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)

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 114,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses ([1]),

nach Stellungnahme des Ausschusses der Regionen ([2]),

gemäß dem ordentlichen Gesetzgebungsverfahren ([3]),

in Erwägung nachstehender Gründe:

(1) Netz- und Informationssysteme sowie elektronische Kommunikationsnetze und -dienste spielen eine lebenswichtige Rolle in der Gesellschