verbundenen Schutzmaßnahmen dem konkreten Schutzbedürfnis entsprechen.

Eine Einstufung als Verschlusssache des Geheimhaltungsgrades VS-VERTRAULICH oder höher hat zur Folge, dass alle Personen, die Zugang zu der Verschlusssache haben oder ihn sich verschaffen können einer aufwendigen, in Persönlichkeitsrechte eingreifenden Sicherheitsüberprüfung unterzogen und kostenintensive materielle Schutzmaßnahmen getroffen werden müssen.

3 Beispiele für VS-Einstufungen:

3.1 STRENG GEHEIM

Eine Einstufung als Verschlusssache des Geheimhaltungsgrades STRENG GEHEIM kommt zum Beispiel in Betracht für:

- den (Gesamt-)Alarmplan der Bundeswehr,
- das (Gesamt-)Informationsaufkommen eines Nachrichtendienstes und
- Zusammenstellungen, deren einzelne Teile GEHEIM eingestuft sind, die jedoch in ihrer Gesamtheit STRENG GEHEIM einzustufen sind.

3.2 GEHEIM

Eine Einstufung als Verschlusssache des Geheimhaltungsgrades GEHEIM kommt zum Beispiel in Betracht für:

- Maßnahmen nach dem Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses,
- Informationen zur „Elektronischen Kampfführung“ der Bundeswehr,
- Teile des Alarmplanes der Bundeswehr,
- besondere Einsatzmittel und -verfahren von Spezialeinheiten der Polizei,
- Kryptodaten, die für die Verschlüsselung von VS-VERTRAULICH und höher eingestuften Verschlusssachen eingesetzt werden und
- Zusammenstellungen, deren einzelne Teile VS-VERTRAULICH eingestuft sind, die jedoch in ihrer Gesamtheit GEHEIM einzustufen sind.

3.3 VS-VERTRAULICH

Eine Einstufung als Verschlusssache des Geheimhaltungsgrades VS-VERTRAULICH kommt zum Beispiel in Betracht für:

- Ermittlungsberichte in Spionageverdachtsfällen,
- Erkenntnisse über die Arbeitsweise extremistischer/terroristischer Organisationen, deren Preisgabe die weitere Beobachtung/Aufklärung gefährden würde,
- außenpolitische Verhandlungspositionen, deren frühzeitige Bekanntgabe deutschen Interessen schaden würde und

- Zusammenstellungen, deren einzelne Teile VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuft sind, die jedoch in ihrer Gesamtheit VS-VERTRAULICH einzustufen sind.

3.4 VS-NUR FÜR DEN DIENSTGEBRAUCH

Eine Einstufung als Verschlusssache des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH kommt zum Beispiel in Betracht für:

- Fahndungsunterlagen aus den Bereichen Terrorismus/Extremismus,
- Geheimschutzdokumentationen und
- Zusammenstellungen, deren einzelne Teile nicht eingestuft sind, die jedoch in ihrer Gesamtheit VS-NUR FÜR DEN DIENSTGEBRAUCH einzustufen sind.

Anlage IV
Verschlusssachenanweisung

Hinweise zur Handhabung von Verschlusssachen

1 Kennzeichnung von Verschlusssachen

1.1 Kennzeichnung von Schriftgut

Bei STRENG GEHEIM und GEHEIM eingestuften Verschlusssachen wird der Geheimhaltungsgrad mit dem Zusatz „amtlich geheim gehalten“ in roter Farbe durch Stempel oder Druck am oberen und unteren Rand jeder beschriebenen Seite angebracht.

Bei VS-VERTRAULICH eingestuften Verschlusssachen wird der Geheimhaltungsgrad mit dem Zusatz „amtlich geheim gehalten“ in schwarzer oder blauer Farbe durch Stempel oder Druck am oberen Rand jeder beschriebenen Seite angebracht.

Bei VS-NUR FÜR DEN DIENSTGEBRAUCH eingestuften Verschlusssachen wird der Geheimhaltungsgrad in schwarzer oder blauer Farbe durch Stempel oder Druck am oberen Rand jeder beschriebenen Seite angebracht.

1.2 Kennzeichnung von VS-Schriftgutbehältern, Behältern von VS-Datenträgern und VS-Bestandsverzeichnissen

Die äußeren Vorder- und Rückseiten sowie gegebenenfalls die Rücken von Schriftgutbehältern und Behältern von VS-Datenträgern (zum Beispiel Boxen, Ordner, Hefter, Hüllen, Lauf-, Klebe- oder Sammelmappen), in denen VS-VERTRAULICH oder höher eingestufte Verschlusssachen befördert oder verwahrt werden, sind wie folgt zu kennzeichnen:

1. Bei STRENG GEHEIM eingestuften Verschlusssachen mit einem gelben und einem roten Diagonalstreifen (überkreuzt).
2. Bei GEHEIM eingestuften Verschlusssachen mit einem roten Diagonalstreifen.
3. Bei VS-VERTRAULICH eingestuften Verschlusssachen mit einem blauen Diagonalstreifen.

VS-Bestandsverzeichnisse sind in derselben Weise zu kennzeichnen

1.3 Warn- und Sperrvermerke

Warn- und Sperrvermerke begrenzen den zugangsberechtigten Empfängerkreis einer Verschlusssache. Eine Weitergabe einer mit Warn- oder Sperrvermerk gekennzeichneten Ver-

schlusssache an andere als die entsprechend berechtigten Personen ist nur mit Zustimmung des Herausgebers zulässig. Zudem können Warn- und Sperrvermerke weitere Auflagen zur Handhabung der Verschlusssache regeln.

Für die Handhabung von Verschlusssachen, die mit einem Warnvermerk versehen sind, gibt es zusätzliche Handhabungsanweisungen, die den entsprechend berechtigten und ermächtigten Personen bekannt sind.

1.3.1 Warnvermerke

Es können insbesondere die nachfolgend aufgeführten Warnvermerke verwendet werden:

- „KRYPTOSICHERHEIT“ oder „KRYPTO“ oder „CRYPTOSECURITY“ oder „CRYPTO“
- „Controlled COMSEC Item“ oder „CCI“
- „Atomal“
- „Auswertesache (Schutzwort)“ oder „ANRECHT“ oder „Schutzwort-VS“ oder „SW-VS“

Warnvermerke für nichtdeutsche Verschlusssachen regeln die jeweiligen über- oder zwischenstaatlichen Bestimmungen.

1.3.2 Sperrvermerke

Es können insbesondere die nachfolgend aufgeführten Sperrvermerke verwendet werden:

- „<jeweilige Behörde> intern“
- „Für Geheimschutzbeauftragte“
- „Nur Deutschen zur Kenntnis“ oder „GE eyes only“
- „Weitergabe an <jeweiliger Name>“
- „FÜR KRYPTOVERWALTER“ oder „for crypto custodian“
- „Nur zu ihrer Information“
- „Die Fertigung von Kopien dieser VS ist untersagt“

2 Nachweis von VS-VERTRAULICH oder höher eingestufter Verschlusssachen

Die papiergestützte Nachweisführung von Verschlusssachen erfolgt anhand von VS-Bestandsverzeichnissen, VS-Quittungsbüchern, VS-Begleitzetteln, VS-Empfangsscheinen, VS-Übergabeprotokollen und VS-Vernichtungsprotokollen.

Jede Eintragung, Änderung, nachträgliche Ergänzung und Streichung in papiergestützten VS-Nachweisen muss mit Datum versehen und der jeweils handelnden Person zuzuordnen sein. Bei Änderungen und Streichungen muss der ursprüngliche Text lesbar bleiben. Es ist unzulässig, Eintragungen zu löschen oder unkenntlich zu machen sowie Teile zu entfernen oder einzufügen.

Die elektronische Nachweisführung von Verschlusssachen erfolgt anhand von VS-Registratursystemen.

Jede Erstellung, Änderung, nachträgliche Ergänzung und Löschung eines Datensatzes in elektronischen VS-Nachweisen ist mit Datum, Uhrzeit und Namen des Nutzers zu protokollieren. Änderungen und Löschungen von bestehenden Datensätzen müssen so vorgenommen werden, dass der ursprüngliche Inhalt nachvollziehbar bleibt. Die Protokolldaten sind min-

destens fünf Jahre nach Vernichtung, Abgabe oder Herabstufung der betroffenen Verschlusssache verfügbar zu halten.

2.1 VS-Bestandsverzeichnisse und VS-Registratursysteme

Die Registrierung von Verschlusssachen in VS-Bestandsverzeichnissen und VS-Registratursystemen erfolgt auf der Grundlage der aktuellen Grundsätze ordnungsgemäßer Aktenführung und der hierzu jeweils in den Dienststellen getroffenen Festlegungen. VS-Registratur und offene Registratur in der jeweiligen Dienststelle stimmen sich hierbei ab.

2.1.1 Papiergestützte VS-Bestandsverzeichnisse

Papiergestützte VS-Bestandsverzeichnisse werden von den Geheimschutzbeauftragten oder von besonders beauftragten Mitarbeitern an die VS-Registratoren herausgegeben. Diese bestätigen den Empfang. Die Empfangsbestätigungen sind zur Geheimschutzdokumentation zu nehmen.

VS-Bestandsverzeichnisse sind in gebundener Form zu führen. Die Doppelseiten sind fortlaufend zu nummerieren. Das Titelblatt wird nicht nummeriert. Auf dem Titelblatt eines VS-Bestandsverzeichnisses sind zu vermerken:

- die Behörde,
- welche Geheimhaltungsgrade nachgewiesen werden,
- von wem das VS-Bestandsverzeichnis geführt wird,
- die Nummer/der Band des VS-Bestandsverzeichnisses,
- die Anzahl der enthaltenen Doppelseiten,
- das Datum des ersten und letzten Eintrags sowie
- die Unterschrift des Geheimschutzbeauftragten und das Dienstsiegel.

Jede Verschlusssache ist im Bestandsverzeichnis unter einer eigenen, fortlaufenden Nummer (Tagebuchnummer) zu registrieren. Jede Anlage und jede Vervielfältigung einer Verschlusssache ist einzeln ebenfalls unter dieser Tagebuchnummer zu registrieren.

2.1.2 VS-Registratursysteme

VS-Registratursysteme sind gegen unbefugten Zugriff zu schützen. Sie sollen auf nicht vernetzten Einzelplatzrechnern oder in einem isolierten, ausschließlich für den Zweck der VS-Nachweisführung genutzten Netz betrieben werden.

In VS-Registratursystemen ist bei der Registrierung für jede Verschlusssache unter einer eigenen fortlaufenden Nummer (Tagebuchnummer) ein eigener Datensatz anzulegen. Für jede Anlage und jede Vervielfältigung einer Verschlusssache sind jeweils eigene Datensätze unter derselben Tagebuchnummer anzulegen.

VS-Registratursysteme stellen Funktionen bereit, die die Ausgabe aller für die VS-Nachweisführung relevanten Daten nach bestimmten Auswahl- und Sortierungskriterien ermöglichen.

Näheres regelt eine technische Leitlinie des Bundesamtes für Sicherheit in der Informationstechnik.

2.2 Nachweisführung bei elektronischer VS-Bearbeitung

Werden Verschlusssachen innerhalb von VS-IT hergestellt, bearbeitet, vervielfältigt, gespeichert, übertragen oder gelöscht, kann die Nachweisführung durch Prozesse innerhalb der VS-IT automatisiert vorgenommen werden.

Die Nachweisführung bei elektronischer VS-Bearbeitung hat nach den Nummern 2.1 und 2.1.2 zu erfolgen. Das Anlegen von Ordnungsstrukturen (zum Beispiel Akten und Vorgänge), das Ändern und Löschen von Datensätzen sowie die Aussonderung von Verschlusssachen sind ausschließlich auf Weisung eines zeichnungsbefugten VS-Bearbeiters durch VS-Registratoren vorzunehmen.

3. Weitergabe von Verschlusssachen

3.1 Beförderung durch Boten

Innerhalb einer geschlossenen Gebäudegruppe können Verschlusssachen durch Boten befördert werden.

VS-VERTRAULICH oder höher eingestufte Verschlusssachen sind dabei in Klebemappen oder Umschlägen zu verschließen. Bei STRENG-GEHEIM eingestuften Verschlusssachen sollen die Klebemappen oder Umschläge in verschlossenen VS-Transportbehältern mit Zählwerk oder in anderen Transportmitteln mit vergleichbarem Schutzniveau befördert werden.

Der Klebestreifen oder Umschlag muss neben der Unterschrift des Absenders die Aufschrift tragen:

„STRENG GEHEIM/GEHEIM/VS-VERTRAULICH – diese Mappe/dieser Umschlag darf nur von [Name des Adressaten] oder dem STRENG GEHEIM/GEHEIM/VS-VERTRAULICH ermächtigten Vertreter geöffnet werden!“

Der Absender hat die erforderlichen Eintragungen im VS-Quittungsbuch vorzunehmen. Das VS-Quittungsbuch ist dem Boten mitzugeben.

Der Bote hat die Verschlusssache unverzüglich zu befördern und bis zu ihrer Ablieferung im persönlichen Gewahrsam zu halten. Kann eine STRENG GEHEIM eingestufte Verschlusssache nicht sofort zugestellt werden, so ist sie dem Absender oder der zuständigen VS-Registratur zur einstweiligen Aufbewahrung unmittelbar zurückzugeben.

Der Empfänger hat die Unversehrtheit des Verschlusses der Klebemappe oder des Umschlages zu prüfen und ihn persönlich zu öffnen. Er hat anhand der Eintragungen im VS-Quittungsbuch die für die Beförderung benötigte Zeit sowie bei VS-Transportbehältern den Zählwerkstand zu prüfen, das Datum, die Uhrzeit und bei VS-Transportbehältern den Zählwerkstand in das VS-Quittungsbuch einzutragen und den Erhalt der Verschlusssache durch Unterschrift zu quittieren.

Der Absender hat auf baldige Rückgabe des Quittungsbuches zu achten.

Verschlusssachen, die den Vermerk „Persönlich“ oder „Nicht durch die Registratur zu öffnen“ tragen, sind dem Empfänger ungeöffnet mit einem VS-Begleitzettel zuzuleiten. Der Empfänger kann eine solche Verschlusssache von der Weitergabe in den Geschäftsgang ausschließen, wenn es der Grundsatz „Kenntnis nur, wenn nötig“ erfordert. In diesem Falle wird der VS-Registratur nur der ausgefüllte VS-Begleitzettel zugeleitet.

Vorzimmerberechtigte sollen VS-VERTRAULICH oder höher eingestufte Verschlusssachen grundsätzlich persönlich entgegennehmen. Die Geheimschutzbeauftragten können mit Zustimmung der zuständigen obersten Bundesbehörde Ausnahmen zulassen, zum Beispiel bei hohem Aufkommen an Verschlusssachen, die Annahme durch Vorzimmerkräfte erlauben. Die Ausnahmeregelung ist in der Geheimschutzdokumentation nachzuweisen.

3.2 Versand durch VS-Kurier oder privaten Zustelldienst

Zwischen zwei getrennt liegenden Gebäuden, die nicht zu einer geschlossenen Gebäudegruppe gehören, können Verschlusssachen bis zum Geheimhaltungsgrad GEHEIM durch VS-Kurier oder privaten Zustelldienst versandt werden.

STRENG GEHEIM eingestufte Verschlusssachen sind durch VS-Kurier zu versenden.

3.2.1 Versand durch VS-Kurier

VS-VERTRAULICH oder höher eingestufte Verschlusssachen, die durch VS-Kurier versandt werden, sind in verschlossenen Umschlägen zu verpacken, die mit dem Geheimhaltungsgrad der enthaltenen Verschlusssache zu kennzeichnen sind. Die In-Empfangnahme der Verschlusssache ist von dem VS-Kurier im Quittungsbuch des Absenders zu quittieren. Der Verschlusssache ist ein ausgefüllter VS-Empfangsschein beizufügen.

VS-Kuriere haben für den Transport einen äußerlich neutralen, verschlossenen VS-Transportbehälter mit Zählwerkschloss zu nutzen. An verdeckter Stelle ist die Anschrift der Dienststelle anzubringen.

VS-Kuriere, die STRENG GEHEIM oder GEHEIM eingestufte Verschlusssachen befördern, sollen einen Dienstwagen nutzen. Ist dies nicht möglich, sind STRENG GEHEIM eingestufte Verschlusssachen mit mindestens zwei VS-Kurieren zu befördern.

VS-Kuriere haben die Verschlusssache ständig in persönlichen Gewahrsam zu halten. Ist dies nicht möglich, hat die Aufbewahrung nach § 23 zu erfolgen.

Als VS-Kurier kann jede ausreichend ermächtigte oder zugelassene Person eingesetzt werden.

Der Empfänger hat die Unversehrtheit des Verschlusses des Umschlages zu prüfen und ihn persönlich zu öffnen. Er hat den Zählwerkstand des VS-Transportbehälters zu prüfen, in den VS-Empfangsschein einzutragen und diesen an den Absender unterschrieben zurückzusenden. Geht der VS-Empfangsschein innerhalb einer angemessenen Frist (in der Regel eine Woche) nicht beim Absender ein, hat sich dieser beim Empfänger nach dem Verbleib zu erkundigen.

3.2.2 Versand an Auslandsvertretungen der Bundesrepublik Deutschland

An Auslandsvertretungen der Bundesrepublik Deutschland sind VS-VERTRAULICH oder höher eingestufte Verschlusssachen durch den Kurierdienst des Auswärtigen Amtes oder mittels technischer Kommunikationsverbindungen nach § 55 zu versenden.

3.2.3 Versand durch privaten Zustelldienst

Sollen VS-VERTRAULICH oder GEHEIM eingestufte Verschlusssachen, durch privaten Zustelldienst versandt werden, muss dieser gewährleisten, dass

1. die Zustellung der Sendung bis zum Mittag des folgenden Arbeitstages erfolgt,

2. die Annahme und Zustellung der Sendung nachgewiesen werden und

3. die Sendung lückenlos von der Annahme bis zur Zustellung nachverfolgt werden kann.

VS-VERTRAULICH oder GEHEIM eingestufte Verschlusssachen, die durch privaten Zustelldienst versandt werden, sind in doppelten Umschlägen zu verschließen. Der innere Umschlag enthält die Verschlusssache und darf nicht mehr als einen Vorgang enthalten.

Die inneren Umschläge sind mit folgenden Angaben zu versehen:

1. dem Empfänger und Absender,

2. der Bezeichnung des Empfangsberechtigten mit dem Zusatz „oder Vertreter im Amt (o.V.i.A.)“ oder „Persönlich“ sowie

3. die Aufschrift:

> „GEHEIM/VS-VERTRAULICH – dieser Umschlag darf nur von [Name des Adressaten] oder dem GEHEIM/VS-VERTRAULICH ermächtigten Vertreter geöffnet werden!“

Dem inneren Umschlag ist ein ausgefüllter VS-Empfangsschein beizufügen.

Der äußere Umschlag darf nur die für die Zustellung erforderlichen Angaben sowie den Absender enthalten. Er darf insbesondere keine Zusätze aufweisen, die Rückschluss auf den Inhalt zulassen oder in anderer Weise auf eine Sonderbehandlung der Sendung hindeuten.

Der Empfänger hat die Unversehrtheit der Verschlüsse der Umschläge zu prüfen, diese persönlich zu öffnen, den Empfangsschein auszufüllen und an den Absender zurückzusenden. Geht der VS-Empfangsschein innerhalb einer angemessenen Frist (in der Regel eine Woche) nicht beim Absender ein, hat sich dieser beim Empfänger nach dem Verbleib zu erkundigen.

Für den Versand von Paketen gelten die vorstehenden Bestimmungen entsprechend.

Anlage V
Verschlusssachenanweisung

Merkblatt zur Behandlung von Verschlusssachen des Geheimhaltungsgrades VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD-Merkblatt)

[Vom Abdruck wurde abgesehen.]

Anlage VI
Verschlusssachenanweisung

Richtlinie für die Abgabe von Verschlusssachen an das Geheimarchiv des Bundesarchivs (VS-Archivrichtlinie)

[Vom Abdruck wurde abgesehen.]

Anlage VII
Verschlusssachenanweisung

Hinweise zur Handhabung von Verschlusssachen ausländischer Staaten sowie über- oder zwischenstaatlicher Organisationen

[Vom Abdruck wurde abgesehen.]

Anlage VIII
Verschlusssachenanweisung

Muster

Muster 1	Nachweis über die Verpflichtung (zu § 4 Abs. 1 VSA)
Muster 2	Nachweis über die Ermächtigung (zu § 4 Abs. 2 VSA), Nachweis über die Zulassung (zu § 4 Abs. 3 VSA), Nachweis über die Verpflichtung (zu § 4 Abs. 2 und Abs. 3 VSA)
Muster 3	Nachweis über die Wiederholung der Belehrung und Unterrichtung (zu § 4 VSA)
Muster 4	Konferenzbescheinigung (zu § 4 VSA)
Muster 5	Nachweis über die Aufhebung/ die Einschränkung/ das Erlöschen der Ermächtigung/ der Zulassung, Unterrichtung und Ablieferung der Verschlusssachen und des Quittungsbuchs (zu § 4 Abs. 6 und 7 VSA)
Muster 6	Ausfertigung einer Verschlusssache STRENG GEHEIM (zu § 20 VSA)
Muster 7	Ausfertigung einer Verschlusssache GEHEIM (zu § 20 VSA)
Muster 8	Anlage zu einer Verschlusssache am Beispiel einer Verschlusssache des Geheimhaltungsgrades GEHEIM (zu § 20 VSA)
Muster 9	Ausfertigung einer Verschlusssache VS-VERTRAULICH (zu § 20 VSA)
Muster 10	Ausfertigung einer Verschlusssache VS-NUR FÜR DEN DIENSTGEBRAUCH (zu § 20 VSA)
Muster 11	Entwurf einer E-Mail bei Übermittlung einer Verschlusssache VS-NUR FÜR DEN DIENSTGEBRAUCH (zu § 20 VSA)
Muster 12	Verschlusssache mit unterschiedlich eingestuften Teilen (zu § 20 VSA)
Muster 13	Kennzeichnung für VS-Datenträger (hier: CD-ROM) (zu § 20 VSA)
Muster 14	Kennzeichnung der Hülle für VS-Datenträger (hier: CD-ROM) (zu § 20 VSA)
Muster 15	Kennzeichnung für VS-Datenträger (hier: USB-Stick) (zu § 20 VSA)
Muster 16	VS-Empfangsschein (zu § 21 VSA)
Muster 17	VS-Bestandsverzeichnis (zu § 21 VSA)
Muster 18	VS-Quittungsbuch (zu § 21 VSA)
Muster 19	VS-Begleitzettel (zu § 21 VSA)
Muster 20	VS-Übergabeprotokoll (zu § 21 VSA)
Muster 21	VS-Vernichtungsprotokoll (zu § 21 VSA)
Muster 22	Umschläge für VS-Sendungen (zu § 24 VSA)
Muster 23	Vereinbarung zu Sicherheitsbestimmungen ausgetauschter Verschlusssachen (zu §§ 34, 35 VSA)
Muster 24	Deutscher VS-Versandschein (zu §§ 34, 35 VSA)
Muster 25	Internationaler Empfangsschein (zu §§ 34, 35 VSA)
Muster 26	Nachweis über die Belehrung über die Behandlung von Kryptomaterial (zu § 62 VSA)

Muster 27	Nachweis über die Kryptoberechtigung, ihre Einschränkung, Aufhebung oder ihr Erlöschen (zu § 62 VSA)
Muster 28	Vorblatt zum Verzeichnis für die Abgabe von VS an das Geheimarchiv (zu Anlage VI VSA)
Muster 29	Abgabeverzeichnis (zu Anlage VI VSA)
Muster 30	Dokumentenverzeichnis (zu Anlage VI VSA)
Muster 31	PSCC NATO (zu Anlage VII VSA)
Muster 32	PSCC EU (zu Anlage VII VSA)
Muster 33	PSCC ESA (zu Anlage VII VSA)
Muster 34	Markierung nichtdeutscher VS (Beispiele) (zu Anlage VII VSA)

[Vom Abdruck wurde abgesehen.]

Verordnung zur Feststellung der Behörden des Bundes mit Aufgaben von vergleichbarer Sicherheitsempfindlichkeit wie die der Nachrichtendienste des Bundes und zur Feststellung der öffentlichen Stellen des Bundes und der nichtöffentlichen Stellen mit lebens- oder verteidigungswichtigen Einrichtungen (Sicherheitsüberprüfungsfeststellungsverordnung - SÜFV)

Eingangsformel

Auf Grund des § 34 des Sicherheitsüberprüfungsgesetzes, der durch Artikel 1 Nummer 37 des Gesetzes vom 16. Juni 2017 (BGBl. I S. 1634) neu gefasst worden ist, verordnet die Bundesregierung:

Teil 1
Feststellung der Behörden des Bundes mit Aufgaben von vergleichbarer Sicherheitsempfindlichkeit wie die der Nachrichtendienste des Bundes

§ 1 Aufgaben mit vergleichbarer Sicherheitsempfindlichkeit

Folgende Behörden des Bundes nehmen Aufgaben von vergleichbarer Sicherheitsempfindlichkeit wie die der Nachrichtendienste des Bundes wahr, soweit dabei jeweils eine dauerhafte Zusammenarbeit mit den Nachrichtendiensten des Bundes erfolgt:

1. die Bundespolizei, soweit sie Aufgaben nach § 10 des Bundespolizeigesetzes auf dem Gebiet der Funktechnik und funkbetrieblichen Auswertung wahrnimmt;
2. das Bundeskriminalamt, soweit es seine polizeiliche Aufgabe wahrnimmt auf den Gebieten der Spionageabwehr, der Extremismus- und Terrorismusbekämpfung, des Personenschutzes und der Strafverfolgung in Erscheinungsformen der organisierten Kriminalität;
3. die Bundeswehr, soweit sie Aufgaben der militärischen Aufklärung wahrnimmt, insbesondere solche der Fernmelde- und der elektronischen Aufklärung;
4. das Zollkriminalamt, soweit es
   a) bei seiner Aufgabe der Verhütung und Verfolgung von Zuwiderhandlungen gegen Bestimmungen des Außenwirtschaftsgesetzes und Kriegswaffenkontrollgesetzes tätig wird,
   b) bei der Strafverfolgung von Erscheinungsformen der organisierten Kriminalität tätig wird oder
   c) Aufgaben nach § 3 Absatz 7 Nummer 3 des Zollfahndungsdienstgesetzes wahrnimmt;
5. der Generalbundesanwalt, soweit diesem Informationen der Nachrichtendienste des Bundes wegen seiner Zuständigkeit nach § 142a in Verbindung mit § 120 Absatz 1 und 2 des Gerichtsverfassungsgesetzes übermittelt werden;
6. die Zentralstelle für Finanztransaktionsuntersuchungen, soweit sie Aufgaben nach § 28 des Geldwäschegesetzes zur Verhinderung, Aufdeckung und Unterstützung bei der Bekämpfung von Geldwäsche und Terrorismusfinanzierung wahrnimmt;

7. die Zentrale Stelle für Informationstechnik im Sicherheitsbereich, soweit sie die in § 2 des Erlasses über die Errichtung der Zentralen Stelle für Informationstechnik im Sicherheitsbereich vom 6. April 2017 (GMBl S. 274) genannten Aufgaben zur Unterstützung und Beratung der Nachrichtendienste des Bundes wahrnimmt;
8. das Bundesamt für Sicherheit in der Informationstechnik, soweit es seine Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, Nummer 13 Satz 1 Buchstabe b und c, Nummer 15 und Nummer 18 des BSI-Gesetzes wahrnimmt.

Teil 2
Feststellung der lebens- oder verteidigungswichtigen Einrichtungen im Sinne des § 1 Absatz 4 des Sicherheitsüberprüfungsgesetzes

Abschnitt 1
Feststellung des öffentlichen Bereichs

§ 2 Deutscher Bundestag

Lebenswichtige Einrichtungen sind der Polizeivollzugsdienst beim Deutschen Bundestag und die technischen Arbeitseinheiten des Deutschen Bundestages, deren Ausfall die Tätigkeit des Deutschen Bundestages erheblich beeinträchtigen würde.

§ 3 Bundesrat

Lebenswichtige Einrichtungen sind die technischen Arbeitseinheiten des Bundesrates, deren Ausfall die Tätigkeit des Bundesrates erheblich beeinträchtigen würde.

§ 4 Bundesverfassungsgericht

Lebenswichtige Einrichtungen sind die Arbeitseinheiten, die den Betrieb der Informations- und Kommunikationstechnik des Bundesverfassungsgerichts sicherstellen und deren Ausfall die Tätigkeit des Bundesverfassungsgerichts erheblich beeinträchtigen würde.

§ 5 Deutsche Bundesbank

Lebenswichtige Einrichtungen sind die Arbeitseinheiten, die den Betrieb der Informations- und Kommunikationstechnik der Deutschen Bundesbank beim unbaren Großbetragszahlungsverkehr sicherstellen, sowie die Einrichtungen der zentralen Bargeldversorgung.

§ 6 Oberste Bundesbehörden

Lebenswichtige Einrichtungen in den obersten Bundesbehörden sind die Arbeitseinheiten, die den Betrieb der Informations- und Kommunikationstechnik sicherstellen und deren Ausfall die Tätigkeit oberster Bundesbehörden erheblich beeinträchtigen würde.

§ 7 Geschäftsbereiche der obersten Bundesbehörden

Lebenswichtige Einrichtungen in den Geschäftsbereichen der obersten Bundesbehörden sind die Arbeitseinheiten, die den Betrieb der Informations- und Kommunikationstechnik

sicherstellen und deren Ausfall die Tätigkeit oberster Bundesbehörden und ihnen nachgeordneter Behörden sowie Bundesgerichte erheblich beeinträchtigen würde.

§ 8 Bundesministerium des Innern und für Heimat

Lebenswichtige Einrichtung ist im Bundesministerium des Innern und für Heimat unbeschadet von § 6 der Leitungsbereich für den Zivil- und Katastrophenschutz.

§ 9 Geschäftsbereich des Bundesministeriums des Innern und für Heimat

Lebenswichtige Einrichtungen sind im Geschäftsbereich des Bundesministeriums des Innern und für Heimat unbeschadet von § 7

1. das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe,
2. die Bundesanstalt Technisches Hilfswerk und
3. die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben.

§ 10 Geschäftsbereich des Bundesministeriums für Arbeit und Soziales

Lebenswichtige Einrichtungen sind im Geschäftsbereich des Bundesministeriums für Arbeit und Soziales unbeschadet von § 7 die Arbeitseinheiten, die den Betrieb der Informations- und Kommunikationstechnik zur Gewährung von unterhaltssichernden Leistungen durch die Bundesagentur für Arbeit sowie von Leistungen zur Daseinsvorsorge bei Sozialversicherungsträgern oder für Sozialversicherungsträger sicherstellen.

§ 11 Bundesministerium für Gesundheit

Lebenswichtige Einrichtungen sind im Geschäftsbereich des Bundesministeriums für Gesundheit unbeschadet von § 7 im Institut mit der Aufgabe der Beobachtung des Auftretens und der Bekämpfung von Krankheiten und relevanten Gesundheitsgefahren in der Bevölkerung der Leitungsbereich, alle Abteilungsleitungen einschließlich der Vorzimmer und darüber hinaus diejenigen Arbeitsbereiche, die für die Prävention und Kontrolle von biologischen Gefahrenlagen auf nationaler oder internationaler Ebene zuständig sind.

§ 12 Geschäftsbereich des Bundesministeriums für Ernährung und Landwirtschaft

Lebenswichtige Einrichtungen sind im Geschäftsbereich des Bundesministeriums für Ernährung und Landwirtschaft unbeschadet von § 7 Arbeitseinheiten wissenschaftlicher Einrichtungen, die in erheblichem Umfang mit hochtoxischen Stoffen oder pathogenen Mikroorganismen arbeiten.

Abschnitt 2
Feststellung des nichtöffentlichen Bereichs

§ 13 Bundesministerium des Innern und für Heimat

Lebenswichtige Einrichtungen sind im Zuständigkeitsbereich des Bundesministeriums des Innern und für Heimat die Teile von Unternehmen, die mit dem Aufbau oder Betrieb des Digitalfunks der Behörden und Organisationen mit Sicherheitsaufgaben sowie der Netze des Bundes beauftragt sind und deren Ausfall den Aufbau oder Betrieb des Digitalfunks der Behörden und Organisationen mit Sicherheitsaufgaben sowie der Netze des Bundes erheblich beeinträchtigen würde.

§ 14 Bundesministerium der Finanzen

Lebenswichtige Einrichtungen sind im Zuständigkeitsbereich des Bundesministeriums der Finanzen die Teile von Unternehmen, die durch das Informationstechnikzentrum Bund mit dem Aufbau oder Betrieb der Informations- und Kommunikationstechnik des Bundes beauftragt sind und deren Ausfall die Tätigkeit oberster Bundesbehörden und ihnen nachgeordneter Behörden erheblich beeinträchtigen würde.

§ 15 Auswärtiges Amt

Lebenswichtige Einrichtungen sind im Zuständigkeitsbereich des Auswärtigen Amtes die Teile von Unternehmen, die mit dem Aufbau oder Betrieb der Auslandsinformations- und -kommunikationstechnik gemäß § 9 des Gesetzes über den Auswärtigen Dienst beauftragt sind und deren Ausfall die Tätigkeit oberster Bundesbehörden erheblich beeinträchtigen würde.

§ 16 Bundesministerium für Wirtschaft und Klimaschutz

(1) Lebenswichtige Einrichtungen sind im Zuständigkeitsbereich des Bundesministeriums für Wirtschaft und Klimaschutz

1. die Teile von Unternehmen, die Leitstellen für das Elektrizitätsübertragungsnetz betreiben, deren Ausfall die überregionale Elektrizitätsversorgung erheblich beeinträchtigen kann,
2. die Teile von Unternehmen, die Leitstellen für Elektrizitätsverteilernetze betreiben, deren maximale Entnahme- oder Rückspeiseleistung aus dem Elektrizitätsübertragungsnetz über der von deutschen Übertragungsnetzbetreibern in der Frequenzhaltungsreservekooperation der Übertragungsnetzbetreiber vorgehaltenen Primärregelleistung liegt,
3. die Teile von Unternehmen, die Verdichterstationen und Importstationen für Gasmessungen und Druckminderungen importierter Gasmengen an Netzkopplungspunkten im Gasnetz zwischen einem Netzbetreiber im Ausland und einem Netzbetreiber in Deutschland betreiben, deren Ausfall die überregionale Gasversorgung erheblich beeinträchtigen kann.

(2) Verteidigungswichtige Einrichtungen im Sinne von § 1 Absatz 5 Satz 2 des Sicherheitsüberprüfungsgesetzes sind im Zuständigkeitsbereich des Bundesministeriums für Wirtschaft und Klimaschutz die Teile von Unternehmen, die unmittelbar dem Bau, der Wartung oder der Reparatur von wehrtechnischen Fahrzeugen, wehrtechnischem Material oder von Marineschiffen dienen. Soweit sicherheitsempfindliche Stellen dieser Einrichtungen nicht bereits der Sicherheitsüberprüfung durch das Bundesministerium für Wirtschaft und Klimaschutz unterliegen, teilt das Bundesministerium der Verteidigung im Einvernehmen mit

dem Bundesministerium des Innern und für Heimat die sicherheitsempfindlichen Stellen dem Bundesministerium für Wirtschaft und Klimaschutz mit.

§ 17 Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz

Lebenswichtige Einrichtungen sind, soweit der Betrieb nicht ausreichend durch organisatorische oder technische Maßnahmen gegen Eingriffe Unbefugter geschützt und dies im Sicherheitsbericht nach § 9 der Störfall-Verordnung dokumentiert ist, im Zuständigkeitsbereich des Bundesministeriums für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz

1. die Teile von Unternehmen, die als Betriebsbereich in den Anwendungsbereich des § 1 Absatz 1 Satz 2 der Störfall-Verordnung fallen, und
2. die Teile von Unternehmen, die nach § 1 Absatz 2 der Störfall-Verordnung Betriebsbereichen nach Nummer 1 gleichgestellt sind.

§ 18 Bundesministerium für Digitales und Verkehr

Lebenswichtige Einrichtungen sind im Zuständigkeitsbereich des Bundesministeriums für Digitales und Verkehr

1. die Teile von Telekommunikationsunternehmen, die Telekommunikationsanlagen im Sinne des § 3 Nummer 60 des Telekommunikationsgesetzes betreiben, deren Ausfall das Bereitstellen oder Aufrechterhalten der Übertragungswege oder der aufrechtzuerhaltenden Telekommunikationsdienste nach Teil 10 Abschnitt 2 des Telekommunikationsgesetzes erheblich beeinträchtigen kann;
2. die Leitstellen von Unternehmen, die mit Eisenbahnen Personen oder Güter befördern;
3. die Teile von Unternehmen, in denen folgende Sicherungspläne verantwortlich erstellt werden oder die zu diesen vollständigen Sicherungsplänen Zugang haben:
   a) Sicherungspläne nach Unterabschnitt 1.10.3.2 der Anlage A zu dem Europäischen Übereinkommen vom 30. September 1957 über die internationale Beförderung gefährlicher Güter auf der Straße (ADR) in der Fassung der Bekanntmachung vom 16. November 2021 (BGBl. 2021 II S. 1184), die zuletzt nach Maßgabe der 29. ADR-Änderungsverordnung vom 22. November 2022 (BGBl. 2022 II S. 601) geändert worden ist, in der jeweils geltenden Fassung,
   b) Sicherungspläne nach Unterabschnitt 1.10.3.2 der Ordnung für die internationale Eisenbahnbeförderung gefährlicher Güter (RID) in der Fassung der Bekanntmachung vom 22. April 2022 (BGBl. 2022 II S. 279), die zuletzt durch die mit der 23. RID-Änderungsverordnung vom 3. November 2022 veröffentlichten Änderungen (BGBl. 2022 II S. 555) geändert worden ist, in der jeweils geltenden Fassung und
   c) Sicherungspläne nach Unterabschnitt 1.10.3.2 der Anlage zu dem Europäischen Übereinkommen vom 26. Mai 2000 über die internationale Beförderung von gefährlichen Gütern auf Binnenwasserstraßen (ADN) (BGBl. 2007 II S. 1906, 1908), die zuletzt nach Maßgabe der 9. ADN-Änderungsverord-

nung vom 14. Dezember 2022 (BGBl. 2022 II S. 690) geändert worden ist, in der jeweils geltenden Fassung.

Abschnitt 3
Zuständigkeits- und Schlussvorschriften

§ 19 Zuständigkeit

(1) Zuständig für die Durchführung der Sicherheitsüberprüfungen nach § 13 ist die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben.

(2) Zuständig für die Durchführung der Sicherheitsüberprüfungen nach den §§ 14 bis 18 ist das Bundesministerium für Wirtschaft und Klimaschutz.

§ 20 Inkrafttreten, Außerkrafttreten

Diese Verordnung tritt am Tag nach der Verkündung in Kraft. Gleichzeitig tritt die Sicherheitsüberprüfungsfeststellungsverordnung in der Fassung der Bekanntmachung vom 12. September 2007 (BGBl. I S. 2294), die zuletzt durch Artikel 5 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1858) geändert worden ist, außer Kraft.

Gesetz zum Schutz vor Gefährdung der Sicherheit der Bundesrepublik Deutschland durch das Verbreiten von hochwertigen Erdfernerkundungsdaten

Inhaltsübersicht

Teil 1
Anwendungsbereich

§ 1 Anwendungsbereich
§ 2 Begriffsbestimmungen

Teil 2
Betrieb eines hochwertigen Erdfernerkundungssystems

§ 3 Genehmigung
§ 4 Genehmigungsvoraussetzungen
§ 5 Dokumentationspflicht
§ 6 Anzeigepflicht
§ 7 Auskunftspflicht
§ 8 Betretens- und Prüfungsrechte
§ 9 Maßnahmen der zuständigen Behörde
§ 10 Betriebsübernahme

Teil 3
Verbreiten von Daten

Kapitel 1
Allgemeine Voraussetzungen

§ 11 Zulassung
§ 12 Zulassungsvoraussetzungen
§ 13 Anzeigepflicht
§ 14 Auskunftspflicht
§ 15 Betretens- und Prüfungsrechte
§ 16 Maßnahmen der zuständigen Behörde

Kapitel 2
Verfahren des Verbreitens von Daten

§ 17 Sensitivitätsprüfung

§ 18 Dokumentationspflicht
§ 19 Erlaubnis
§ 20 Sammelerlaubnis

Teil 4
Vorrangige Bedienung von Anfragen der Bundesrepublik Deutschland

§ 21 Verpflichtung des Datenanbieters
§ 22 Verpflichtung des Betreibers
§ 23 Vergütung

Teil 5
Durchführungsvorschriften

§ 24 Zuständigkeit
§ 25 Verfahren
§ 26 (weggefallen)
§ 27 Übermittlung von personenbezogenen Daten, Betriebs- und Geschäftsgeheimnissen

Teil 6
Bußgeldvorschriften, Strafvorschriften

§ 28 Ordnungswidrigkeiten
§ 29 Straftaten
§ 30 Auslandstaten Deutscher
§ 31 Straf- und Bußgeldverfahren

Teil 7
Übergangs- und Schlussbestimmungen

§ 32 Änderung des Bundesverfassungsschutzgesetzes
§ 33 Änderung des Sicherheitsüberprüfungsgesetzes
§ 34 Übergangsregelung
§ 35 Inkrafttreten

Teil 1
Anwendungsbereich

§ 1 Anwendungsbereich

(1) Dieses Gesetz gilt

1. für den Betrieb von hochwertigen Erdfernerkundungssystemen
   a) durch deutsche Staatsangehörige, juristische Personen oder Personenvereinigungen deutschen Rechts,
   b) durch ausländische juristische Personen oder Personenvereinigungen, die ihren Verwaltungssitz im Bundesgebiet haben, oder
   c) soweit das unveränderbare Absetzen der Befehlsfolgen zur Kommandierung des Orbitalsystems vom Bundesgebiet aus erfolgt;
2. für den Umgang mit den Daten, die von einem hochwertigen Erdfernerkundungssystem nach Nummer 1 erzeugt worden sind, bis zu deren Verbreiten
   a) durch deutsche Staatsangehörige, juristische Personen oder Personenvereinigungen deutschen Rechts,
   b) durch ausländische juristische Personen oder Personenvereinigungen, die ihren Verwaltungssitz im Bundesgebiet haben, oder
   c) soweit das Verbreiten der Daten vom Bundesgebiet aus erfolgt.

(2) Dieses Gesetz gilt nicht für den Betrieb hochwertiger Erdfernerkundungssysteme durch eine staatliche Stelle mit militärischen oder nachrichtendienstlichen Aufgaben, soweit die Kenntnisnahme der erzeugten Daten durch Unbefugte ausgeschlossen ist. Von der Anwendung des Gesetzes ist abzusehen, wenn der Betrieb eines hochwertigen Erdfernerkundungssystems nach den Rechtsvorschriften eines anderen Mitgliedstaates der Europäischen Union erlaubt ist und diese Rechtsvorschriften den Regelungen und Schutzinteressen dieses Gesetzes vergleichbar sind. Die zuständige Behörde kann von der Anwendung des Gesetzes absehen, soweit die Rechtsvorschriften eines Drittstaates die Voraussetzungen des Satzes 2 erfüllen und eine völkerrechtliche Vereinbarung zwischen dem Drittstaat und der Bundesrepublik Deutschland besteht, in der die Vergleichbarkeit der Regelungen und Schutzinteressen festgestellt ist.

§ 2 Begriffsbestimmungen

(1) Im Sinne dieses Gesetzes

1. ist Betreiber:
   wer das Erdfernerkundungssystem in eigener Verantwortung steuert;
2. sind Daten:
   Signale eines Sensors oder mehrerer Sensoren eines Orbital- oder Transportsystems und alle daraus abgeleiteten Produkte, unabhängig vom Grad ihrer Verarbeitung und der Art ihrer Speicherung oder Darstellung; Datum im Sinne des § 27 ist jede Einzelangabe;

3. ist Datenanbieter:
wer Daten, die von einem hochwertigen Erdfernerkundungssystem erzeugt worden sind, verbreitet;

4. ist ein hochwertiges Erdfernerkundungssystem:
ein raumgestütztes Transport- oder Orbitalsystem, einschließlich des Bodensegments, mit dem Daten über die Erde erzeugt werden, soweit dessen Sensor oder Sensoren selbst oder in Kombination mit einem oder mehreren anderen Sensoren technisch in der Lage ist, Daten mit besonders hohem Informationsgehalt im Sinne von Absatz 2 zu erzeugen;

5. ist ein Sensor:
ein Teil eines raumgestützten Erdfernerkundungssystems, das elektromagnetische Wellen aller Spektralbereiche oder gravimetrische Felder aufzeichnet;

6. ist Verbreiten:
das Inverkehrbringen oder das Zugänglichmachen der Daten für Dritte.

(2) Das Bundesministerium für Wirtschaft und Energie hat durch Rechtsverordnung ohne Zustimmung des Bundesrates Bestimmungen zu erlassen, unter welchen Voraussetzungen Daten einen besonders hohen Informationsgehalt haben. Der Informationsgehalt ist dabei zu bestimmen nach

1. der geometrischen Auflösung,
2. der spektralen Abdeckung,
3. der Zahl der Spektralkanäle und der spektralen Auflösung,
4. der radiometrischen Auflösung und
5. der zeitlichen Auflösung.

Bei Mikrowellen- oder Radarsensoren ist der Informationsgehalt auch zu bestimmen nach

1. den Polarisationsmerkmalen und
2. der Phasengeschichte.

Die Bestimmungen berücksichtigen die möglichen Auswirkungen, die ein Verbreiten von Daten mit besonders hohem Informationsgehalt auf die wesentlichen Sicherheitsinteressen der Bundesrepublik Deutschland, das friedliche Zusammenleben der Völker und die auswärtigen Beziehungen der Bundesrepublik Deutschland hat.

Teil 2
Betrieb eines hochwertigen Erdfernerkundungssystems

§ 3 Genehmigung

(1) Der Betrieb eines hochwertigen Erdfernerkundungssystems bedarf der Genehmigung.

(2) Nachträgliche Änderungen der Genehmigung sind zulässig, wenn dies erforderlich ist, um die Einhaltung der Genehmigungsvoraussetzungen im Falle nachträglich eingetretener Tatsachen oder einer geänderten Rechtsvorschrift sicherzustellen.

(3) Anforderungen anderer Gesetze an den Betrieb eines hochwertigen Erdfernerkundungssystems bleiben unberührt. Die Genehmigung wird unbeschadet privater Rechte Dritter erteilt.

(4) Ist ein raumgestütztes Erdfernerkundungssystem nicht hochwertig, so hat die zuständige Behörde dies auf Antrag des Betreibers festzustellen. Entfällt nachträglich das Genehmigungserfordernis durch Änderung der Bestimmungen nach § 2 Abs. 2, so erlischt die Genehmigung.

§ 4 Genehmigungsvoraussetzungen

(1) Die Genehmigung ist zu erteilen, wenn

1. der Betreiber des hochwertigen Erdfernerkundungssystems die erforderliche Zuverlässigkeit besitzt,
2. die Befehlsfolgen zur
   a) Kommandierung des Orbital- oder Transportsystems,
   b) Steuerung des Sensors oder der Sensoren,
   c) Steuerung der Übermittlung der Daten durch das Orbital- oder Transportsystem an ein Bodensegment des Betreibers oder einer nach § 11 zugelassenen Person und
   d) Steuerung des Verbreitens der Daten unmittelbar durch das Orbital- oder Transportsystem

   im Bundesgebiet hergestellt und durch ein vom Bundesamt für Sicherheit in der Informationstechnik geprüftes und für geeignet erklärtes Verfahren gegen Veränderung durch Dritte geschützt werden,
3. die Übermittlung der Daten durch das Orbital- oder Transportsystem an ein Bodensegment des Betreibers oder einer nach § 11 zugelassenen Person, die Übermittlung der Daten zwischen verschiedenen Standorten des Bodensegments des Betreibers und die Übermittlung der Daten vom Betreiber an eine nach § 11 zugelassene Person durch ein vom Bundesamt für Sicherheit in der Informationstechnik geprüftes und für geeignet erklärtes Verfahren gegen unbefugte Kenntnisnahme geschützt sind, und
4. der Betreiber technische und organisatorische Maßnahmen getroffen hat, die verhindern, dass Unbefugte Zugang zu den Anlagen der Kommandierung des hochwertigen Erdfernerkundungssystems sowie zu den Anlagen zum Empfang, zur Verarbeitung und zur Speicherung der Daten oder Zutritt zu den dafür genutzten Betriebsräumen haben.

(2) Der Betreiber hat Personen, welche Zugang zu den Anlagen der Kommandierung eines hochwertigen Erdfernerkundungssystems oder zu den Anlagen zum Empfang, zur Verarbeitung und zur Speicherung der Daten solcher Systeme haben, durch die zuständige Behörde einer einfachen Sicherheitsüberprüfung nach dem Sicherheitsüberprüfungsgesetz unterziehen zu lassen.

§ 5 Dokumentationspflicht

(1) Der Betreiber eines hochwertigen Erdfernerkundungssystems ist verpflichtet,

1. die Befehlsfolgen zur Kommandierung des Orbital- oder Transportsystems,
2. die Befehlsfolgen zur Steuerung des Sensors oder der Sensoren,
3. Angaben zu Verschlüsselungsverfahren, verwendeten Schlüsseln und Schlüsselmanagement und
4. den Zeitpunkt und den Weg der Befehlsfolgen

aufzuzeichnen.

(2) Die Aufzeichnungen nach Absatz 1 sind mindestens fünf Jahre nach Ausführung der jeweiligen Befehlsfolge aufzubewahren und zur Einsichtnahme durch die zuständige Behörde bereitzuhalten.

§ 6 Anzeigepflicht

(1) Der Betreiber eines hochwertigen Erdfernerkundungssystems hat der zuständigen Behörde

1. Änderungen von Tatsachen, die er zur Eintragung in das Handels- oder Vereinsregister anzumelden hat, und
   a) soweit der Betreiber in der Rechtsform einer Personenhandelsgesellschaft tätig ist, Änderungen des Gesellschaftsvertrages oder
   b) soweit der Betreiber in der Rechtsform einer Gesellschaft mit beschränkter Haftung tätig ist, Änderungen in den Personen der Gesellschafter oder des Umfangs ihrer Beteiligung,
2. tatsächliche Anhaltspunkte dafür, dass ein Dritter die Befehlsfolgen zur Kommandierung des Orbital- oder Transportsystems, zur Steuerung des Sensors oder der Sensoren oder zur Steuerung der Übermittlung der Daten vom Orbital- oder Transportsystem absetzt oder abzusetzen versucht, sowie
3. Änderungen der nach § 4 Abs. 1 Nr. 4 getroffenen Maßnahmen

unverzüglich schriftlich oder elektronisch anzuzeigen.

(2) Der Betreiber eines hochwertigen Erdfernerkundungssystems hat der zuständigen Behörde unverzüglich schriftlich oder elektronisch anzuzeigen, an welche nach § 11 zugelassenen Personen er Daten übermittelt.

§ 7 Auskunftspflicht

(1) Der Betreiber eines hochwertigen Erdfernerkundungssystems hat der zuständigen Behörde auf Verlangen Auskünfte zu erteilen und Unterlagen vorzulegen, soweit dies zur Überwachung der Einhaltung dieses Gesetzes und der zu diesem Gesetz erlassenen Rechtsverordnungen erforderlich ist.

(2) Auskunftspflichtige Personen können die Auskunft auf solche Fragen verweigern, deren Beantwortung sie selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozessordnung be-

zeichneten Angehörigen der Gefahr einer strafrechtlichen Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde.

§ 8 Betretens- und Prüfungsrechte

Die Beauftragten der zuständigen Behörde sind befugt, zu den üblichen Betriebs- und Geschäftszeiten die Betriebs- und Geschäftsräume des Betreibers eines hochwertigen Erdfernerkundungssystems zu betreten und die zur Erfüllung ihrer Aufgaben erforderlichen Prüfungen vorzunehmen; die §§ 196, 197 Abs. 1 Satz 1 und 2 und Abs. 2, §§ 198, 199 Abs. 2 und §§ 200 bis 202 der Abgabenordnung gelten entsprechend.

§ 9 Maßnahmen der zuständigen Behörde

(1) Die zuständige Behörde kann gegenüber dem Betreiber eines hochwertigen Erdfernerkundungssystems im Einzelfall diejenigen Maßnahmen anordnen, die zur ordnungsgemäßen Erfüllung seiner Pflichten erforderlich sind.

(2) Die zuständige Behörde kann insbesondere

1. vorübergehend die Übermittlung von Daten an ein Bodensegment oder an eine nach § 11 zugelassene Person untersagen oder
2. anordnen, den Betrieb ganz oder teilweise auf einen geeigneten Sonderbeauftragten zu übertragen.

(3) Die durch die Bestellung des Sonderbeauftragten entstehenden Kosten einschließlich der diesem zu gewährenden Vergütung trägt der Betreiber des hochwertigen Erdfernerkundungssystems. Die zuständige Behörde setzt die Höhe der Vergütung fest.

§ 10 Betriebsübernahme

Die vollständige oder teilweise Übernahme des Betriebs eines hochwertigen Erdfernerkundungssystems oder von Teilen eines solchen bedarf der Erlaubnis, wenn durch die Übernahme die Genehmigungspflicht nach § 3 Abs. 1 entfällt. Der Antrag auf Erteilung der Erlaubnis ist vom Übernehmenden zu stellen. Die Erlaubnis ist zu erteilen, wenn der weitere Betrieb des hochwertigen Erdfernerkundungssystems oder von Teilen des hochwertigen Erdfernerkundungssystems die wesentlichen Sicherheitsinteressen der Bundesrepublik Deutschland nicht gefährdet.

Teil 3
Verbreiten von Daten

Kapitel 1
Allgemeine Voraussetzungen

§ 11 Zulassung

(1) Ein Datenanbieter, der Daten verbreiten will, bedarf der Zulassung.

(2) Nachträgliche Änderungen der Zulassung sind zulässig, wenn dies erforderlich ist, um die Einhaltung der Zulassungsvoraussetzungen im Falle nachträglich eingetretener Tatsachen oder einer geänderten Rechtsvorschrift sicherzustellen.

§ 12 Zulassungsvoraussetzungen

(1) Die Zulassung ist zu erteilen, wenn

1. der Datenanbieter die erforderliche Zuverlässigkeit besitzt,
2. der Datenanbieter technische und organisatorische Maßnahmen getroffen hat, die verhindern, dass Unbefugte Zugang zu den Anlagen zum Empfang, zur Verarbeitung und zur Speicherung von Daten eines hochwertigen Erdfernerkundungssystems oder Zutritt zu den dafür genutzten Betriebsräumen haben,
3. die Übermittlung der Daten zwischen verschiedenen Standorten des Bodensegments des Datenanbieters und die Übermittlung der Daten an einen anderen Datenanbieter durch ein vom Bundesamt für Sicherheit in der Informationstechnik geprüftes und für geeignet erklärtes Verfahren gegen unbefugte Kenntnisnahme geschützt sind und
4. das sichere Verbreiten der von einem hochwertigen Erdfernerkundungssystem erzeugten Daten nach dem Stand der Technik gewährleistet ist.

(2) Der Datenanbieter hat Personen, welche Zugang zu den Anlagen zum Empfang, zur Verarbeitung und zur Speicherung von Daten eines hochwertigen Erdfernerkundungssystems haben, durch die zuständige Behörde einer einfachen Sicherheitsüberprüfung nach dem Sicherheitsüberprüfungsgesetz unterziehen zu lassen.

§ 13 Anzeigepflicht

Der Datenanbieter hat der zuständigen Behörde

1. Änderungen von Tatsachen, die er zur Eintragung in das Handels- oder Vereinsregister anzumelden hat, und
   a) soweit der Datenanbieter in der Rechtsform einer Personenhandelsgesellschaft tätig ist, Änderungen des Gesellschaftsvertrages oder
   b) soweit der Datenanbieter in der Rechtsform einer Gesellschaft mit beschränkter Haftung tätig ist, Änderungen in den Personen der Gesellschafter oder des Umfangs ihrer Beteiligung,
2. Änderungen der nach § 12 Abs. 1 Nr. 2 getroffenen Maßnahmen sowie
3. tatsächliche Anhaltspunkte dafür, dass die Sicherung der Daten, die mit einem hochwertigen Erdfernerkundungssystem erzeugt worden sind, nicht aufrechterhalten wird,

unverzüglich schriftlich oder elektronisch anzuzeigen.

§ 14 Auskunftspflicht

(1) Der Datenanbieter hat der zuständigen Behörde auf Verlangen Auskünfte zu erteilen und Unterlagen vorzulegen, soweit dies zur Überwachung der Einhaltung dieses Gesetzes und der zu diesem Gesetz erlassenen Rechtsverordnungen erforderlich ist.

(2) Der Datenanbieter kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr einer strafrechtlichen Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde.

§ 15 Betretens- und Prüfungsrechte

Die Beauftragten der zuständigen Behörde sind befugt, zu den üblichen Betriebs- und Geschäftszeiten die Betriebs- und Geschäftsräume des Datenanbieters zu betreten und die zur Erfüllung ihrer Aufgaben erforderlichen Prüfungen durchzuführen; die §§ 196, 197 Abs. 1 Satz 1 und 2 und Abs. 2, §§ 198, 199 Abs. 2 und §§ 200 bis 202 der Abgabenordnung gelten entsprechend.

§ 16 Maßnahmen der zuständigen Behörde

Die zuständige Behörde kann gegenüber dem Datenanbieter im Einzelfall diejenigen Maßnahmen anordnen, die zur ordnungsgemäßen Erfüllung seiner Pflichten erforderlich sind. Sie kann insbesondere

1. verlangen, das Verbreiten der Daten dem Stand der Technik anzupassen, oder
2. vorübergehend das Verbreiten von Daten untersagen.

Kapitel 2
Verfahren des Verbreitens von Daten

§ 17 Sensitivitätsprüfung

(1) Der Datenanbieter, der eine Anfrage auf Verbreiten von Daten eines hochwertigen Erdfernerkundungssystems bedienen will, hat die Anfrage nach Maßgabe einer Rechtsverordnung nach Absatz 3 auf ihre Sensitivität zu prüfen.

(2) Eine Anfrage ist sensitiv, wenn

1. der durch den verwendeten Sensorbetriebsmodus und durch die verwendete Verarbeitung erzielte Informationsgehalt der Daten,
2. das mit den Daten dargestellte Zielgebiet,
3. der Zeitpunkt der Erzeugung der Daten und der Zeitraum zwischen der Erzeugung der Daten und der Bedienung der Anfrage und
4. die Bodensegmente, an welche die Daten übermittelt werden sollen,

in ihrer Zusammenschau die Möglichkeit eines Schadenseintritts für die wesentlichen Sicherheitsinteressen der Bundesrepublik Deutschland, das friedliche Zusammenleben der Völker oder die auswärtigen Beziehungen der Bundesrepublik Deutschland ergeben. Die Zusammenschau nach Satz 1 erfolgt in Ansehung der Person des Anfragenden und soll die

Personen berücksichtigen, die bestimmungsgemäß mit den Daten in Kontakt kommen, einschließlich deren gewöhnlichen Aufenthaltsortes. Der Datenanbieter hat dazu die Identität des Anfragenden in geeigneter Weise zu prüfen und die Nennung der Personen einschließlich deren gewöhnlichen Aufenthaltsortes zu verlangen, die bestimmungsgemäß mit den Daten in Kontakt kommen.

(3) Das Bundesministerium für Wirtschaft und Energie hat im Einvernehmen mit dem Bundesministerium der Verteidigung, dem Auswärtigen Amt und dem Bundesministerium des Innern, für Bau und Heimat durch Rechtsverordnung ohne Zustimmung des Bundesrates Bestimmungen zu erlassen, unter welchen Voraussetzungen nach Absatz 2 die Möglichkeit eines Schadenseintritts für die genannten Schutzgüter gegeben ist. Dabei berücksichtigt es regelmäßig zu aktualisierende Feststellungen der Sicherheitsanforderungen der betroffenen Behörden, die Verpflichtungen und Vereinbarungen der Bundesrepublik Deutschland gegenüber den Mitgliedstaaten der Europäischen Union, den Parteien des Nordatlantikvertrages vom 4. April 1949 (BGBl. 1955 II S. 289) in der Fassung des Protokolls vom 17. Oktober 1951 (BGBl. 1955 II S. 293) und gegenüber Australien, Japan, Neuseeland und der Schweiz, den Stand der Technik in Bezug auf die Erzeugung von Daten mit besonders hohem Informationsgehalt, die bestehenden Regelungen, unter denen der Anfragende die Daten weiter übermitteln könnte, und die Verfügbarkeit von vergleichbaren Daten auf internationalen Märkten. In der Rechtsverordnung ist festzulegen, nach welchem Verfahren die Zusammenschau nach Absatz 2 Satz 1 und 2 erfolgt. Die Rechtsverordnung darf dem Datenanbieter keinen eigenen Einschätzungsspielraum belassen, ob eine Anfrage sensitiv ist. Auf bevorstehende Änderungen der Rechtsverordnung kann der Datenanbieter hingewiesen werden. Das Bundesministerium für Wirtschaft und Energie kann im Einvernehmen mit dem Bundesministerium der Verteidigung und dem Auswärtigen Amt die Ermächtigung durch Rechtsverordnung ohne Zustimmung des Bundesrates ganz oder teilweise auf das Bundesamt für Wirtschaft und Ausfuhrkontrolle übertragen.

§ 18 Dokumentationspflicht

(1) Der Datenanbieter ist verpflichtet, alle Anfragen auf Verbreiten von Daten eines hochwertigen Erdfernerkundungssystems aufzuzeichnen. Dies umfasst

1. die Anfrage einschließlich der Personen, die bestimmungsgemäß mit den Daten in Kontakt kommen, und deren gewöhnlichen Aufenthaltsortes,
2. die Prüfung der Identität des Anfragenden,
3. das Verfahren und das Ergebnis der Prüfung auf Sensitivität der Anfrage nach § 17 Abs. 1 in Verbindung mit den Bestimmungen einer Rechtsverordnung nach § 17 Abs. 3,
4. den Auftrag gegenüber dem Betreiber des hochwertigen Erdfernerkundungssystems auf Erzeugung der Daten,
5. die Empfangsprotokolle von Bodensegmenten,
6. die Angaben zu Verschlüsselungsverfahren, verwendeten Schlüsseln und Schlüsselmanagement,
7. die Protokolle der Verarbeitungsketten des Bodensegments,

8. die Metadaten der Daten, insbesondere das Zielgebiet, den Zeitpunkt der Erzeugung der Daten, den Sensorbetriebsmodus und die Parameter der Verarbeitung der Daten,
9. die Transferprotokolle oder Lieferscheine einschließlich Auslieferungsbestätigungen in Bezug auf die Bedienung der Anfrage und
10. die Rechnungen.

Die Sätze 1 und 2 Nr. 4 bis 10 gelten entsprechend, wenn Daten ohne Anfrage verbreitet werden. Wird eine Anfrage auf Verbreiten von Daten eines hochwertigen Erdfernerkundungssystems aus einem Archiv ausgeführt, so ist für die Protokollierung und Dokumentation nach Satz 2 Nr. 4 und 5 ein Verweis auf eine anderweitige Protokollierung und Dokumentation ausreichend.

(2) Die Aufzeichnungen nach Absatz 1 sind mindestens fünf Jahre nach Erzeugung der jeweiligen Daten aufzubewahren und zur Einsichtnahme durch die zuständige Behörde bereitzuhalten.

(3) Der Datenanbieter ist verpflichtet, gleichartige Protokolle und Dokumentationen fremder Bodensegmente bereitzuhalten, die er bei der Bedienung der Anfrage auf Verbreiten von Daten eines hochwertigen Erdfernerkundungssystems einsetzt. Absatz 2 gilt entsprechend.

(4) Der Datenanbieter hat dem Anfragenden die Aufbewahrung der Daten und die Möglichkeit der behördlichen Einsichtnahme mitzuteilen.

§ 19 Erlaubnis

(1) Will ein Datenanbieter eine sensitive Anfrage bedienen, bedarf er der Erlaubnis. Dies gilt auch, wenn er Daten eines hochwertigen Erdfernerkundungssystems ohne Anfrage verbreiten will.

(2) Die Erlaubnis nach Absatz 1 ist zu erteilen, wenn das Verbreiten der Daten im Einzelfall die wesentlichen Sicherheitsinteressen der Bundesrepublik Deutschland nicht gefährdet, das friedliche Zusammenleben der Völker nicht und die auswärtigen Beziehungen der Bundesrepublik Deutschland nicht erheblich stört.

(3) Die zuständige Behörde soll über den Antrag auf Erlaubnis spätestens einen Monat nach Eingang entscheiden.

(4) Die Erlaubnis wird unbeschadet privater Rechte Dritter erteilt.

§ 20 Sammelerlaubnis

Die zuständige Behörde kann eine Sammelerlaubnis erteilen, wenn ein Datenanbieter

1. Darstellungen von Daten mit stark vermindertem Informationsgehalt oder Metadaten für jedermann zugänglich machen oder
2. sensitive Anfragen, die in gleichartiger Weise von derselben Person für eine unbestimmte Anzahl von Daten eines hochwertigen Erdfernerkundungssystems angefragt werden, bedienen will.

Die Sammelerlaubnis ergeht unter den Voraussetzungen des § 19 Abs. 2 und darf nur unter Vorbehalt des Widerrufs erteilt werden. Eine Sammelerlaubnis nach Satz 1 Nr. 1 hat zu bestimmen, welchen Informationsgehalt die Daten höchstens haben dürfen. Eine Sammeler-

laubnis nach Satz 1 Nr. 2 darf nur für eine bestimmte Frist erteilt werden, die drei Jahre nicht überschreiten soll.

Teil 4
Vorrangige Bedienung von Anfragen der Bundesrepublik Deutschland

§ 21 Verpflichtung des Datenanbieters

In folgenden Fällen ist der Datenanbieter verpflichtet, Anfragen der Bundesrepublik Deutschland, vertreten durch das Bundeskanzleramt, auf Verbreiten von Daten gegenüber jeder anderen Anfrage vorrangig zu bedienen:

1. im Bündnisfall gemäß Artikel 5 des Nordatlantikvertrages vom 4. April 1949 (BGBl. 1955 II S. 289) in der Fassung des Protokolls vom 17. Oktober 1951 (BGBl. 1955 II S. 293),
2. im Verteidigungsfall gemäß Artikel 115 Buchstabe a bis l des Grundgesetzes,
3. wenn die Voraussetzungen des inneren Notstandes gemäß Artikel 91 des Grundgesetzes vorliegen,
4. im Spannungsfall gemäß Artikel 80a des Grundgesetzes oder
5. wenn im Ausland eingesetzte militärische oder zivile Kräfte der Bundesrepublik Deutschland oder an den deutschen Auslandsvertretungen tätige Beschäftigte des auswärtigen Dienstes, die einer konkreten Beeinträchtigung der äußeren Sicherheit der Bundesrepublik Deutschland entgegenwirken, gegenwärtig gefährdet sind.

§ 22 Verpflichtung des Betreibers

Der Betreiber eines hochwertigen Erdfernerkundungssystems ist verpflichtet, in den Fällen des § 21 Aufträge zur Erzeugung von Daten für die Bundesrepublik Deutschland gegenüber jedem anderen Auftrag zur Erzeugung von Daten vorrangig zu behandeln. Unbeschadet des Satzes 1 soll die Erdfernerkundungsanfrage der Bundesrepublik Deutschland, vertreten durch das Bundeskanzleramt, bei einem Datenanbieter erfolgen. Erfolgt diese dennoch bei dem Betreiber eines hochwertigen Erdfernerkundungssystems, bedarf dieser zum Verbreiten dieser Daten keiner Zulassung nach § 11.

§ 23 Vergütung

(1) Unbeschadet der Verpflichtungen aus diesem Teil kann für die Erzeugung der Daten nach § 22 sowie für die Bedienung der Anfrage nach § 21 eine Vergütung verlangt werden. Die Vergütung soll dem jeweiligen durchschnittlichen Marktpreis entsprechen.

(2) Weitergehende Ansprüche gegen die Bundesrepublik Deutschland sind ausgeschlossen.

Teil 5
Durchführungsvorschriften

§ 24 Zuständigkeit

(1) Zuständige Behörde nach diesem Gesetz ist vorbehaltlich der Absätze 2 und 3 das Bundesamt für Wirtschaft und Ausfuhrkontrolle.

(2) Zuständig für die Durchführung einer Sicherheitsüberprüfung nach § 4 Abs. 2 und § 12 Abs. 2 ist das Bundesministerium für Wirtschaft und Energie.

(3) (weggefallen)

§ 25 Verfahren

(1) Eine Genehmigung nach § 3 Abs. 1, eine Zulassung nach § 11 Absatz 1 und eine Erlaubnis nach § 10 Satz 1 setzen jeweils einen schriftlichen Antrag voraus. Eine Erlaubnis nach § 19 Absatz 1 Satz 1 und 2 sowie nach § 20 Satz 1 setzt einen schriftlichen oder elektronischen Antrag voraus. Einem Antrag sind die zur Prüfung der Erteilungsvoraussetzungen notwendigen Unterlagen beizufügen.

(2) Zur Feststellung der Eignung eines Verfahrens nach § 4 Absatz 1 Nummer 2 und 3 sowie § 12 Absatz 1 Nummer 3 ist das Bundesamt für Sicherheit in der Informationstechnik frühzeitig zu beteiligen. Das Bundesamt für Sicherheit in der Informationstechnik stellt dem Antragsteller Unterlagen zum Umfang und Ablauf der Prüfung zur Verfügung.

(3) Verwaltungsakte nach diesem Gesetz sind schriftlich oder elektronisch zu erlassen.

§ 26 (weggefallen)

§ 27 Übermittlung von personenbezogenen Daten, Betriebs- und Geschäftsgeheimnissen

(1) Die zuständige Behörde kann personenbezogene Daten, die ihr bei der Erfüllung ihrer Aufgaben nach diesem Gesetz bekannt geworden sind, an andere Behörden übermitteln, soweit die Kenntnis der personenbezogenen Daten aus ihrer Sicht erforderlich ist

1. zur Abwehr einer Gefahr für die wesentlichen Sicherheitsinteressen der Bundesrepublik Deutschland oder zur Verhinderung einer Störung des friedlichen Zusammenlebens der Völker oder einer erheblichen Störung der auswärtigen Beziehungen der Bundesrepublik Deutschland oder
2. zur Verhütung oder zur Verfolgung von Straftaten.

Eine Übermittlung nach Satz 1 Nr. 2 ist nur zulässig, wenn tatsächliche Anhaltspunkte für die zukünftige Begehung oder das Vorliegen von Straftaten bestehen. Darüber hinaus kann die zuständige Behörde diese personenbezogenen Daten an den Bundesnachrichtendienst übermitteln, wenn die Voraussetzungen des § 10 Absatz 3 des BND-Gesetzes erfüllt sind. Der Dritte, an den die personenbezogenen Daten übermittelt werden, darf diese nur für den Zweck verwenden, zu dessen Erfüllung sie übermittelt werden.

(2) In Strafverfahren wegen eines Verstoßes gegen dieses Gesetz dürfen Gerichte und Staatsanwaltschaften obersten Bundesbehörden personenbezogene Daten übermitteln, wenn dies zur Abwehr einer Gefahr für die wesentlichen Sicherheitsinteressen der Bundesrepublik Deutschland oder zur Verhinderung einer Störung des friedlichen Zusammenlebens der Völker oder einer erheblichen Störung der auswärtigen Beziehungen der Bundesrepublik Deutschland erforderlich ist. Die nach Satz 1 erlangten personenbezogenen Daten dürfen

nur zu den dort genannten Zwecken verwendet werden. Der Dritte, an den die personenbezogenen Daten übermittelt werden, darf diese an eine nicht in Satz 1 genannte öffentliche Stelle zudem nur weiter übermitteln, wenn das Interesse an der Verwendung der übermittelten personenbezogenen Daten das Interesse des Betroffenen an der Geheimhaltung erheblich überwiegt und der Untersuchungszweck des Strafverfahrens nicht gefährdet werden kann.

(3) Betriebs- und Geschäftsgeheimnisse stehen personenbezogenen Daten gleich.

Teil 6
Bußgeldvorschriften, Strafvorschriften

§ 28 Ordnungswidrigkeiten

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. ohne Genehmigung nach § 3 Abs. 1 ein hochwertiges Erdfernerkundungssystem betreibt,
2. (weggefallen)
3. ohne Erlaubnis
   a) nach § 10 Satz 1 den Betrieb eines hochwertigen Erdfernerkundungssystems oder von Teilen eines solchen übernimmt,
   b) nach § 19 Abs. 1 Satz 1 eine sensitive Anfrage bedient oder
   c) nach § 19 Abs. 1 Satz 2 Daten ohne Anfrage verbreitet,
4. einer vollziehbaren Anordnung nach § 9 Abs. 1, 2 oder § 16 zuwiderhandelt,
5. ohne Zulassung nach § 11 Abs. 1 Daten verbreitet,
6. entgegen § 17 Abs. 1 in Verbindung mit den Bestimmungen einer Rechtsverordnung nach § 17 Abs. 3 eine Anfrage auf Verbreiten von Daten eines hochwertigen Erdfernerkundungssystems nicht, nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise auf dessen Sensitivität prüft,
7. entgegen § 5 Abs. 1 oder § 18 Abs. 1 Satz 1 und 2 eine Aufzeichnung nicht, nicht richtig oder nicht vollständig fertigt oder diese Aufzeichnungen nach § 5 Abs. 2 oder § 18 Abs. 2 nicht oder nicht mindestens fünf Jahre aufbewahrt oder
8. entgegen § 18 Abs. 3 Satz 1 keine dort genannten Protokolle und Dokumentationen bereithält.

(2) Ordnungswidrig handelt, wer

1. entgegen § 6 Abs. 1 oder § 13 eine Anzeige nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erstattet oder
2. entgegen § 7 Abs. 1 oder § 14 Abs. 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt.

(3) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nr. 1 bis 5 mit einer Geldbuße bis zu fünfhunderttausend Euro, in den Fällen des Absatzes 1 Nr. 6 bis 8 mit einer Geldbuße

bis zu fünfzigtausend Euro und in den Fällen des Absatzes 2 mit einer Geldbuße von bis zu fünfundzwanzigtausend Euro geahndet werden.

§ 29 Straftaten

(1) Mit Freiheitsstrafe bis fünf Jahren oder mit Geldstrafe wird bestraft, wer eine in § 28 Absatz 1 Nummer 1, 3 bis 5 oder 6 bezeichnete vorsätzliche Handlung begeht, die geeignet ist,

1. die wesentlichen Sicherheitsinteressen der Bundesrepublik Deutschland,
2. das friedliche Zusammenleben der Völker oder
3. die auswärtigen Beziehungen der Bundesrepublik Deutschland erheblich

zu gefährden.

(2) Der Versuch ist strafbar.

§ 30 Auslandstaten Deutscher

§ 29 gilt, unabhängig vom Recht des Tatorts, auch im Ausland, wenn der Täter zur Zeit der Tat Deutscher ist.

§ 31 Straf- und Bußgeldverfahren

(1) Soweit für Straftaten nach § 29 das Amtsgericht sachlich zuständig ist, ist örtlich zuständig das Amtsgericht, in dessen Bezirk das Landgericht seinen Sitz hat.

(2) Im Strafverfahren gelten § 49 Abs. 2, § 63 Abs. 2 und 3 Satz 1 sowie § 76 Abs. 1 und 4 des Gesetzes über Ordnungswidrigkeiten über die Beteiligung der Verwaltungsbehörden im Verfahren der Staatsanwaltschaft und im gerichtlichen Verfahren entsprechend.

Teil 7
Übergangs- und Schlussbestimmungen

§ 32 -

§ 33 -

§ 34 Übergangsregelung

(1) Der bei Inkrafttreten dieses Gesetzes bestehende Betrieb eines hochwertigen Erdfernerkundungssystems gilt bis zum Eintritt der Unanfechtbarkeit der Entscheidung über den Genehmigungsantrag als genehmigt, wenn dieser Antrag innerhalb von drei Monaten ab Inkrafttreten dieses Gesetzes gestellt wird.

(2) Absatz 1 gilt entsprechend für die Zulassung als Datenanbieter. Die Pflichten des Datenanbieters nach § 17 Abs. 1 und § 19 Abs. 1 gelten bis zum Inkrafttreten der Rechtsverordnung nach § 17 Abs. 3 als erfüllt.

§ 35 Inkrafttreten

(1) § 2 Abs. 2, § 17 Abs. 3 und § 26 Satz 2 bis 4 treten am Tag nach der Verkündung in Kraft.

(2) Im Übrigen tritt dieses Gesetz am 1. Dezember 2007 in Kraft.

Gesetz für einen besseren Schutz hinweisgebender Personen (Hinweisgeberschutzgesetz - HinSchG)

Inhaltsübersicht

Abschnitt 1
Allgemeine Vorschriften

§ 1 Zielsetzung und persönlicher Anwendungsbereich

§ 2 Sachlicher Anwendungsbereich

§ 3 Begriffsbestimmungen

§ 4 Verhältnis zu sonstigen Bestimmungen

§ 5 Vorrang von Sicherheitsinteressen sowie Verschwiegenheits- und Geheimhaltungspflichten

§ 6 Verhältnis zu sonstigen Verschwiegenheits- und Geheimhaltungspflichten

Abschnitt 2
Meldungen

Unterabschnitt 1
Grundsätze

§ 7 Wahlrecht zwischen interner und externer Meldung

§ 8 Vertraulichkeitsgebot

§ 9 Ausnahmen vom Vertraulichkeitsgebot

§ 10 Verarbeitung personenbezogener Daten

§ 11 Dokumentation der Meldungen

Unterabschnitt 2
Interne Meldungen

§ 12 Pflicht zur Einrichtung interner Meldestellen

§ 13 Aufgaben der internen Meldestellen

§ 14 Organisationsformen interner Meldestellen

§ 15 Unabhängige Tätigkeit; notwendige Fachkunde

§ 16 Meldekanäle für interne Meldestellen

§ 17 Verfahren bei internen Meldungen

§ 18 Folgemaßnahmen der internen Meldestelle

Unterabschnitt 3
Externe Meldestellen

§ 19 Errichtung und Zuständigkeit einer externen Meldestelle des Bundes

§ 20 Errichtung und Zuständigkeit externer Meldestellen der Länder

§ 21 Bundesanstalt für Finanzdienstleistungsaufsicht als externe Meldestelle

§ 22 Bundeskartellamt als externe Meldestelle

§ 23 Weitere externe Meldestellen

§ 24 Aufgaben der externen Meldestellen

§ 25 Unabhängige Tätigkeit; Schulung

§ 26 Berichtspflichten der externen Meldestellen

Unterabschnitt 4
Externe Meldungen

§ 27 Meldekanäle für externe Meldestellen

§ 28 Verfahren bei externen Meldungen

§ 29 Folgemaßnahmen der externen Meldestellen

§ 30 Zusammenarbeit mit anderen öffentlichen Stellen

§ 31 Abschluss des Verfahrens

Abschnitt 3
Offenlegung

§ 32 Offenlegen von Informationen

Abschnitt 4
Schutzmaßnahmen

§ 33 Voraussetzungen für den Schutz hinweisgebender Personen

§ 34 Weitere geschützte Personen

§ 35 Ausschluss der Verantwortlichkeit

§ 36 Verbot von Repressalien; Beweislastumkehr

§ 37 Schadensersatz nach Repressalien

§ 38 Schadensersatz nach einer Falschmeldung

§ 39 Verbot abweichender Vereinbarungen

Abschnitt 5
Sanktionen

§ 40 Bußgeldvorschriften

Abschnitt 6
Schlussvorschriften

§ 41 Verordnungsermächtigung

§ 42 Übergangsregelung

Abschnitt 1
Allgemeine Vorschriften

§ 1 Zielsetzung und persönlicher Anwendungsbereich

(1) Dieses Gesetz regelt den Schutz von natürlichen Personen, die im Zusammenhang mit ihrer beruflichen Tätigkeit oder im Vorfeld einer beruflichen Tätigkeit Informationen über Verstöße erlangt haben und diese an die nach diesem Gesetz vorgesehenen Meldestellen melden oder offenlegen (hinweisgebende Personen).

(2) Darüber hinaus werden Personen geschützt, die Gegenstand einer Meldung oder Offenlegung sind, sowie sonstige Personen, die von einer Meldung oder Offenlegung betroffen sind.

§ 2 Sachlicher Anwendungsbereich

(1) Dieses Gesetz gilt für die Meldung (§ 3 Absatz 4) und die Offenlegung (§ 3 Absatz 5) von Informationen über

1. Verstöße, die strafbewehrt sind,
2. Verstöße, die bußgeldbewehrt sind, soweit die verletzte Vorschrift dem Schutz von Leben, Leib oder Gesundheit oder dem Schutz der Rechte von Beschäftigten oder ihrer Vertretungsorgane dient,
3. sonstige Verstöße gegen Rechtsvorschriften des Bundes und der Länder sowie unmittelbar geltende Rechtsakte der Europäischen Union und der Europäischen Atomgemeinschaft
   a) zur Bekämpfung von Geldwäsche und Terrorismusfinanzierung, unter Einschluss insbesondere des Geldwäschegesetzes und der Verordnung (EU) 2015/847 des Europäischen Parlaments und des Rates vom 20. Mai 2015 über die Übermittlung von Angaben bei Geldtransfers und zur Aufhebung der Verordnung (EU) Nr. 1781/2006 (ABl. L 141 vom 5.6.2015, S. 1), die durch die Verordnung (EU) 2019/2175 (ABl. L 334 vom 27.12.2019, S. 1) geändert worden ist, in der jeweils geltenden Fassung,
   b) mit Vorgaben zur Produktsicherheit und -konformität,
   c) mit Vorgaben zur Sicherheit im Straßenverkehr, die das Straßeninfrastruktursicherheitsmanagement, die Sicherheitsanforderungen in Straßentunneln sowie die Zulassung zum Beruf des Güterkraftverkehrsunternehmers oder des Personenkraftverkehrsunternehmers (Kraftomnibusunternehmen) betreffen,
   d) mit Vorgaben zur Gewährleistung der Eisenbahnbetriebssicherheit,

e) mit Vorgaben zur Sicherheit im Seeverkehr betreffend Vorschriften der Europäischen Union für die Anerkennung von Schiffsüberprüfungs- und -besichtigungsorganisationen, die Haftung und Versicherung des Beförderers bei der Beförderung von Reisenden auf See, die Zulassung von Schiffsausrüstung, die Seesicherheitsuntersuchung, die Seeleute-Ausbildung, die Registrierung von Personen auf Fahrgastschiffen in der Seeschifffahrt sowie Vorschriften und Verfahrensregeln der Europäischen Union für das sichere Be- und Entladen von Massengutschiffen,

f) mit Vorgaben zur zivilen Luftverkehrssicherheit im Sinne der Abwehr von Gefahren für die betriebliche und technische Sicherheit und im Sinne der Flugsicherung,

g) mit Vorgaben zur sicheren Beförderung gefährlicher Güter auf der Straße, per Eisenbahn und per Binnenschiff,

h) mit Vorgaben zum Umweltschutz,

i) mit Vorgaben zum Strahlenschutz und zur kerntechnischen Sicherheit,

j) zur Förderung der Nutzung von Energie aus erneuerbaren Quellen und der Energieeffizienz,

k) zur Lebensmittel- und Futtermittelsicherheit, zur ökologischen Produktion und zur Kennzeichnung von ökologischen Erzeugnissen, zum Schutz geografischer Angaben für Agrarerzeugnisse und Lebensmittel einschließlich Wein, aromatisierter Weinerzeugnisse und Spirituosen sowie garantiert traditioneller Spezialitäten, zum Inverkehrbringen und Verwenden von Pflanzenschutzmitteln sowie zur Tiergesundheit und zum Tierschutz, soweit sie den Schutz von landwirtschaftlichen Nutztieren, den Schutz von Tieren zum Zeitpunkt der Tötung, die Haltung von Wildtieren in Zoos, den Schutz der für wissenschaftliche Zwecke verwendeten Tiere sowie den Transport von Tieren und die damit zusammenhängenden Vorgänge betreffen,

l) zu Qualitäts- und Sicherheitsstandards für Organe und Substanzen menschlichen Ursprungs, Human- und Tierarzneimittel, Medizinprodukte sowie die grenzüberschreitende Patientenversorgung,

m) zur Herstellung, zur Aufmachung und zum Verkauf von Tabakerzeugnissen und verwandten Erzeugnissen,

n) zur Regelung der Verbraucherrechte und des Verbraucherschutzes im Zusammenhang mit Verträgen zwischen Unternehmern und Verbrauchern sowie zum Schutz von Verbrauchern im Bereich der Zahlungskonten und Finanzdienstleistungen, bei Preisangaben sowie vor unlauteren geschäftlichen Handlungen,

o) zum Schutz der Privatsphäre in der elektronischen Kommunikation, zum Schutz der Vertraulichkeit der Kommunikation, zum Schutz personenbezogener Daten im Bereich der elektronischen Kommunikation, zum Schutz der Privatsphäre der Endeinrichtungen von Nutzern und von in diesen Endeinrichtungen gespeicherten Informationen, zum Schutz vor unzumutbaren Belästigungen durch Werbung mittels Telefonanrufen, automatischen Anruf-

maschinen, Faxgeräten oder elektronischer Post sowie über die Rufnummernanzeige und -unterdrückung und zur Aufnahme in Teilnehmerverzeichnisse,

p) zum Schutz personenbezogener Daten im Anwendungsbereich der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2; L 74 vom 4.3.2021, S. 35) gemäß deren Artikel 2,

q) zur Sicherheit in der Informationstechnik im Sinne des § 2 Absatz 2 des BSI-Gesetzes von Anbietern digitaler Dienste im Sinne des § 2 Absatz 12 des BSI-Gesetzes,

r) zur Regelung der Rechte von Aktionären von Aktiengesellschaften,

s) zur Abschlussprüfung bei Unternehmen von öffentlichem Interesse nach § 316a Satz 2 des Handelsgesetzbuchs,

t) zur Rechnungslegung einschließlich der Buchführung von Unternehmen, die kapitalmarktorientiert im Sinne des § 264d des Handelsgesetzbuchs sind, von Kreditinstituten im Sinne des § 340 Absatz 1 des Handelsgesetzbuchs, Finanzdienstleistungsinstituten im Sinne des § 340 Absatz 4 Satz 1 des Handelsgesetzbuchs, Wertpapierinstituten im Sinne des § 340 Absatz 4a Satz 1 des Handelsgesetzbuchs, Instituten im Sinne des § 340 Absatz 5 Satz 1 des Handelsgesetzbuchs, Versicherungsunternehmen im Sinne des § 341 Absatz 1 des Handelsgesetzbuchs und Pensionsfonds im Sinne des § 341 Absatz 4 Satz 1 des Handelsgesetzbuchs,

4. Verstöße gegen bundesrechtlich und einheitlich geltende Regelungen für Auftraggeber zum Verfahren der Vergabe von öffentlichen Aufträgen und Konzessionen und zum Rechtsschutz in diesen Verfahren ab Erreichen der jeweils maßgeblichen EU-Schwellenwerte,

5. Verstöße, die von § 4d Absatz 1 Satz 1 des Finanzdienstleistungsaufsichtsgesetzes erfasst sind, soweit sich nicht aus § 4 Absatz 1 Satz 1 etwas anderes ergibt,

6. Verstöße gegen für Körperschaften und Personenhandelsgesellschaften geltende steuerliche Rechtsnormen,

7. Verstöße in Form von Vereinbarungen, die darauf abzielen, sich in missbräuchlicher Weise einen steuerlichen Vorteil zu verschaffen, der dem Ziel oder dem Zweck des für Körperschaften und Personenhandelsgesellschaften geltenden Steuerrechts zuwiderläuft,

8. Verstöße gegen die Artikel 101 und 102 des Vertrags über die Arbeitsweise der Europäischen Union sowie Verstöße gegen die in § 81 Absatz 2 Nummer 1, 2 Buchstabe a und Nummer 5 sowie Absatz 3 des Gesetzes gegen Wettbewerbsbeschränkungen genannten Rechtsvorschriften,

9. Verstöße gegen Vorschriften der Verordnung (EU) 2022/1925 des Europäischen Parlaments und des Rates vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte) (ABl. L 265 vom 12.10.2022, S. 1),

10. Äußerungen von Beamtinnen und Beamten, die einen Verstoß gegen die Pflicht zur Verfassungstreue darstellen.

(2) Dieses Gesetz gilt außerdem für die Meldung und Offenlegung von Informationen über

1. Verstöße gegen den Schutz der finanziellen Interessen der Europäischen Union im Sinne des Artikels 325 des Vertrags über die Arbeitsweise der Europäischen Union und
2. Verstöße gegen Binnenmarktvorschriften im Sinne des Artikels 26 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union, einschließlich über Absatz 1 Nummer 8 hinausgehender Vorschriften der Europäischen Union über Wettbewerb und staatliche Beihilfen.

§ 3 Begriffsbestimmungen

(1) Für dieses Gesetz gelten die Begriffsbestimmungen der folgenden Absätze.

(2) Verstöße sind Handlungen oder Unterlassungen im Rahmen einer beruflichen, unternehmerischen oder dienstlichen Tätigkeit, die rechtswidrig sind und Vorschriften oder Rechtsgebiete betreffen, die in den sachlichen Anwendungsbereich nach § 2 fallen. Hierzu können auch missbräuchliche Handlungen oder Unterlassungen gehören, die dem Ziel oder dem Zweck der Regelungen in den Vorschriften oder Rechtsgebieten zuwiderlaufen, die in den sachlichen Anwendungsbereich nach § 2 fallen.

(3) Informationen über Verstöße sind begründete Verdachtsmomente oder Wissen über tatsächliche oder mögliche Verstöße, die bei dem Beschäftigungsgeber, bei dem die hinweisgebende Person tätig ist oder war, oder bei einer anderen Stelle, mit der die hinweisgebende Person aufgrund ihrer beruflichen Tätigkeit im Kontakt steht oder stand, bereits begangen wurden oder sehr wahrscheinlich erfolgen werden, sowie über Versuche der Verschleierung solcher Verstöße.

(4) Meldungen sind Mitteilungen von Informationen über Verstöße an interne Meldestellen (§ 12) oder externe Meldestellen (§§ 19 bis 24).

(5) Offenlegung bezeichnet das Zugänglichmachen von Informationen über Verstöße gegenüber der Öffentlichkeit.

(6) Repressalien sind Handlungen oder Unterlassungen im Zusammenhang mit der beruflichen Tätigkeit, die eine Reaktion auf eine Meldung oder eine Offenlegung sind und durch die der hinweisgebenden Person ein ungerechtfertigter Nachteil entsteht oder entstehen kann.

(7) Folgemaßnahmen sind die von einer internen Meldestelle nach § 18 oder von einer externen Meldestelle nach § 29 ergriffenen Maßnahmen zur Prüfung der Stichhaltigkeit einer Meldung, zum weiteren Vorgehen gegen den gemeldeten Verstoß oder zum Abschluss des Verfahrens.

(8) Beschäftigte sind

1. Arbeitnehmerinnen und Arbeitnehmer,
2. die zu ihrer Berufsbildung Beschäftigten,
3. Beamtinnen und Beamte,

4. Richterinnen und Richter mit Ausnahme der ehrenamtlichen Richterinnen und Richter,
5. Soldatinnen und Soldaten,
6. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,
7. Menschen mit Behinderung, die in einer Werkstatt für behinderte Menschen oder bei einem anderen Leistungsanbieter nach § 60 des Neunten Buches Sozialgesetzbuch beschäftigt sind.

(9) Beschäftigungsgeber sind, sofern mindestens eine Person bei ihnen beschäftigt ist,

1. natürliche Personen sowie juristische Personen des öffentlichen und des privaten Rechts,
2. rechtsfähige Personengesellschaften und
3. sonstige, nicht in den Nummern 1 und 2 genannte rechtsfähige Personenvereinigungen.

(10) Private Beschäftigungsgeber sind Beschäftigungsgeber mit Ausnahme juristischer Personen des öffentlichen Rechts und solcher Beschäftigungsgeber, die im Eigentum oder unter der Kontrolle einer juristischen Person des öffentlichen Rechts stehen.

§ 4 Verhältnis zu sonstigen Bestimmungen

(1) Diesem Gesetz gehen spezifische Regelungen über die Mitteilung von Informationen über Verstöße in den folgenden Vorschriften vor:

1. § 6 Absatz 5 und § 53 des Geldwäschegesetzes,
2. § 25a Absatz 1 Satz 6 Nummer 3 des Kreditwesengesetzes und § 13 Absatz 1 des Wertpapierinstitutsgesetzes,
3. § 58 des Wertpapierhandelsgesetzes,
4. § 23 Absatz 6 des Versicherungsaufsichtsgesetzes,
5. § 28 Absatz 1 Satz 2 Nummer 9 und § 68 Absatz 4 Satz 3 des Kapitalanlagegesetzbuchs,
6. §§ 3b und 5 Absatz 8 des Börsengesetzes,
7. § 55b Absatz 2 Nummer 7 der Wirtschaftsprüferordnung,
8. Artikel 32 der Verordnung (EU) Nr. 596/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über Marktmissbrauch (Marktmissbrauchsverordnung) und zur Aufhebung der Richtlinie 2003/6/EG des Europäischen Parlaments und des Rates und der Richtlinien 2003/124/EG, 2003/125/EG und 2004/72/EG der Kommission (ABl. L 173 vom 12.6.2014, S. 1; L 287 vom 21.10.2016, S. 320; L 348 vom 21.12.2016, S. 83), die zuletzt durch die Delegierte Verordnung (EU) 2021/1783 (ABl. L 359 vom 11.10.2021, S. 1) geändert worden ist, in der jeweils geltenden Fassung,

9. Artikel 4 und 5 der Verordnung (EU) Nr. 376/2014 des Europäischen Parlaments und des Rates vom 3. April 2014 über die Meldung, Analyse und Weiterverfolgung von Ereignissen in der Zivilluftfahrt, zur Änderung der Verordnung (EU) Nr. 996/2010 des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 2003/42/EG des Europäischen Parlaments und des Rates und der Verordnungen (EG) Nr. 1321/2007 und (EG) Nr. 1330/2007 der Kommission (ABl. L 122 vom 24.4.2014, S. 18), die zuletzt durch die Delegierte Verordnung (EU) 2020/2034 (ABl. L 416 vom 11.12.2020, S. 1) geändert worden ist, in der jeweils geltenden Fassung, und der aufgrund des § 32 Absatz 1 Nummer 1 des Luftverkehrsgesetzes erlassenen Rechtsverordnungen,

10. §§ 127 und 128 des Seearbeitsgesetzes,

11. § 14 Absatz 1 des Schiffssicherheitsgesetzes in Verbindung mit Abschnitt D Nummer 8 der Anlage zum Schiffssicherheitsgesetz und den aufgrund der §§ 9, 9a und 9c des Seeaufgabengesetzes erlassenen Rechtsverordnungen für Beschwerden, die die Sicherheit eines Schiffes unter ausländischer Flagge einschließlich der Sicherheit und Gesundheit seiner Besatzung, der Lebens- und Arbeitsbedingungen an Bord und der Verhütung von Verschmutzung durch Schiffe unter ausländischer Flagge betreffen, und

12. aufgrund des § 57c Satz 1 Nummer 1 und des § 68 Absatz 2 in Verbindung mit Absatz 3 und mit den §§ 65, 66 und 67 Nummer 1 und 8 und den §§ 126, 128 und 129 des Bundesberggesetzes erlassenen Rechtsverordnungen.

Soweit die spezifischen Regelungen in Satz 1 keine Vorgaben machen, gelten die Bestimmungen dieses Gesetzes.

(2) Das Verbraucherinformationsgesetz, das Informationsfreiheitsgesetz sowie Regelungen der Länder über den Zugang zu amtlichen Informationen finden keine Anwendung auf die Vorgänge nach diesem Gesetz. Satz 1 gilt nicht für die Regelungen des Bundes und der Länder über den Zugang zu Umweltinformationen.

(3) Die §§ 81h bis 81n des Gesetzes gegen Wettbewerbsbeschränkungen bleiben unberührt.

(4) Die Regelungen des Strafprozessrechts werden von den Vorgaben dieses Gesetzes nicht berührt.

§ 5 Vorrang von Sicherheitsinteressen sowie Verschwiegenheits- und Geheimhaltungspflichten

(1) Eine Meldung oder Offenlegung fällt nicht in den Anwendungsbereich dieses Gesetzes, wenn sie folgende Informationen beinhaltet:

1. Informationen, die die nationale Sicherheit oder wesentliche Sicherheitsinteressen des Staates, insbesondere militärische oder sonstige sicherheitsempfindliche Belange des Geschäftsbereiches des Bundesministeriums der Verteidigung oder Kritische Infrastrukturen im Sinne der BSI-Kritisverordnung, betreffen,

2. Informationen von Nachrichtendiensten des Bundes oder der Länder oder von Behörden oder sonstigen öffentlichen Stellen des Bundes oder der Länder, soweit sie Aufgaben im Sinne des § 10 Nummer 3 des Sicherheitsüberprüfungsgesetzes oder im Sinne entsprechender Rechtsvorschriften der Länder wahrnehmen, oder

3. Informationen, die die Vergabe öffentlicher Aufträge und Konzessionen, die in den Anwendungsbereich des Artikels 346 des Vertrags über die Arbeitsweise der Europäischen Union fallen, betreffen.

(2) Eine Meldung oder Offenlegung fällt auch nicht in den Anwendungsbereich dieses Gesetzes, wenn ihr entgegenstehen:

1. eine Geheimhaltungs- oder Vertraulichkeitspflicht zum materiellen oder organisatorischen Schutz von Verschlusssachen, es sei denn, es handelt sich um die Meldung eines Verstoßes nach § 2 Absatz 1 Nummer 1 an eine interne Meldestelle (§ 12), mit den Aufgaben der internen Meldestelle wurde kein Dritter nach § 14 Absatz 1 betraut und die betreffende Geheimhaltungs- oder Vertraulichkeitspflicht bezieht sich auf eine Verschlusssache des Bundes nach § 4 Absatz 2 Nummer 4 des Sicherheitsüberprüfungsgesetzes oder auf eine entsprechende Verschlusssache nach den Rechtsvorschriften der Länder,
2. das richterliche Beratungsgeheimnis,
3. die Pflichten zur Wahrung der Verschwiegenheit durch Rechtsanwälte, Verteidiger in einem gesetzlich geordneten Verfahren, Kammerrechtsbeistände, Patentanwälte und Notare,
4. die Pflichten zur Wahrung der Verschwiegenheit durch Ärzte, Zahnärzte, Apotheker und Angehörige eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert, mit Ausnahme von Tierärzten, soweit es um Verstöße gegen von § 2 Absatz 1 Nummer 3 Buchstabe k erfasste Rechtsvorschriften zum Schutz von gewerblich gehaltenen landwirtschaftlichen Nutztieren geht, oder
5. die Pflichten zur Wahrung der Verschwiegenheit durch Personen, die aufgrund eines Vertragsverhältnisses einschließlich der gemeinschaftlichen Berufsausübung, einer berufsvorbereitenden Tätigkeit oder einer sonstigen Hilfstätigkeit an der beruflichen Tätigkeit der in den Nummern 2, 3 und 4 genannten Berufsgeheimnisträger mitwirken.

§ 6 Verhältnis zu sonstigen Verschwiegenheits- und Geheimhaltungspflichten

(1) Beinhaltet eine interne oder eine externe Meldung oder eine Offenlegung ein Geschäftsgeheimnis im Sinne des § 2 Nummer 1 des Gesetzes zum Schutz von Geschäftsgeheimnissen, so ist die Weitergabe des Geschäftsgeheimnisses an eine zuständige Meldestelle oder dessen Offenlegung erlaubt, sofern

1. die hinweisgebende Person hinreichenden Grund zu der Annahme hatte, dass die Weitergabe oder die Offenlegung des Inhalts dieser Informationen notwendig ist, um einen Verstoß aufzudecken, und
2. die Voraussetzungen des § 33 Absatz 1 Nummer 2 und 3 erfüllt sind.

(2) Vorbehaltlich der Vorgaben des § 5 dürfen Informationen, die einer vertraglichen Verschwiegenheitspflicht, einer Rechtsvorschrift des Bundes, eines Landes oder einem unmittelbar geltenden Rechtsakt der Europäischen Union über die Geheimhaltung oder über Verschwiegenheitspflichten, dem Steuergeheimnis nach § 30 der Abgabenordnung oder dem Sozialgeheimnis nach § 35 des Ersten Buches Sozialgesetzbuch unterliegen, an eine zuständi-

ge Meldestelle weitergegeben oder unter den Voraussetzungen des § 32 offengelegt werden, sofern

1. die hinweisgebende Person hinreichenden Grund zu der Annahme hatte, dass die Weitergabe oder die Offenlegung des Inhalts dieser Informationen notwendig ist, um einen Verstoß aufzudecken, und
2. die Voraussetzungen des § 33 Absatz 1 Nummer 2 und 3 erfüllt sind.

(3) Personen, die im Rahmen ihrer Tätigkeit für eine Meldestelle Informationen erlangen, die einer vertraglichen Verschwiegenheitspflicht, einer Rechtsvorschrift des Bundes über die Geheimhaltung oder über Verschwiegenheitspflichten, dem Steuergeheimnis nach § 30 der Abgabenordnung oder dem Sozialgeheimnis nach § 35 des Ersten Buches Sozialgesetzbuch unterliegen, haben ab dem Zeitpunkt des Eingangs der Informationen

1. diese Verschwiegenheits- oder Geheimhaltungsvorschriften vorbehaltlich des Absatzes 4 anzuwenden und
2. die schutzwürdigen Belange Betroffener in gleicher Weise zu beachten wie sie die hinweisgebende Person zu beachten hat, die die Informationen der Meldestelle mitgeteilt hat.

(4) Meldestellen dürfen Geheimnisse im Sinne der Absätze 1 und 2 nur insoweit verwenden oder weitergeben, wie dies für das Ergreifen von Folgemaßnahmen erforderlich ist.

(5) In Bezug auf Informationen, die einer vertraglichen Verschwiegenheitspflicht unterliegen, gelten die Absätze 3 und 4 ab dem Zeitpunkt, zu dem Kenntnis von der Verschwiegenheitspflicht besteht.

Abschnitt 2
Meldungen

Unterabschnitt 1
Grundsätze

§ 7 Wahlrecht zwischen interner und externer Meldung

(1) Personen, die beabsichtigen, Informationen über einen Verstoß zu melden, können wählen, ob sie sich an eine interne Meldestelle (§ 12) oder eine externe Meldestelle (§§ 19 bis 24) wenden. Diese Personen sollten in den Fällen, in denen intern wirksam gegen den Verstoß vorgegangen werden kann und sie keine Repressalien befürchten, die Meldung an eine interne Meldestelle bevorzugen. Wenn einem intern gemeldeten Verstoß nicht abgeholfen wurde, bleibt es der hinweisgebenden Person unbenommen, sich an eine externe Meldestelle zu wenden.

(2) Es ist verboten, Meldungen oder die auf eine Meldung folgende Kommunikation zwischen hinweisgebender Person und Meldestelle zu behindern oder dies zu versuchen.

(3) Beschäftigungsgeber, die nach § 12 Absatz 1 und 3 zur Einrichtung interner Meldestellen verpflichtet sind, sollen Anreize dafür schaffen, dass sich hinweisgebende Personen vor einer Meldung an eine externe Meldestelle zunächst an die jeweilige interne Meldestelle wenden. Diese Beschäftigungsgeber stellen für Beschäftigte klare und leicht zugängliche Informatio-

nen über die Nutzung des internen Meldeverfahrens bereit. Die Möglichkeit einer externen Meldung darf hierdurch nicht beschränkt oder erschwert werden.

§ 8 Vertraulichkeitsgebot

(1) Die Meldestellen haben die Vertraulichkeit der Identität der folgenden Personen zu wahren:

1. der hinweisgebenden Person, sofern die gemeldeten Informationen Verstöße betreffen, die in den Anwendungsbereich dieses Gesetzes fallen, oder die hinweisgebende Person zum Zeitpunkt der Meldung hinreichenden Grund zu der Annahme hatte, dass dies der Fall sei,
2. der Personen, die Gegenstand einer Meldung sind, und
3. der sonstigen in der Meldung genannten Personen.

Die Identität der in Satz 1 genannten Personen darf ausschließlich den Personen, die für die Entgegennahme von Meldungen oder für das Ergreifen von Folgemaßnahmen zuständig sind, sowie den sie bei der Erfüllung dieser Aufgaben unterstützenden Personen bekannt werden.

(2) Das Gebot der Vertraulichkeit der Identität gilt unabhängig davon, ob die Meldestelle für die eingehende Meldung zuständig ist.

§ 9 Ausnahmen vom Vertraulichkeitsgebot

(1) Die Identität einer hinweisgebenden Person, die vorsätzlich oder grob fahrlässig unrichtige Informationen über Verstöße meldet, wird nicht nach diesem Gesetz geschützt.

(2) Informationen über die Identität einer hinweisgebenden Person oder über sonstige Umstände, die Rückschlüsse auf die Identität dieser Person erlauben, dürfen abweichend von § 8 Absatz 1 an die zuständige Stelle weitergegeben werden

1. in Strafverfahren auf Verlangen der Strafverfolgungsbehörden,
2. aufgrund einer Anordnung in einem einer Meldung nachfolgenden Verwaltungsverfahren, einschließlich verwaltungsbehördlicher Bußgeldverfahren,
3. aufgrund einer gerichtlichen Entscheidung,
4. von der Bundesanstalt für Finanzdienstleistungsaufsicht als externe Meldestelle nach § 21 an die zuständigen Fachabteilungen innerhalb der Bundesanstalt für Finanzdienstleistungsaufsicht sowie bei in § 109a des Wertpapierhandelsgesetzes genannten Vorgängen an die in § 109a des Wertpapierhandelsgesetzes genannten Stellen oder
5. von dem Bundeskartellamt als externe Meldestelle nach § 22 an die zuständigen Fachabteilungen innerhalb des Bundeskartellamtes sowie in den Fällen des § 49 Absatz 2 Satz 2 und Absatz 4 und § 50d des Gesetzes gegen Wettbewerbsbeschränkungen an die jeweils zuständige Wettbewerbsbehörde.

Die Meldestelle hat die hinweisgebende Person vorab über die Weitergabe zu informieren. Hiervon ist abzusehen, wenn die Strafverfolgungsbehörde, die zuständige Behörde oder das Gericht der Meldestelle mitgeteilt hat, dass durch die Information die entsprechenden Ermittlungen, Untersuchungen oder Gerichtsverfahren gefährdet würden. Der hinweisgeben-

den Person sind mit der Information zugleich die Gründe für die Weitergabe schriftlich oder elektronisch darzulegen.

(3) Über die Fälle des Absatzes 2 hinaus dürfen Informationen über die Identität der hinweisgebenden Person oder über sonstige Umstände, die Rückschlüsse auf die Identität dieser Person erlauben, weitergegeben werden, wenn

1. die Weitergabe für Folgemaßnahmen erforderlich ist und
2. die hinweisgebende Person zuvor in die Weitergabe eingewilligt hat.

Die Einwilligung nach Satz 1 Nummer 2 muss für jede einzelne Weitergabe von Informationen über die Identität gesondert und in Textform vorliegen. Die Regelung des § 26 Absatz 2 des Bundesdatenschutzgesetzes bleibt unberührt.

(4) Informationen über die Identität von Personen, die Gegenstand einer Meldung sind, und von sonstigen in der Meldung genannten Personen dürfen abweichend von § 8 Absatz 1 an die jeweils zuständige Stelle weitergegeben werden

1. bei Vorliegen einer diesbezüglichen Einwilligung,
2. von internen Meldestellen, sofern dies im Rahmen interner Untersuchungen bei dem jeweiligen Beschäftigungsgeber oder in der jeweiligen Organisationseinheit erforderlich ist,
3. sofern dies für das Ergreifen von Folgemaßnahmen erforderlich ist,
4. in Strafverfahren auf Verlangen der Strafverfolgungsbehörde,
5. aufgrund einer Anordnung in einem einer Meldung nachfolgenden Verwaltungsverfahren, einschließlich verwaltungsbehördlicher Bußgeldverfahren,
6. aufgrund einer gerichtlichen Entscheidung,
7. von der Bundesanstalt für Finanzdienstleistungsaufsicht als externe Meldestelle nach § 21 an die zuständigen Fachabteilungen innerhalb der Bundesanstalt für Finanzdienstleistungsaufsicht sowie bei in § 109a des Wertpapierhandelsgesetzes genannten Vorgängen an die in § 109a des Wertpapierhandelsgesetzes genannten Stellen oder
8. von dem Bundeskartellamt als externe Meldestelle nach § 22 an die zuständigen Fachabteilungen innerhalb des Bundeskartellamtes sowie in den Fällen des § 49 Absatz 2 Satz 2 und Absatz 4 und § 50d des Gesetzes gegen Wettbewerbsbeschränkungen an die jeweils zuständige Wettbewerbsbehörde.

§ 10 Verarbeitung personenbezogener Daten

Die Meldestellen sind befugt, personenbezogene Daten zu verarbeiten, soweit dies zur Erfüllung ihrer in den §§ 13 und 24 bezeichneten Aufgaben erforderlich ist. Abweichend von Artikel 9 Absatz 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten durch eine Meldestelle zulässig, wenn dies zur Erfüllung ihrer Aufgaben erforderlich ist. In diesem Fall hat die Meldestelle spezifische und angemessene Maßnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen; § 22 Absatz 2 Satz 2 des Bundesdatenschutzgesetzes ist entsprechend anzuwenden.

§ 11 Dokumentation der Meldungen

(1) Die Personen, die in einer Meldestelle für die Entgegennahme von Meldungen zuständig sind, dokumentieren alle eingehenden Meldungen in dauerhaft abrufbarer Weise unter Beachtung des Vertraulichkeitsgebots (§ 8).

(2) Bei telefonischen Meldungen oder Meldungen mittels einer anderen Art der Sprachübermittlung darf eine dauerhaft abrufbare Tonaufzeichnung des Gesprächs oder dessen vollständige und genaue Niederschrift (Wortprotokoll) nur mit Einwilligung der hinweisgebenden Person erfolgen. Liegt eine solche Einwilligung nicht vor, ist die Meldung durch eine von der für die Bearbeitung der Meldung verantwortlichen Person zu erstellende Zusammenfassung ihres Inhalts (Inhaltsprotokoll) zu dokumentieren.

(3) Erfolgt die Meldung im Rahmen einer Zusammenkunft gemäß § 16 Absatz 3 oder § 27 Absatz 3, darf mit Zustimmung der hinweisgebenden Person eine vollständige und genaue Aufzeichnung der Zusammenkunft erstellt und aufbewahrt werden. Die Aufzeichnung kann durch Erstellung einer Tonaufzeichnung des Gesprächs in dauerhaft abrufbarer Form oder durch ein von der für die Bearbeitung der Meldung verantwortlichen Person erstelltes Wortprotokoll der Zusammenkunft erfolgen.

(4) Der hinweisgebenden Person ist Gelegenheit zu geben, das Protokoll zu überprüfen, gegebenenfalls zu korrigieren und es durch ihre Unterschrift oder in elektronischer Form zu bestätigen. Wird eine Tonaufzeichnung zur Anfertigung eines Protokolls verwendet, so ist sie zu löschen, sobald das Protokoll fertiggestellt ist.

(5) Die Dokumentation wird drei Jahre nach Abschluss des Verfahrens gelöscht. Die Dokumentation kann länger aufbewahrt werden, um die Anforderungen nach diesem Gesetz oder nach anderen Rechtsvorschriften zu erfüllen, solange dies erforderlich und verhältnismäßig ist.

Unterabschnitt 2
Interne Meldungen

§ 12 Pflicht zur Einrichtung interner Meldestellen

(1) Beschäftigungsgeber haben dafür zu sorgen, dass bei ihnen mindestens eine Stelle für interne Meldungen eingerichtet ist und betrieben wird, an die sich Beschäftigte wenden können (interne Meldestelle). Ist der Bund oder ein Land Beschäftigungsgeber, bestimmen die obersten Bundes- oder Landesbehörden Organisationseinheiten in Form von einzelnen oder mehreren Behörden, Verwaltungsstellen, Betrieben oder Gerichten. Die Pflicht nach Satz 1 gilt sodann für die Einrichtung und den Betrieb der internen Meldestelle bei den jeweiligen Organisationseinheiten. Für Gemeinden und Gemeindeverbände und solche Beschäftigungsgeber, die im Eigentum oder unter der Kontrolle von Gemeinden und Gemeindeverbänden stehen, gilt die Pflicht zur Einrichtung und zum Betrieb interner Meldestellen nach Maßgabe des jeweiligen Landesrechts.

(2) Die Pflicht nach Absatz 1 Satz 1 gilt nur für Beschäftigungsgeber mit jeweils in der Regel mindestens 50 Beschäftigten.

(3) Abweichend von Absatz 2 gilt die Pflicht nach Absatz 1 Satz 1 unabhängig von der Zahl der Beschäftigten für

1. Wertpapierdienstleistungsunternehmen im Sinne des § 2 Absatz 10 des Wertpapierhandelsgesetzes,
2. Datenbereitstellungsdienste im Sinne des § 2 Absatz 40 des Wertpapierhandelsgesetzes,
3. Börsenträger im Sinne des Börsengesetzes,
4. Institute im Sinne des § 1 Absatz 1b des Kreditwesengesetzes und Institute im Sinne des § 2 Absatz 1 des Wertpapierinstitutsgesetzes,
5. Gegenparteien im Sinne des Artikels 3 Nummer 2 der Verordnung (EU) 2015/2365 des Europäischen Parlaments und des Rates vom 25. November 2015 über die Transparenz von Wertpapierfinanzierungsgeschäften und der Weiterverwendung sowie zur Änderung der Verordnung (EU) Nr. 648/2012 (ABl. L 337 vom 23.12.2015, S. 1), die zuletzt durch die Verordnung (EU) 2021/23 (ABl. L 22 vom 22.1.2021, S. 1) geändert worden ist, in der jeweils geltenden Fassung,
6. Kapitalverwaltungsgesellschaften gemäß § 17 Absatz 1 des Kapitalanlagegesetzbuchs,
7. Unternehmen gemäß § 1 Absatz 1 des Versicherungsaufsichtsgesetzes mit Ausnahme der nach den §§ 61 bis 66a des Versicherungsaufsichtsgesetzes tätigen Unternehmen mit Sitz in einem anderen Mitgliedstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum,
8. Institute im Sinne des § 2 Absatz 4 des Kryptomärkteaufsichtsgesetzes sowie
9. Institute im Sinne des § 1 Absatz 3 des Zahlungsdiensteaufsichtsgesetzes.

(4) Die nach Absatz 1 Satz 1 verpflichteten Beschäftigungsgeber erteilen der internen Meldestelle die notwendigen Befugnisse, um ihre Aufgaben wahrzunehmen, insbesondere, um Meldungen zu prüfen und Folgemaßnahmen zu ergreifen. Ist der Beschäftigungsgeber der Bund oder ein Land, gilt Satz 1 für die jeweiligen Organisationseinheiten entsprechend.

§ 13 Aufgaben der internen Meldestellen

(1) Die internen Meldestellen betreiben Meldekanäle nach § 16, führen das Verfahren nach § 17 und ergreifen Folgemaßnahmen nach § 18.

(2) Die internen Meldestellen halten für Beschäftigte klare und leicht zugängliche Informationen über externe Meldeverfahren gemäß Unterabschnitt 3 und einschlägige Meldeverfahren von Organen, Einrichtungen oder sonstigen Stellen der Europäischen Union bereit.

§ 14 Organisationsformen interner Meldestellen

(1) Eine interne Meldestelle kann eingerichtet werden, indem eine bei dem jeweiligen Beschäftigungsgeber oder bei der jeweiligen Organisationseinheit beschäftigte Person, eine aus mehreren beschäftigten Personen bestehende Arbeitseinheit oder ein Dritter mit den Aufgaben einer internen Meldestelle betraut wird. Die Betrauung eines Dritten mit den Aufgaben einer internen Meldestelle entbindet den betrauenden Beschäftigungsgeber nicht von der Pflicht, selbst geeignete Maßnahmen zu ergreifen, um einen etwaigen Verstoß abzustellen. Ist der Beschäftigungsgeber der Bund oder ein Land, gilt Satz 2 für die jeweiligen Organisationseinheiten entsprechend.

(2) Mehrere private Beschäftigungsgeber mit in der Regel 50 bis 249 Beschäftigten können für die Entgegennahme von Meldungen und für die weiteren nach diesem Gesetz vorgesehenen Maßnahmen eine gemeinsame Stelle einrichten und betreiben. Die Pflicht, Maßnahmen zu ergreifen, um den Verstoß abzustellen, und die Pflicht zur Rückmeldung an die hinweisgebende Person verbleiben bei dem einzelnen Beschäftigungsgeber.

§ 15 Unabhängige Tätigkeit; notwendige Fachkunde

(1) Die mit den Aufgaben einer internen Meldestelle beauftragten Personen sind bei der Ausübung ihrer Tätigkeit unabhängig. Sie dürfen neben ihrer Tätigkeit für die interne Meldestelle andere Aufgaben und Pflichten wahrnehmen. Es ist dabei sicherzustellen, dass derartige Aufgaben und Pflichten nicht zu Interessenkonflikten führen.

(2) Beschäftigungsgeber tragen dafür Sorge, dass die mit den Aufgaben einer internen Meldestelle beauftragten Personen über die notwendige Fachkunde verfügen. Ist der Beschäftigungsgeber der Bund oder ein Land, gilt Satz 1 für die jeweiligen Organisationseinheiten entsprechend.

§ 16 Meldekanäle für interne Meldestellen

(1) Nach § 12 zur Einrichtung interner Meldestellen verpflichtete Beschäftigungsgeber richten für diese Meldekanäle ein, über die sich Beschäftigte und dem Beschäftigungsgeber überlassene Leiharbeitnehmerinnen und Leiharbeitnehmer an die internen Meldestellen wenden können, um Informationen über Verstöße zu melden. Ist der Beschäftigungsgeber der Bund oder ein Land, gilt Satz 1 für die jeweiligen Organisationseinheiten entsprechend. Der interne Meldekanal kann so gestaltet werden, dass er darüber hinaus auch natürlichen Personen offensteht, die im Rahmen ihrer beruflichen Tätigkeiten mit dem jeweiligen zur Einrichtung der internen Meldestelle verpflichteten Beschäftigungsgeber oder mit der jeweiligen Organisationseinheit in Kontakt stehen. Die interne Meldestelle sollte auch anonym eingehende Meldungen bearbeiten. Es besteht allerdings keine Verpflichtung, die Meldekanäle so zu gestalten, dass sie die Abgabe anonymer Meldungen ermöglichen.

(2) Die Meldekanäle sind so zu gestalten, dass nur die für die Entgegennahme und Bearbeitung der Meldungen zuständigen sowie die sie bei der Erfüllung dieser Aufgaben unterstützenden Personen Zugriff auf die eingehenden Meldungen haben.

(3) Interne Meldekanäle müssen Meldungen in mündlicher oder in Textform ermöglichen. Mündliche Meldungen müssen per Telefon oder mittels einer anderen Art der Sprachübermittlung möglich sein. Auf Ersuchen der hinweisgebenden Person ist für eine Meldung innerhalb einer angemessenen Zeit eine persönliche Zusammenkunft mit einer für die Entgegennahme einer Meldung zuständigen Person der internen Meldestelle zu ermöglichen. Mit Einwilligung der hinweisgebenden Person kann die Zusammenkunft auch im Wege der Bild- und Tonübertragung erfolgen.

§ 17 Verfahren bei internen Meldungen

(1) Die interne Meldestelle

1. bestätigt der hinweisgebenden Person den Eingang einer Meldung spätestens nach sieben Tagen,
2. prüft, ob der gemeldete Verstoß in den sachlichen Anwendungsbereich nach § 2 fällt,

3. hält mit der hinweisgebenden Person Kontakt,
4. prüft die Stichhaltigkeit der eingegangenen Meldung,
5. ersucht die hinweisgebende Person erforderlichenfalls um weitere Informationen und
6. ergreift angemessene Folgemaßnahmen nach § 18.

(2) Die interne Meldestelle gibt der hinweisgebenden Person innerhalb von drei Monaten nach der Bestätigung des Eingangs der Meldung oder, wenn der Eingang nicht bestätigt wurde, spätestens drei Monate und sieben Tage nach Eingang der Meldung eine Rückmeldung. Die Rückmeldung umfasst die Mitteilung geplanter sowie bereits ergriffener Folgemaßnahmen sowie die Gründe für diese. Eine Rückmeldung an die hinweisgebende Person darf nur insoweit erfolgen, als dadurch interne Nachforschungen oder Ermittlungen nicht berührt und die Rechte der Personen, die Gegenstand einer Meldung sind oder die in der Meldung genannt werden, nicht beeinträchtigt werden.

§ 18 Folgemaßnahmen der internen Meldestelle

Als Folgemaßnahmen kann die interne Meldestelle insbesondere

1. interne Untersuchungen bei dem Beschäftigungsgeber oder bei der jeweiligen Organisationseinheit durchführen und betroffene Personen und Arbeitseinheiten kontaktieren,
2. die hinweisgebende Person an andere zuständige Stellen verweisen,
3. das Verfahren aus Mangel an Beweisen oder aus anderen Gründen abschließen oder
4. das Verfahren zwecks weiterer Untersuchungen abgeben an
   a) eine bei dem Beschäftigungsgeber oder bei der jeweiligen Organisationseinheit für interne Ermittlungen zuständige Arbeitseinheit oder
   b) eine zuständige Behörde.

Unterabschnitt 3
Externe Meldestellen

§ 19 Errichtung und Zuständigkeit einer externen Meldestelle des Bundes

(1) Der Bund errichtet beim Bundesamt für Justiz eine Stelle für externe Meldungen (externe Meldestelle des Bundes). Die externe Meldestelle des Bundes ist organisatorisch vom übrigen Zuständigkeitsbereich des Bundesamts für Justiz getrennt.

(2) Die Aufgaben der externen Meldestelle des Bundes werden unabhängig von den sonstigen Aufgaben des Bundesamts für Justiz wahrgenommen. Die Dienstaufsicht über die externe Meldestelle des Bundes führt die Präsidentin oder der Präsident des Bundesamts für Justiz. Die externe Meldestelle des Bundes untersteht einer Dienstaufsicht nur, soweit nicht ihre Unabhängigkeit beeinträchtigt wird.

(3) Der externen Meldestelle des Bundes ist die für die Erfüllung ihrer Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen.

(4) Die externe Meldestelle des Bundes ist zuständig, soweit nicht eine externe Meldestelle nach den §§ 20 bis 23 zuständig ist.

§ 20 Errichtung und Zuständigkeit externer Meldestellen der Länder

Jedes Land kann eine eigene externe Meldestelle einrichten für Meldungen, die die jeweilige Landesverwaltung und die jeweiligen Kommunalverwaltungen betreffen.

§ 21 Bundesanstalt für Finanzdienstleistungsaufsicht als externe Meldestelle

Die Bundesanstalt für Finanzdienstleistungsaufsicht ist zuständige externe Meldestelle für

1. Meldungen, die von § 4d des Finanzdienstleistungsaufsichtsgesetzes erfasst werden, einschließlich Meldungen, die Vorschriften des Wertpapiererwerbs- und Übernahmegesetzes betreffen,
2. Meldungen von Informationen über Verstöße
   a) nach § 2 Absatz 1 Nummer 3 Buchstabe a, soweit die Bundesanstalt für Finanzdienstleistungsaufsicht zuständige Behörde im Sinne des § 50 Absatz 1 Nummer 1 oder Nummer 2 des Geldwäschegesetzes ist, sowie
   b) nach § 2 Absatz 1 Nummer 3 Buchstabe r bis t.

Für die über dieses Gesetz hinausgehende nähere Ausgestaltung der Organisation und des Verfahrens der Bundesanstalt für Finanzdienstleistungsaufsicht als externe Meldestelle gilt § 4d des Finanzdienstleistungsaufsichtsgesetzes.

§ 22 Bundeskartellamt als externe Meldestelle

(1) Das Bundeskartellamt ist zuständige externe Meldestelle für Meldungen von Informationen über Verstöße nach § 2 Absatz 1 Nummer 8 und 9. § 7 Absatz 1 Satz 3 findet mit der Maßgabe Anwendung, dass sich die hinweisgebende Person jederzeit und unabhängig vom Ausgang des Verfahrens über die interne Meldung an das Bundeskartellamt wenden kann.

(2) Die Befugnisse des Bundeskartellamts nach anderen Vorschriften bleiben unberührt.

§ 23 Weitere externe Meldestellen

(1) Der Bund richtet eine weitere externe Meldestelle ein für externe Meldungen, die die externe Meldestelle des Bundes nach § 19 betreffen.

(2) Für Meldungen, die eine externe Meldestelle nach den §§ 20 bis 22 betreffen, ist weitere externe Meldestelle die externe Meldestelle des Bundes nach § 19.

§ 24 Aufgaben der externen Meldestellen

(1) Die externen Meldestellen errichten und betreiben Meldekanäle nach § 27, prüfen die Stichhaltigkeit einer Meldung und führen das Verfahren nach § 28.

(2) Die externen Meldestellen bieten natürlichen Personen, die in Erwägung ziehen, eine Meldung zu erstatten, umfassende und unabhängige Informationen und Beratung über bestehende Abhilfemöglichkeiten und Verfahren für den Schutz vor Repressalien. Dabei in-

formieren die externen Meldestellen insbesondere auch über die Möglichkeit einer internen Meldung.

(3) Die externen Meldestellen veröffentlichen in einem gesonderten, leicht erkennbaren und leicht zugänglichen Abschnitt ihres Internetauftritts

1. die Voraussetzungen für den Schutz nach Maßgabe dieses Gesetzes,
2. Erläuterungen zum Meldeverfahren sowie die Art der möglichen Folgemaßnahmen nach § 29,
3. die geltende Vertraulichkeitsregelung für Meldungen und Informationen über die Verarbeitung personenbezogener Daten,
4. Informationen über die verfügbaren Abhilfemöglichkeiten und Verfahren zum Schutz vor Repressalien sowie die Verfügbarkeit einer vertraulichen Beratung von Personen, die in Erwägung ziehen, eine Meldung zu erstatten,
5. eine leicht verständliche Erläuterung dazu, unter welchen Voraussetzungen Personen, die eine Meldung an die externe Meldestelle richten, nicht wegen Verletzung der Verschwiegenheits- und Geheimhaltungspflichten haftbar gemacht werden können,
6. ihre Erreichbarkeiten, insbesondere E-Mail-Adresse, Postanschrift und Telefonnummer, sowie die Angabe, ob Telefongespräche aufgezeichnet werden.

(4) Die externen Meldestellen halten klare und leicht zugängliche Informationen über ihre jeweiligen Meldeverfahren bereit, auf die interne Meldestellen zugreifen oder verweisen können, um ihrer Pflicht nach § 13 Absatz 2 nachzukommen. Die externe Meldestelle des Bundes hält zudem klare und leicht zugängliche Informationen über die in § 13 Absatz 2 genannten Meldeverfahren bereit, auf die interne Meldestellen zugreifen oder verweisen können, um ihrer Pflicht nach § 13 Absatz 2 nachzukommen.

§ 25 Unabhängige Tätigkeit; Schulung

(1) Die externen Meldestellen arbeiten im Rahmen ihrer Aufgaben und Befugnisse fachlich unabhängig und von den internen Meldestellen getrennt. Die Aufsicht über sie erstreckt sich auf die Beachtung von Gesetz und sonstigem Recht.

(2) Die für die Bearbeitung von Meldungen zuständigen Personen werden regelmäßig für diese Aufgabe geschult. Sie dürfen neben ihrer Tätigkeit für eine externe Meldestelle andere Aufgaben und Pflichten wahrnehmen. Es ist dabei sicherzustellen, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

§ 26 Berichtspflichten der externen Meldestellen

(1) Die externen Meldestellen berichten jährlich in zusammengefasster Form über die eingegangenen Meldungen. Der Bericht darf keine Rückschlüsse auf die beteiligten Personen oder Unternehmen zulassen. Er ist der Öffentlichkeit zugänglich zu machen.

(2) Für den Bericht erfassen die externen Meldestellen die folgenden Daten und weisen sie im Bericht aus:

1. die Anzahl der eingegangenen Meldungen,

2. die Anzahl der Fälle, in denen interne Untersuchungen bei den betroffenen Unternehmen oder Behörden eingeleitet wurden,
3. die Anzahl der Fälle, die Ermittlungen einer Staatsanwaltschaft oder ein gerichtliches Verfahren zur Folge hatten, und
4. die Anzahl der Fälle, die eine Abgabe an eine sonstige zuständige Stelle zur Folge hatten.

(3) Die externe Meldestelle des Bundes nach § 19 übermittelt ihren Jahresbericht darüber hinaus dem Deutschen Bundestag, dem Bundesrat und der Bundesregierung und übermittelt eine Zusammenstellung der Berichte nach den Absätzen 1 und 2 der Europäischen Kommission.

Unterabschnitt 4
Externe Meldungen

§ 27 Meldekanäle für externe Meldestellen

(1) Für externe Meldestellen werden Meldekanäle eingerichtet, über die sich hinweisgebende Personen an die externen Meldestellen wenden können, um Informationen über Verstöße zu melden. § 16 Absatz 2 gilt entsprechend. Die externe Meldestelle sollte auch anonym eingehende Meldungen bearbeiten. Vorbehaltlich spezialgesetzlicher Regelungen besteht allerdings keine Verpflichtung, die Meldekanäle so zu gestalten, dass sie die Abgabe anonymer Meldungen ermöglichen.

(2) Wird eine Meldung bei einer externen Meldestelle von anderen als den für die Bearbeitung zuständigen Personen entgegengenommen, so ist sie unverzüglich, unverändert und unmittelbar an die für die Bearbeitung zuständigen Personen weiterzuleiten.

(3) Externe Meldekanäle müssen Meldungen in mündlicher und in Textform ermöglichen. Mündliche Meldungen müssen per Telefon oder mittels einer anderen Art der Sprachübermittlung möglich sein. Auf Ersuchen der hinweisgebenden Person ist für eine Meldung innerhalb einer angemessenen Zeit eine persönliche Zusammenkunft mit den für die Entgegennahme einer Meldung zuständigen Personen der externen Meldestelle zu ermöglichen. Mit Einwilligung der hinweisgebenden Person kann die Zusammenkunft auch im Wege der Bild- und Tonübertragung erfolgen.

§ 28 Verfahren bei externen Meldungen

(1) Die externen Meldestellen bestätigen den Eingang einer Meldung umgehend, spätestens jedoch sieben Tage nach Eingang der Meldung. Eine Eingangsbestätigung erfolgt nicht, wenn die hinweisgebende Person darauf ausdrücklich verzichtet oder wenn hinreichender Grund zu der Annahme besteht, dass die Eingangsbestätigung den Schutz der Identität der hinweisgebenden Person beeinträchtigen würde. In für ein internes Meldeverfahren geeigneten Fällen weisen die externen Meldestellen zusammen mit der Eingangsbestätigung die hinweisgebende Person auf die Möglichkeit einer internen Meldung hin.

(2) Die externen Meldestellen prüfen, ob der gemeldete Verstoß in den sachlichen Anwendungsbereich nach § 2 fällt und keine Ausnahmen vom Anwendungsbereich dieses Gesetzes nach § 5 greifen. Ist dies der Fall, prüfen sie die Stichhaltigkeit der Meldung und ergreifen angemessene Folgemaßnahmen nach § 29.

(3) Für die Akteneinsicht durch Beteiligte im Sinne dieses Gesetzes gilt § 29 des Verwaltungsverfahrensgesetzes. Bestehende Verschwiegenheits- und Geheimhaltungspflichten im Sinne des § 6 Absatz 3 sind zu beachten. Für die hinweisgebende Person gelten die Sätze 1 und 2 entsprechend; hierbei ist sicherzustellen, dass die Rechte der Personen, die Gegenstand einer Meldung sind oder die in der Meldung genannt werden, nicht beeinträchtigt werden.

(4) Die hinweisgebende Person erhält auf ihre Meldung hin innerhalb einer angemessenen Zeit eine Rückmeldung. Diese erfolgt spätestens nach drei Monaten. In Fällen, in denen die Bearbeitung umfangreich ist, beträgt diese Frist sechs Monate. Die Gründe für die Verlängerung der Frist sind der hinweisgebenden Person mitzuteilen. § 17 Absatz 2 Satz 2 und 3 gilt entsprechend.

(5) Meldungen über Verstöße von besonderer Schwere können vorrangig behandelt werden. Die Fristen des Absatzes 4 für eine Rückmeldung bleiben davon unberührt.

§ 29 Folgemaßnahmen der externen Meldestellen

(1) Die externen Meldestellen können nach pflichtgemäßem Ermessen Auskünfte von den betroffenen natürlichen Personen, von dem betroffenen Beschäftigungsgeber, von Dritten sowie von Behörden verlangen, soweit dies zur Überprüfung der Stichhaltigkeit der Meldung erforderlich ist. Für die Beantwortung des Auskunftsverlangens ist eine angemessene Frist zu gewähren. Für Auskunftsverlangen nach Satz 1 gelten das Zeugnisverweigerungsrecht nach den §§ 53 und 53a und das Auskunftsverweigerungsrecht nach § 55 der Strafprozessordnung entsprechend. Für die Beantwortung von Auskunftsverlangen wird auf Antrag eine Entschädigung entsprechend den Vorschriften des Justizvergütungs- und -entschädigungsgesetzes über die Entschädigung von Zeugen gewährt. § 23 Absatz 2 Satz 2 des Justizvergütungs- und -entschädigungsgesetzes gilt entsprechend.

(2) Als weitere Folgemaßnahmen können die externen Meldestellen nach pflichtgemäßem Ermessen

1. betroffene Beschäftigungsgeber kontaktieren,
2. die hinweisgebende Person an andere zuständige Stellen verweisen,
3. das Verfahren aus Mangel an Beweisen oder aus anderen Gründen abschließen oder
4. das Verfahren an eine zuständige Behörde zwecks weiterer Untersuchungen abgeben.

§ 30 Zusammenarbeit mit anderen öffentlichen Stellen

Die externen Meldestellen sowie die sonstigen öffentlichen Stellen, die für die Aufklärung, Verhütung und Verfolgung von Verstößen im Anwendungsbereich dieses Gesetzes zuständig sind, arbeiten zur Durchführung dieses Gesetzes zusammen und unterstützen sich gegenseitig. Spezielle gesetzliche Regelungen zur Zusammenarbeit öffentlicher Stellen bleiben hiervon unberührt.

§ 31 Abschluss des Verfahrens

(1) Hat eine externe Meldestelle die Stichhaltigkeit einer Meldung geprüft und das Verfahren nach § 28 geführt, schließt sie das Verfahren ab.

(2) Ist eine externe Meldestelle nicht zuständig für eine Meldung oder ist es ihr nicht möglich, dem gemeldeten Verstoß innerhalb einer angemessenen Zeit weiter nachzugehen, so leitet sie die Meldung unverzüglich unter Wahrung der Vertraulichkeit der Identität der hinweisgebenden Person an die jeweilige für die Aufklärung, Verhütung und Verfolgung des Verstoßes zuständige Stelle weiter. Dies gilt auch für Meldungen, für deren Weiterverfolgung nach § 4 Absatz 1 die externe Meldestelle nicht zuständig ist. Über die Weiterleitung setzt die externe Meldestelle die hinweisgebende Person unverzüglich in Kenntnis. Ist die Weiterleitung unter Wahrung der Vertraulichkeit der Identität nicht möglich, ist § 9 Absatz 3 zu beachten.

(3) Kommt eine externe Meldestelle zu dem Ergebnis, dass ein gemeldeter Verstoß als geringfügig anzusehen ist, so kann sie nach pflichtgemäßem Ermessen das Verfahren abschließen.

(4) Betrifft eine Meldung einen Sachverhalt, zu dem bereits ein Verfahren nach diesem Gesetz abgeschlossen wurde, so kann eine externe Meldestelle nach pflichtgemäßem Ermessen das Verfahren abschließen, wenn die Meldung keine neuen Tatsachen enthält. Dies gilt nicht, wenn neue rechtliche oder sachliche Umstände ein anderes Vorgehen rechtfertigen.

(5) Schließt eine externe Meldestelle das Verfahren nach Absatz 3 oder Absatz 4 ab, teilt sie der hinweisgebenden Person die Entscheidung und die Gründe für die Entscheidung unverzüglich mit. Die externe Meldestelle soll die Entscheidung nach Satz 1 unter Wahrung der Vertraulichkeit der Identität der in § 8 Absatz 1 genannten Personen dem betroffenen Beschäftigungsgeber mitteilen, wenn dieser zuvor gemäß § 29 Absatz 2 Nummer 1 von der externen Meldestelle kontaktiert wurde.

(6) Eine externe Meldestelle teilt der hinweisgebenden Person das Ergebnis der durch die Meldung ausgelösten Untersuchungen nach deren Abschluss mit, soweit dies mit gesetzlichen Verschwiegenheitspflichten vereinbar ist. Absatz 5 Satz 2 ist anzuwenden.

(7) Für Streitigkeiten wegen der Entscheidungen einer externen Meldestelle nach den Absätzen 1 bis 6 ist der Verwaltungsrechtsweg gegeben. Vor Erhebung einer Klage bedarf es keiner Nachprüfung in einem Vorverfahren.

Abschnitt 3
Offenlegung

§ 32 Offenlegen von Informationen

(1) Personen, die Informationen über Verstöße offenlegen, fallen unter die Schutzmaßnahmen dieses Gesetzes, wenn sie

1. zunächst gemäß Abschnitt 2 Unterabschnitt 4 eine externe Meldung erstattet haben und
   a) hierauf innerhalb der Fristen für eine Rückmeldung nach § 28 Absatz 4 keine geeigneten Folgemaßnahmen nach § 29 ergriffen wurden oder
   b) sie keine Rückmeldung über das Ergreifen solcher Folgemaßnahmen erhalten haben oder
2. hinreichenden Grund zu der Annahme hatten, dass

a) der Verstoß wegen eines Notfalls, der Gefahr irreversibler Schäden oder vergleichbarer Umstände eine unmittelbare oder offenkundige Gefährdung des öffentlichen Interesses darstellen kann,

b) im Fall einer externen Meldung Repressalien zu befürchten sind oder

c) Beweismittel unterdrückt oder vernichtet werden könnten, Absprachen zwischen der zuständigen externen Meldestelle und dem Urheber des Verstoßes bestehen könnten oder aufgrund sonstiger besonderer Umstände die Aussichten gering sind, dass die externe Meldestelle wirksame Folgemaßnahmen nach § 29 einleiten wird.

(2) Das Offenlegen unrichtiger Informationen über Verstöße ist verboten.

Abschnitt 4
Schutzmaßnahmen

§ 33 Voraussetzungen für den Schutz hinweisgebender Personen

(1) Die §§ 35 bis 37 sind auf hinweisgebende Personen anwendbar, sofern

1. diese intern gemäß § 17 oder extern gemäß § 28 Meldung erstattet haben oder eine Offenlegung gemäß § 32 vorgenommen haben,
2. die hinweisgebende Person zum Zeitpunkt der Meldung oder Offenlegung hinreichenden Grund zu der Annahme hatte, dass die von ihr gemeldeten oder offengelegten Informationen der Wahrheit entsprechen, und
3. die Informationen Verstöße betreffen, die in den Anwendungsbereich dieses Gesetzes fallen, oder die hinweisgebende Person zum Zeitpunkt der Meldung oder Offenlegung hinreichenden Grund zu der Annahme hatte, dass dies der Fall sei.

(2) Die §§ 35 bis 37 sind unter den Voraussetzungen des Absatzes 1 auch anwendbar auf Personen, die zuständigen Organen, Einrichtungen oder sonstigen Stellen der Europäischen Union in den Anwendungsbereich dieses Gesetzes fallende Verstöße gegen das Unionsrecht melden.

§ 34 Weitere geschützte Personen

(1) Die §§ 35 bis 37 gelten entsprechend für natürliche Personen, die die hinweisgebende Person bei einer internen oder externen Meldung oder einer Offenlegung im beruflichen Zusammenhang vertraulich unterstützen, sofern die gemeldeten oder offengelegten Informationen

1. zutreffend sind oder die unterstützende Person zum Zeitpunkt der Unterstützung hinreichenden Grund zu der Annahme hatte, dass die von der hinweisgebenden Person gemeldeten oder offengelegten Informationen der Wahrheit entsprachen, und
2. Verstöße betreffen, die in den Anwendungsbereich dieses Gesetzes fallen, oder die unterstützende Person zum Zeitpunkt der Unterstützung hinreichenden Grund zu der Annahme hatte, dass dies der Fall sei.

(2) Sofern die Voraussetzungen des § 33 erfüllt sind, gelten die §§ 35 bis 37 entsprechend für

1. Dritte, die mit der hinweisgebenden Person in Verbindung stehen und in einem beruflichen Zusammenhang Repressalien erlitten haben, es sei denn, diese beruhen nicht auf der Meldung oder Offenlegung durch die hinweisgebende Person, und
2. juristische Personen, rechtsfähige Personengesellschaften und sonstige rechtsfähige Personenvereinigungen, die mit der hinweisgebenden Person infolge einer Beteiligung rechtlich verbunden sind oder für die die hinweisgebende Person tätig ist oder mit denen sie in einem beruflichen Kontext anderweitig in Verbindung steht.

§ 35 Ausschluss der Verantwortlichkeit

(1) Eine hinweisgebende Person kann nicht für die Beschaffung von oder den Zugriff auf Informationen, die sie gemeldet oder offengelegt hat, rechtlich verantwortlich gemacht werden, sofern die Beschaffung nicht als solche oder der Zugriff nicht als solcher eine eigenständige Straftat darstellt.

(2) Eine hinweisgebende Person verletzt keine Offenlegungsbeschränkungen und kann nicht für die bei einer Meldung oder Offenlegung erfolgte Weitergabe von Informationen rechtlich verantwortlich gemacht werden, sofern sie hinreichenden Grund zu der Annahme hatte, dass die Weitergabe der Informationen erforderlich war, um einen Verstoß aufzudecken.

§ 36 Verbot von Repressalien; Beweislastumkehr

(1) Gegen hinweisgebende Personen gerichtete Repressalien sind verboten. Das gilt auch für die Androhung und den Versuch, Repressalien auszuüben.

(2) Erleidet eine hinweisgebende Person eine Benachteiligung im Zusammenhang mit ihrer beruflichen Tätigkeit und macht sie geltend, diese Benachteiligung infolge einer Meldung oder Offenlegung nach diesem Gesetz erlitten zu haben, so wird vermutet, dass diese Benachteiligung eine Repressalie für diese Meldung oder Offenlegung ist. In diesem Fall hat die Person, die die hinweisgebende Person benachteiligt hat, zu beweisen, dass die Benachteiligung auf hinreichend gerechtfertigten Gründen basierte oder dass sie nicht auf der Meldung oder Offenlegung beruhte.

§ 37 Schadensersatz nach Repressalien

(1) Bei einem Verstoß gegen das Verbot von Repressalien ist der Verursacher verpflichtet, der hinweisgebenden Person den daraus entstehenden Schaden zu ersetzen.

(2) Ein Verstoß gegen das Verbot von Repressalien begründet keinen Anspruch auf Begründung eines Beschäftigungsverhältnisses, eines Berufsausbildungsverhältnisses oder eines anderen Vertragsverhältnisses oder auf einen beruflichen Aufstieg.

§ 38 Schadensersatz nach einer Falschmeldung

Die hinweisgebende Person ist zum Ersatz des Schadens verpflichtet, der aus einer vorsätzlichen oder grob fahrlässigen Meldung oder Offenlegung unrichtiger Informationen entstanden ist.

§ 39 Verbot abweichender Vereinbarungen

Vereinbarungen, die die nach diesem Gesetz bestehenden Rechte hinweisgebender Personen oder sonst nach diesem Gesetz geschützter Personen einschränken, sind unwirksam.

Abschnitt 5
Sanktionen

§ 40 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer wissentlich entgegen § 32 Absatz 2 eine unrichtige Information offenlegt.

(2) Ordnungswidrig handelt, wer

1. entgegen § 7 Absatz 2 eine Meldung oder dort genannte Kommunikation behindert,
2. entgegen § 12 Absatz 1 Satz 1 nicht dafür sorgt, dass eine interne Meldestelle eingerichtet ist und betrieben wird, oder
3. entgegen § 36 Absatz 1 Satz 1, auch in Verbindung mit § 34, eine Repressalie ergreift.

(3) Ordnungswidrig handelt, wer vorsätzlich oder leichtfertig entgegen § 8 Absatz 1 Satz 1 die Vertraulichkeit nicht wahrt.

(4) Ordnungswidrig handelt, wer eine in Absatz 3 bezeichnete Handlung fahrlässig begeht.

(5) Der Versuch einer Ordnungswidrigkeit kann in den Fällen des Absatzes 2 Nummer 1 und 3 geahndet werden.

(6) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 2 Nummer 1 und 3, der Absätze 3 und 5 mit einer Geldbuße bis zu fünfzigtausend Euro, in den Fällen der Absätze 1 und 2 Nummer 2 mit einer Geldbuße bis zu zwanzigtausend Euro und in den übrigen Fällen mit einer Geldbuße bis zu zehntausend Euro geahndet werden. § 30 Absatz 2 Satz 3 des Gesetzes über Ordnungswidrigkeiten ist in den Fällen des Absatzes 2 Nummer 1 und 3 und der Absätze 3 und 4 anzuwenden.

Abschnitt 6
Schlussvorschriften

§ 41 Verordnungsermächtigung

Das Bundesministerium der Justiz wird ermächtigt, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, im Einvernehmen mit dem Bundesministerium für Wirtschaft und Klimaschutz, dem Bundesministerium der Finanzen, dem Bundesministerium des Innern und für Heimat, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium der Verteidigung, dem Bundesministerium für Gesundheit und dem Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz

1. die nähere Ausgestaltung der Organisation und des Verfahrens der externen Meldestelle des Bundes zu regeln und
2. eine weitere externe Meldestelle nach § 23 Absatz 1 zu bestimmen.

§ 42 Übergangsregelung

(1) Abweichend von § 12 Absatz 1 müssen private Beschäftigungsgeber mit in der Regel 50 bis 249 Beschäftigten ihre internen Meldestellen erst ab dem 17. Dezember 2023 einrichten. Satz 1 gilt nicht für die in § 12 Absatz 3 genannten Beschäftigungsgeber.

(2) § 40 Absatz 2 Nummer 2 ist erst ab dem 1. Dezember 2023 anzuwenden.

Strafgesetzbuch (StGB)

§ 1 Keine Strafe ohne Gesetz

Eine Tat kann nur bestraft werden, wenn die Strafbarkeit gesetzlich bestimmt war, bevor die Tat begangen wurde.

§ 93 Begriff des Staatsgeheimnisses

(1) Staatsgeheimnisse sind Tatsachen, Gegenstände oder Erkenntnisse, die nur einem begrenzten Personenkreis zugänglich sind und vor einer fremden Macht geheimgehalten werden müssen, um die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland abzuwenden.

(2) Tatsachen, die gegen die freiheitliche demokratische Grundordnung oder unter Geheimhaltung gegenüber den Vertragspartnern der Bundesrepublik Deutschland gegen zwischenstaatlich vereinbarte Rüstungsbeschränkungen verstoßen, sind keine Staatsgeheimnisse.

§ 94 Landesverrat

(1) Wer ein Staatsgeheimnis

1. einer fremden Macht oder einem ihrer Mittelsmänner mitteilt oder
2. sonst an einen Unbefugten gelangen läßt oder öffentlich bekanntmacht, um die Bundesrepublik Deutschland zu benachteiligen oder eine fremde Macht zu begünstigen,

und dadurch die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland herbeiführt, wird mit Freiheitsstrafe nicht unter einem Jahr bestraft.

(2) In besonders schweren Fällen ist die Strafe lebenslange Freiheitsstrafe oder Freiheitsstrafe nicht unter fünf Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. eine verantwortliche Stellung mißbraucht, die ihn zur Wahrung von Staatsgeheimnissen besonders verpflichtet, oder
2. durch die Tat die Gefahr eines besonders schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland herbeiführt.

§ 95 Offenbaren von Staatsgeheimnissen

(1) Wer ein Staatsgeheimnis, das von einer amtlichen Stelle oder auf deren Veranlassung geheimgehalten wird, an einen Unbefugten gelangen läßt oder öffentlich bekanntmacht und dadurch die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland herbeiführt, wird mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren bestraft, wenn die Tat nicht in § 94 mit Strafe bedroht ist.

(2) Der Versuch ist strafbar.

(3) In besonders schweren Fällen ist die Strafe Freiheitsstrafe von einem Jahr bis zu zehn Jahren. § 94 Abs. 2 Satz 2 ist anzuwenden.

StGB (Auszug)

§ 96 Landesverräterische Ausspähung; Auskundschaften von Staatsgeheimnissen

(1) Wer sich ein Staatsgeheimnis verschafft, um es zu verraten (§ 94), wird mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren bestraft.

(2) Wer sich ein Staatsgeheimnis, das von einer amtlichen Stelle oder auf deren Veranlassung geheimgehalten wird, verschafft, um es zu offenbaren (§ 95), wird mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren bestraft. Der Versuch ist strafbar.

§ 97 Preisgabe von Staatsgeheimnissen

(1) Wer ein Staatsgeheimnis, das von einer amtlichen Stelle oder auf deren Veranlassung geheimgehalten wird, an einen Unbefugten gelangen läßt oder öffentlich bekanntmacht und dadurch fahrlässig die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland verursacht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Wer ein Staatsgeheimnis, das von einer amtlichen Stelle oder auf deren Veranlassung geheimgehalten wird und das ihm kraft seines Amtes, seiner Dienststellung oder eines von einer amtlichen Stelle erteilten Auftrags zugänglich war, leichtfertig an einen Unbefugten gelangen läßt und dadurch fahrlässig die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland verursacht, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(3) Die Tat wird nur mit Ermächtigung der Bundesregierung verfolgt.

§ 97a Verrat illegaler Geheimnisse

Wer ein Geheimnis, das wegen eines der in § 93 Abs. 2 bezeichneten Verstöße kein Staatsgeheimnis ist, einer fremden Macht oder einem ihrer Mittelsmänner mitteilt und dadurch die Gefahr eines schweren Nachteils für die äußere Sicherheit der Bundesrepublik Deutschland herbeiführt, wird wie ein Landesverräter (§ 94) bestraft. § 96 Abs. 1 in Verbindung mit § 94 Abs. 1 Nr. 1 ist auf Geheimnisse der in Satz 1 bezeichneten Art entsprechend anzuwenden.

§ 97b Verrat in irriger Annahme eines illegalen Geheimnisses

(1) Handelt der Täter in den Fällen der §§ 94 bis 97 in der irrigen Annahme, das Staatsgeheimnis sei ein Geheimnis der in § 97a bezeichneten Art, so wird er, wenn

1. dieser Irrtum ihm vorzuwerfen ist,
2. er nicht in der Absicht handelt, dem vermeintlichen Verstoß entgegenzuwirken, oder
3. die Tat nach den Umständen kein angemessenes Mittel zu diesem Zweck ist,

nach den bezeichneten Vorschriften bestraft. Die Tat ist in der Regel kein angemessenes Mittel, wenn der Täter nicht zuvor ein Mitglied des Bundestages um Abhilfe angerufen hat.

(2) War dem Täter als Amtsträger oder als Soldat der Bundeswehr das Staatsgeheimnis dienstlich anvertraut oder zugänglich, so wird er auch dann bestraft, wenn nicht zuvor der Amtsträger einen Dienstvorgesetzten, der Soldat einen Disziplinarvorgesetzten um Abhilfe angerufen hat. Dies gilt für die für den öffentlichen Dienst besonders Verpflichteten und für Personen, die im Sinne des § 353b Abs. 2 verpflichtet worden sind, sinngemäß.

§ 98 Landesverräterische Agententätigkeit

(1) Wer

1. für eine fremde Macht eine Tätigkeit ausübt, die auf die Erlangung oder Mitteilung von Staatsgeheimnissen gerichtet ist, oder
2. gegenüber einer fremden Macht oder einem ihrer Mittelsmänner sich zu einer solchen Tätigkeit bereit erklärt,

wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in § 94 oder § 96 Abs. 1 mit Strafe bedroht ist. In besonders schweren Fällen ist die Strafe Freiheitsstrafe von einem Jahr bis zu zehn Jahren; § 94 Abs. 2 Satz 2 Nr. 1 gilt entsprechend.

(2) Das Gericht kann die Strafe nach seinem Ermessen mildern (§ 49 Abs. 2) oder von einer Bestrafung nach diesen Vorschriften absehen, wenn der Täter freiwillig sein Verhalten aufgibt und sein Wissen einer Dienststelle offenbart. Ist der Täter in den Fällen des Absatzes 1 Satz 1 von der fremden Macht oder einem ihrer Mittelsmänner zu seinem Verhalten gedrängt worden, so wird er nach dieser Vorschrift nicht bestraft, wenn er freiwillig sein Verhalten aufgibt und sein Wissen unverzüglich einer Dienststelle offenbart.

§ 99 Geheimdienstliche Agententätigkeit

(1) Wer

1. für den Geheimdienst einer fremden Macht eine geheimdienstliche Tätigkeit gegen die Bundesrepublik Deutschland ausübt, die auf die Mitteilung oder Lieferung von Tatsachen, Gegenständen oder Erkenntnissen gerichtet ist, oder
2. gegenüber dem Geheimdienst einer fremden Macht oder einem seiner Mittelsmänner sich zu einer solchen Tätigkeit bereit erklärt,

wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in § 94 oder § 96 Abs. 1, in § 97a oder in § 97b in Verbindung mit § 94 oder § 96 Abs. 1 mit Strafe bedroht ist.

(2) In besonders schweren Fällen ist die Strafe Freiheitsstrafe von einem Jahr bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter Tatsachen, Gegenstände oder Erkenntnisse, die von einer amtlichen Stelle oder auf deren Veranlassung geheimgehalten werden, mitteilt oder liefert und wenn er

1. eine verantwortliche Stellung mißbraucht, die ihn zur Wahrung solcher Geheimnisse besonders verpflichtet, oder
2. durch die Tat die Gefahr eines schweren Nachteils für die Bundesrepublik Deutschland herbeiführt.

(3) § 98 Abs. 2 gilt entsprechend.

§ 109f Sicherheitsgefährdender Nachrichtendienst

(1) Wer für eine Dienststelle, eine Partei oder eine andere Vereinigung außerhalb des räumlichen Geltungsbereichs dieses Gesetzes, für eine verbotene Vereinigung oder für einen ihrer Mittelsmänner

1. Nachrichten über Angelegenheiten der Landesverteidigung sammelt,

2. einen Nachrichtendienst betreibt, der Angelegenheiten der Landesverteidigung zum Gegenstand hat, oder
3. für eine dieser Tätigkeiten anwirbt oder sie unterstützt

und dadurch Bestrebungen dient, die gegen die Sicherheit der Bundesrepublik Deutschland oder die Schlagkraft der Truppe gerichtet sind, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist. Ausgenommen ist eine zur Unterrichtung der Öffentlichkeit im Rahmen der üblichen Presse- oder Funkberichterstattung ausgeübte Tätigkeit.

(2) Der Versuch ist strafbar.

§ 109g Sicherheitsgefährdendes Abbilden

(1) Wer von einem Wehrmittel, einer militärischen Einrichtung oder Anlage oder einem militärischen Vorgang eine Abbildung oder Beschreibung anfertigt oder eine solche Abbildung oder Beschreibung an einen anderen gelangen läßt und dadurch wissentlich die Sicherheit der Bundesrepublik Deutschland oder die Schlagkraft der Truppe gefährdet, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Wer von einem Luftfahrzeug aus eine Lichtbildaufnahme von einem Gebiet oder Gegenstand im räumlichen Geltungsbereich dieses Gesetzes anfertigt oder eine solche Aufnahme oder eine danach hergestellte Abbildung an einen anderen gelangen läßt und dadurch wissentlich die Sicherheit der Bundesrepublik Deutschland oder die Schlagkraft der Truppe gefährdet, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in Absatz 1 mit Strafe bedroht ist.

(3) Der Versuch ist strafbar.

(4) Wer in den Fällen des Absatzes 1 die Abbildung oder Beschreibung an einen anderen gelangen läßt und dadurch die Gefahr nicht wissentlich, aber vorsätzlich oder leichtfertig herbeiführt, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Die Tat ist jedoch nicht strafbar, wenn der Täter mit Erlaubnis der zuständigen Dienststelle gehandelt hat.

§ 126a Gefährdendes Verbreiten personenbezogener Daten

(1) Wer öffentlich, in einer Versammlung oder durch Verbreiten eines Inhalts (§ 11 Absatz 3) personenbezogene Daten einer anderen Person in einer Art und Weise verbreitet, die geeignet und nach den Umständen bestimmt ist, diese Person oder eine ihr nahestehende Person der Gefahr

1. eines gegen sie gerichteten Verbrechens oder
2. einer gegen sie gerichteten sonstigen rechtswidrigen Tat gegen die sexuelle Selbstbestimmung, die körperliche Unversehrtheit, die persönliche Freiheit oder gegen eine Sache von bedeutendem Wert

auszusetzen, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Handelt es sich um nicht allgemein zugängliche Daten, so ist die Strafe Freiheitsstrafe bis zu drei Jahren oder Geldstrafe.

(3) § 86 Absatz 4 gilt entsprechend.

§ 127 Betreiben krimineller Handelsplattformen im Internet

(1) Wer eine Handelsplattform im Internet betreibt, deren Zweck darauf ausgerichtet ist, die Begehung von rechtswidrigen Taten zu ermöglichen oder zu fördern, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist. Rechtswidrige Taten im Sinne des Satzes 1 sind

1. Verbrechen,
2. Vergehen nach
   a) den §§ 86, 86a, 91, 130, 147 und 148 Absatz 1 Nummer 3, den §§ 149, 152a und 176a Absatz 2, § 176b Absatz 2, § 180 Absatz 2, § 184b Absatz 1, § 184c Absatz 1, § 184l Absatz 1 und 3, den §§ 202a, 202b, 202c, 202d, 232 und 232a Absatz 1, 2, 5 und 6, nach § 232b Absatz 1, 2 und 4 in Verbindung mit § 232a Absatz 5, nach den §§ 233, 233a, 236, 259 und 260, nach § 261 Absatz 1 und 2 unter den in § 261 Absatz 5 Satz 2 genannten Voraussetzungen sowie nach den §§ 263, 263a, 267, 269, 275, 276, 303a und 303b,
   b) § 4 Absatz 1 bis 3 des Anti-Doping-Gesetzes,
   c) § 29 Absatz 1 Satz 1 Nummer 1, auch in Verbindung mit Absatz 6, sowie Absatz 2 und 3 des Betäubungsmittelgesetzes,
   d) § 19 Absatz 1 bis 3 des Grundstoffüberwachungsgesetzes,
   e) § 4 Absatz 1 und 2 des Neue-psychoaktive-Stoffe-Gesetzes,
   f) § 95 Absatz 1 bis 3 des Arzneimittelgesetzes,
   g) § 52 Absatz 1 Nummer 1 und 2 Buchstabe b und c, Absatz 2 und 3 Nummer 1 und 7 sowie Absatz 5 und 6 des Waffengesetzes,
   h) § 40 Absatz 1 bis 3 des Sprengstoffgesetzes,
   i) § 13 des Ausgangsstoffgesetzes,
   j) § 83 Absatz 1 Nummer 4 und 5 sowie Absatz 4 des Kulturgutschutzgesetzes,
   k) den §§ 143, 143a und 144 des Markengesetzes sowie
   l) den §§ 51 und 65 des Designgesetzes.

(2) Handelsplattform im Internet im Sinne dieser Vorschrift ist jede virtuelle Infrastruktur im frei zugänglichen wie im durch technische Vorkehrungen zugangsbeschränkten Bereich des Internets, die Gelegenheit bietet, Menschen, Waren, Dienstleistungen oder Inhalte (§ 11 Absatz 3) anzubieten oder auszutauschen.

(3) Mit Freiheitsstrafe von sechs Monaten bis zu zehn Jahren wird bestraft, wer im Fall des Absatzes 1 gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung solcher Taten verbunden hat.

(4) Mit Freiheitsstrafe von einem Jahr bis zu zehn Jahren wird bestraft, wer bei der Begehung einer Tat nach Absatz 1 beabsichtigt oder weiß, dass die Handelsplattform im Internet den Zweck hat, Verbrechen zu ermöglichen oder zu fördern.

StGB (Auszug)

§ 201 Verletzung der Vertraulichkeit des Wortes

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer unbefugt

1. das nichtöffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt oder
2. eine so hergestellte Aufnahme gebraucht oder einem Dritten zugänglich macht.

(2) Ebenso wird bestraft, wer unbefugt

1. das nicht zu seiner Kenntnis bestimmte nichtöffentlich gesprochene Wort eines anderen mit einem Abhörgerät abhört oder
2. das nach Absatz 1 Nr. 1 aufgenommene oder nach Absatz 2 Nr. 1 abgehörte nichtöffentlich gesprochene Wort eines anderen im Wortlaut oder seinem wesentlichen Inhalt nach öffentlich mitteilt.

Die Tat nach Satz 1 Nr. 2 ist nur strafbar, wenn die öffentliche Mitteilung geeignet ist, berechtigte Interessen eines anderen zu beeinträchtigen. Sie ist nicht rechtswidrig, wenn die öffentliche Mitteilung zur Wahrnehmung überragender öffentlicher Interessen gemacht wird.

(3) Mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe wird bestraft, wer als Amtsträger oder als für den öffentlichen Dienst besonders Verpflichteter die Vertraulichkeit des Wortes verletzt (Absätze 1 und 2).

(4) Der Versuch ist strafbar.

(5) Die Tonträger und Abhörgeräte, die der Täter oder Teilnehmer verwendet hat, können eingezogen werden. § 74a ist anzuwenden.

§ 201a Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen

(1) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer

1. von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, unbefugt eine Bildaufnahme herstellt oder überträgt und dadurch den höchstpersönlichen Lebensbereich der abgebildeten Person verletzt,
2. eine Bildaufnahme, die die Hilflosigkeit einer anderen Person zur Schau stellt, unbefugt herstellt oder überträgt und dadurch den höchstpersönlichen Lebensbereich der abgebildeten Person verletzt,
3. eine Bildaufnahme, die in grob anstößiger Weise eine verstorbene Person zur Schau stellt, unbefugt herstellt oder überträgt,
4. eine durch eine Tat nach den Nummern 1 bis 3 hergestellte Bildaufnahme gebraucht oder einer dritten Person zugänglich macht oder
5. eine befugt hergestellte Bildaufnahme der in den Nummern 1 bis 3 bezeichneten Art wissentlich unbefugt einer dritten Person zugänglich macht und in den Fällen der Nummern 1 und 2 dadurch den höchstpersönlichen Lebensbereich der abgebildeten Person verletzt.

(2) Ebenso wird bestraft, wer unbefugt von einer anderen Person eine Bildaufnahme, die geeignet ist, dem Ansehen der abgebildeten Person erheblich zu schaden, einer dritten Person zugänglich macht. Dies gilt unter den gleichen Voraussetzungen auch für eine Bildaufnahme von einer verstorbenen Person.

(3) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer eine Bildaufnahme, die die Nacktheit einer anderen Person unter achtzehn Jahren zum Gegenstand hat,

1. herstellt oder anbietet, um sie einer dritten Person gegen Entgelt zu verschaffen, oder
2. sich oder einer dritten Person gegen Entgelt verschafft.

(4) Absatz 1 Nummer 2 und 3, auch in Verbindung mit Absatz 1 Nummer 4 oder 5, Absatz 2 und 3 gelten nicht für Handlungen, die in Wahrnehmung überwiegender berechtigter Interessen erfolgen, namentlich der Kunst oder der Wissenschaft, der Forschung oder der Lehre, der Berichterstattung über Vorgänge des Zeitgeschehens oder der Geschichte oder ähnlichen Zwecken dienen.

(5) Die Bildträger sowie Bildaufnahmegeräte oder andere technische Mittel, die der Täter oder Teilnehmer verwendet hat, können eingezogen werden. § 74a ist anzuwenden.

§ 202 Verletzung des Briefgeheimnisses

(1) Wer unbefugt

1. einen verschlossenen Brief oder ein anderes verschlossenes Schriftstück, die nicht zu seiner Kenntnis bestimmt sind, öffnet oder
2. sich vom Inhalt eines solchen Schriftstücks ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,

wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft, wenn die Tat nicht in § 206 mit Strafe bedroht ist.

(2) Ebenso wird bestraft, wer sich unbefugt vom Inhalt eines Schriftstücks, das nicht zu seiner Kenntnis bestimmt und durch ein verschlossenes Behältnis gegen Kenntnisnahme besonders gesichert ist, Kenntnis verschafft, nachdem er dazu das Behältnis geöffnet hat.

(3) Einem Schriftstück im Sinne der Absätze 1 und 2 steht eine Abbildung gleich.

§ 202a Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 202b Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung

oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

§ 202c Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder
2. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist,

herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) § 149 Abs. 2 und 3 gilt entsprechend.

§ 202d Datenhehlerei

(1) Wer Daten (§ 202a Absatz 2), die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Die Strafe darf nicht schwerer sein als die für die Vortat angedrohte Strafe.

(3) Absatz 1 gilt nicht für Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Dazu gehören insbesondere

1. solche Handlungen von Amtsträgern oder deren Beauftragten, mit denen Daten ausschließlich der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren zugeführt werden sollen, sowie
2. solche beruflichen Handlungen der in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Personen, mit denen Daten entgegengenommen, ausgewertet oder veröffentlicht werden.

§ 203 Verletzung von Privatgeheimnissen

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Arzt, Zahnarzt, Tierarzt, Apotheker oder Angehörigen eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert,
2. Berufspsychologen mit staatlich anerkannter wissenschaftlicher Abschlußprüfung,
3. Rechtsanwalt, Kammerrechtsbeistand, Patentanwalt, Notar, Verteidiger in einem gesetzlich geordneten Verfahren, Wirtschaftsprüfer, vereidigtem Buchprüfer, Steuerberater, Steuerbevollmächtigten,

3a. Organ oder Mitglied eines Organs einer Wirtschaftsprüfungs-, Buchprüfungs- oder einer Berufsausübungsgesellschaft von Steuerberatern und Steuerbevollmächtigten, einer Berufsausübungsgesellschaft von Rechtsanwälten oder europäischen niedergelassenen Rechtsanwälten oder einer Berufsausübungsgesellschaft von Patentanwälten oder niedergelassenen europäischen Patentanwälten im Zusammenhang mit der Beratung und Vertretung der Wirtschaftsprüfungs-, Buchprüfungs- oder Berufsausübungsgesellschaft im Bereich der Wirtschaftsprüfung, Buchprüfung oder Hilfeleistung in Steuersachen oder ihrer rechtsanwaltlichen oder patentanwaltlichen Tätigkeit,

4. Ehe-, Familien-, Erziehungs- oder Jugendberater sowie Berater für Suchtfragen in einer Beratungsstelle, die von einer Behörde oder Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts anerkannt ist,

5. Mitglied oder Beauftragten einer anerkannten Beratungsstelle nach den §§ 3 und 8 Absatz 1 des Schwangerschaftskonfliktgesetzes,

6. staatlich anerkanntem Sozialarbeiter oder staatlich anerkanntem Sozialpädagogen oder

7. Angehörigen eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen, steuerberaterlichen oder anwaltlichen Verrechnungsstelle

anvertraut worden oder sonst bekanntgeworden ist, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer unbefugt ein fremdes Geheimnis, namentlich ein zum persönlichen Lebensbereich gehörendes Geheimnis oder ein Betriebs- oder Geschäftsgeheimnis, offenbart, das ihm als

1. Amtsträger oder Europäischer Amtsträger,

2. für den öffentlichen Dienst besonders Verpflichteten,

3. Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt,

4. Mitglied eines für ein Gesetzgebungsorgan des Bundes oder eines Landes tätigen Untersuchungsausschusses, sonstigen Ausschusses oder Rates, das nicht selbst Mitglied des Gesetzgebungsorgans ist, oder als Hilfskraft eines solchen Ausschusses oder Rates,

5. öffentlich bestelltem Sachverständigen, der auf die gewissenhafte Erfüllung seiner Obliegenheiten auf Grund eines Gesetzes förmlich verpflichtet worden ist, oder

6. Person, die auf die gewissenhafte Erfüllung ihrer Geheimhaltungspflicht bei der Durchführung wissenschaftlicher Forschungsvorhaben auf Grund eines Gesetzes förmlich verpflichtet worden ist,

anvertraut worden oder sonst bekanntgeworden ist. Einem Geheimnis im Sinne des Satzes 1 stehen Einzelangaben über persönliche oder sachliche Verhältnisse eines anderen gleich, die für Aufgaben der öffentlichen Verwaltung erfaßt worden sind; Satz 1 ist jedoch nicht anzuwenden, soweit solche Einzelangaben anderen Behörden oder sonstigen Stellen für Aufga-

ben der öffentlichen Verwaltung bekanntgegeben werden und das Gesetz dies nicht untersagt.

(2a) (weggefallen)

(3) Kein Offenbaren im Sinne dieser Vorschrift liegt vor, wenn die in den Absätzen 1 und 2 genannten Personen Geheimnisse den bei ihnen berufsmäßig tätigen Gehilfen oder den bei ihnen zur Vorbereitung auf den Beruf tätigen Personen zugänglich machen. Die in den Absätzen 1 und 2 Genannten dürfen fremde Geheimnisse gegenüber sonstigen Personen offenbaren, die an ihrer beruflichen oder dienstlichen Tätigkeit mitwirken, soweit dies für die Inanspruchnahme der Tätigkeit der sonstigen mitwirkenden Personen erforderlich ist; das Gleiche gilt für sonstige mitwirkende Personen, wenn diese sich weiterer Personen bedienen, die an der beruflichen oder dienstlichen Tätigkeit der in den Absätzen 1 und 2 Genannten mitwirken.

(4) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer unbefugt ein fremdes Geheimnis offenbart, das ihm bei der Ausübung oder bei Gelegenheit seiner Tätigkeit als mitwirkende Person oder als bei den in den Absätzen 1 und 2 genannten Personen tätiger Datenschutzbeauftragter bekannt geworden ist. Ebenso wird bestraft, wer

1. als in den Absätzen 1 und 2 genannte Person nicht dafür Sorge getragen hat, dass eine sonstige mitwirkende Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind,
2. als im Absatz 3 genannte mitwirkende Person sich einer weiteren mitwirkenden Person, die unbefugt ein fremdes, ihr bei der Ausübung oder bei Gelegenheit ihrer Tätigkeit bekannt gewordenes Geheimnis offenbart, bedient und nicht dafür Sorge getragen hat, dass diese zur Geheimhaltung verpflichtet wurde; dies gilt nicht für sonstige mitwirkende Personen, die selbst eine in den Absätzen 1 oder 2 genannte Person sind, oder
3. nach dem Tod der nach Satz 1 oder nach den Absätzen 1 oder 2 verpflichteten Person ein fremdes Geheimnis unbefugt offenbart, das er von dem Verstorbenen erfahren oder aus dessen Nachlass erlangt hat.

(5) Die Absätze 1 bis 4 sind auch anzuwenden, wenn der Täter das fremde Geheimnis nach dem Tod des Betroffenen unbefugt offenbart.

(6) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

§ 204 Verwertung fremder Geheimnisse

(1) Wer unbefugt ein fremdes Geheimnis, namentlich ein Betriebs- oder Geschäftsgeheimnis, zu dessen Geheimhaltung er nach § 203 verpflichtet ist, verwertet, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) § 203 Absatz 5 gilt entsprechend.

§ 205 Strafantrag

(1) In den Fällen des § 201 Abs. 1 und 2 und der §§ 202, 203 und 204 wird die Tat nur auf Antrag verfolgt. Dies gilt auch in den Fällen der §§ 201a, 202a, 202b und 202d, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

(2) Stirbt der Verletzte, so geht das Antragsrecht nach § 77 Abs. 2 auf die Angehörigen über; dies gilt nicht in den Fällen der §§ 202a, 202b und 202d. Gehört das Geheimnis nicht zum persönlichen Lebensbereich des Verletzten, so geht das Antragsrecht bei Straftaten nach den §§ 203 und 204 auf die Erben über. Offenbart oder verwertet der Täter in den Fällen der §§ 203 und 204 das Geheimnis nach dem Tod des Betroffenen, so gelten die Sätze 1 und 2 sinngemäß. In den Fällen des § 201a Absatz 1 Nummer 3 und Absatz 2 Satz 2 steht das Antragsrecht den in § 77 Absatz 2 bezeichneten Angehörigen zu.

§ 206 Verletzung des Post- oder Fernmeldegeheimnisses

(1) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die dem Post- oder Fernmeldegeheimnis unterliegen und die ihm als Inhaber oder Beschäftigtem eines Unternehmens bekanntgeworden sind, das geschäftsmäßig Post- oder Telekommunikationsdienste erbringt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Ebenso wird bestraft, wer als Inhaber oder Beschäftigter eines in Absatz 1 bezeichneten Unternehmens unbefugt

1. eine Sendung, die einem solchen Unternehmen zur Übermittlung anvertraut worden und verschlossen ist, öffnet oder sich von ihrem Inhalt ohne Öffnung des Verschlusses unter Anwendung technischer Mittel Kenntnis verschafft,
2. eine einem solchen Unternehmen zur Übermittlung anvertraute Sendung unterdrückt oder
3. eine der in Absatz 1 oder in Nummer 1 oder 2 bezeichneten Handlungen gestattet oder fördert.

(3) Die Absätze 1 und 2 gelten auch für Personen, die

1. Aufgaben der Aufsicht über ein in Absatz 1 bezeichnetes Unternehmen wahrnehmen,
2. von einem solchen Unternehmen oder mit dessen Ermächtigung mit dem Erbringen von Post- oder Telekommunikationsdiensten betraut sind oder
3. mit der Herstellung einer dem Betrieb eines solchen Unternehmens dienenden Anlage oder mit Arbeiten daran betraut sind.

(4) Wer unbefugt einer anderen Person eine Mitteilung über Tatsachen macht, die ihm als außerhalb des Post- oder Telekommunikationsbereichs tätigem Amtsträger auf Grund eines befugten oder unbefugten Eingriffs in das Post- oder Fernmeldegeheimnis bekanntgeworden sind, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(5) Dem Postgeheimnis unterliegen die näheren Umstände des Postverkehrs bestimmter Personen sowie der Inhalt von Postsendungen. Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob je-

mand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.

§ 263a Computerbetrug

(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflußt, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) § 263 Abs. 2 bis 6 gilt entsprechend.

(3) Wer eine Straftat nach Absatz 1 vorbereitet, indem er

1. Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überlässt oder
2. Passwörter oder sonstige Sicherungscodes, die zur Begehung einer solchen Tat geeignet sind, herstellt, sich oder einem anderen verschafft, feilhält, verwahrt oder einem anderen überlässt,

wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(4) In den Fällen des Absatzes 3 gilt § 149 Abs. 2 und 3 entsprechend.

§ 268 Fälschung technischer Aufzeichnungen

(1) Wer zur Täuschung im Rechtsverkehr

1. eine unechte technische Aufzeichnung herstellt oder eine technische Aufzeichnung verfälscht oder
2. eine unechte oder verfälschte technische Aufzeichnung gebraucht,

wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Technische Aufzeichnung ist eine Darstellung von Daten, Meß- oder Rechenwerten, Zuständen oder Geschehensabläufen, die durch ein technisches Gerät ganz oder zum Teil selbsttätig bewirkt wird, den Gegenstand der Aufzeichnung allgemein oder für Eingeweihte erkennen läßt und zum Beweis einer rechtlich erheblichen Tatsache bestimmt ist, gleichviel ob ihr die Bestimmung schon bei der Herstellung oder erst später gegeben wird.

(3) Der Herstellung einer unechten technischen Aufzeichnung steht es gleich, wenn der Täter durch störende Einwirkung auf den Aufzeichnungsvorgang das Ergebnis der Aufzeichnung beeinflußt.

(4) Der Versuch ist strafbar.

(5) § 267 Abs. 3 und 4 gilt entsprechend.

§ 269 Fälschung beweiserheblicher Daten

(1) Wer zur Täuschung im Rechtsverkehr beweiserhebliche Daten so speichert oder verändert, daß bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde,

oder derart gespeicherte oder veränderte Daten gebraucht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

(3) § 267 Abs. 3 und 4 gilt entsprechend.

§ 270 Täuschung im Rechtsverkehr bei Datenverarbeitung

Der Täuschung im Rechtsverkehr steht die fälschliche Beeinflussung einer Datenverarbeitung im Rechtsverkehr gleich.

§ 274 Urkundenunterdrückung; Veränderung einer Grenzbezeichnung

(1) Mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe wird bestraft, wer

1. eine Urkunde oder eine technische Aufzeichnung, welche ihm entweder überhaupt nicht oder nicht ausschließlich gehört, in der Absicht, einem anderen Nachteil zuzufügen, vernichtet, beschädigt oder unterdrückt,
2. beweiserhebliche Daten (§ 202a Abs. 2), über die er nicht oder nicht ausschließlich verfügen darf, in der Absicht, einem anderen Nachteil zuzufügen, löscht, unterdrückt, unbrauchbar macht oder verändert oder
3. einen Grenzstein oder ein anderes zur Bezeichnung einer Grenze oder eines Wasserstandes bestimmtes Merkmal in der Absicht, einem anderen Nachteil zuzufügen, wegnimmt, vernichtet, unkenntlich macht, verrückt oder fälschlich setzt.

(2) Der Versuch ist strafbar.

§ 303a Datenveränderung

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

(3) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

§ 303b Computersabotage

(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er

1. eine Tat nach § 303a Abs. 1 begeht,
2. Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder
3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,

wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

(3) Der Versuch ist strafbar.

(4) In besonders schweren Fällen des Absatzes 2 ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. einen Vermögensverlust großen Ausmaßes herbeiführt,
2. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat,
3. durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt.

(5) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

§ 303c Strafantrag

In den Fällen der §§ 303, 303a Abs. 1 und 2 sowie § 303b Abs. 1 bis 3 wird die Tat nur auf Antrag verfolgt, es sei denn, daß die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

§ 317 Störung von Telekommunikationsanlagen

(1) Wer den Betrieb einer öffentlichen Zwecken dienenden Telekommunikationsanlage dadurch verhindert oder gefährdet, daß er eine dem Betrieb dienende Sache zerstört, beschädigt, beseitigt, verändert oder unbrauchbar macht oder die für den Betrieb bestimmte elektrische Kraft entzieht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

(3) Wer die Tat fahrlässig begeht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

§ 353b Verletzung des Dienstgeheimnisses und einer besonderen Geheimhaltungspflicht

(1) Wer ein Geheimnis, das ihm als

1. Amtsträger,
2. für den öffentlichen Dienst besonders Verpflichteten,
3. Person, die Aufgaben oder Befugnisse nach dem Personalvertretungsrecht wahrnimmt oder
4. Europäischer Amtsträger,

anvertraut worden oder sonst bekanntgeworden ist, unbefugt offenbart und dadurch wichtige öffentliche Interessen gefährdet, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft. Hat der Täter durch die Tat fahrlässig wichtige öffentliche Interessen gefährdet, so wird er mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Wer, abgesehen von den Fällen des Absatzes 1, unbefugt einen Gegenstand oder eine Nachricht, zu deren Geheimhaltung er

1. auf Grund des Beschlusses eines Gesetzgebungsorgans des Bundes oder eines Landes oder eines seiner Ausschüsse verpflichtet ist oder
2. von einer anderen amtlichen Stelle unter Hinweis auf die Strafbarkeit der Verletzung der Geheimhaltungspflicht förmlich verpflichtet worden ist,

an einen anderen gelangen läßt oder öffentlich bekanntmacht und dadurch wichtige öffentliche Interessen gefährdet, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(3) Der Versuch ist strafbar.

(3a) Beihilfehandlungen einer in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Person sind nicht rechtswidrig, wenn sie sich auf die Entgegennahme, Auswertung oder Veröffentlichung des Geheimnisses oder des Gegenstandes oder der Nachricht, zu deren Geheimhaltung eine besondere Verpflichtung besteht, beschränken.

(4) Die Tat wird nur mit Ermächtigung verfolgt. Die Ermächtigung wird erteilt

1. von dem Präsidenten des Gesetzgebungsorgans
   a) in den Fällen des Absatzes 1, wenn dem Täter das Geheimnis während seiner Tätigkeit bei einem oder für ein Gesetzgebungsorgan des Bundes oder eines Landes bekanntgeworden ist,
   b) in den Fällen des Absatzes 2 Nr. 1;
2. von der obersten Bundesbehörde
   a) in den Fällen des Absatzes 1, wenn dem Täter das Geheimnis während seiner Tätigkeit sonst bei einer oder für eine Behörde oder bei einer anderen amtlichen Stelle des Bundes oder für eine solche Stelle bekanntgeworden ist,
   b) in den Fällen des Absatzes 2 Nr. 2, wenn der Täter von einer amtlichen Stelle des Bundes verpflichtet worden ist;
3. von der Bundesregierung in den Fällen des Absatzes 1 Satz 1 Nummer 4, wenn dem Täter das Geheimnis während seiner Tätigkeit bei einer Dienststelle der Europäischen Union bekannt geworden ist;
4. von der obersten Landesbehörde in allen übrigen Fällen der Absätze 1 und 2 Nr. 2.

In den Fällen des Satzes 2 Nummer 3 wird die Tat nur verfolgt, wenn zudem ein Strafverlangen der Dienststelle vorliegt.

§ 355 Verletzung des Steuergeheimnisses

(1) Wer unbefugt

1. personenbezogene Daten eines anderen, die ihm als Amtsträger
   a) in einem Verwaltungsverfahren, einem Rechnungsprüfungsverfahren oder einem gerichtlichen Verfahren in Steuersachen,
   b) in einem Strafverfahren wegen einer Steuerstraftat oder in einem Bußgeldverfahren wegen einer Steuerordnungswidrigkeit,

c) im Rahmen einer Weiterverarbeitung nach § 29c Absatz 1 Satz 1 Nummer 4, 5 oder 6 der Abgabenordnung oder aus anderem dienstlichen Anlass, insbesondere durch Mitteilung einer Finanzbehörde oder durch die gesetzlich vorgeschriebene Vorlage eines Steuerbescheids oder einer Bescheinigung über die bei der Besteuerung getroffenen Feststellungen

bekannt geworden sind, oder

2. ein fremdes Betriebs- oder Geschäftsgeheimnis, das ihm als Amtsträger in einem der in Nummer 1 genannten Verfahren bekannt geworden ist,

offenbart oder verwertet, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft. Personenbezogene Daten eines anderen oder fremde Betriebs- oder Geschäftsgeheimnisse sind dem Täter auch dann als Amtsträger in einem in Satz 1 Nummer 1 genannten Verfahren bekannt geworden, wenn sie sich aus Daten ergeben, zu denen er Zugang hatte und die er unbefugt abgerufen hat. Informationen, die sich auf identifizierte oder identifizierbare verstorbene natürliche Personen oder Körperschaften, rechtsfähige oder nicht rechtsfähige Personenvereinigungen oder Vermögensmassen beziehen, stehen personenbezogenen Daten eines anderen gleich.

(2) Den Amtsträgern im Sinne des Absatzes 1 stehen gleich

1. die für den öffentlichen Dienst besonders Verpflichteten,
2. amtlich zugezogene Sachverständige und
3. die Träger von Ämtern der Kirchen und anderen Religionsgesellschaften des öffentlichen Rechts.

(3) Die Tat wird nur auf Antrag des Dienstvorgesetzten oder des Verletzten verfolgt. Bei Taten amtlich zugezogener Sachverständiger ist der Leiter der Behörde, deren Verfahren betroffen ist, neben dem Verletzten antragsberechtigt.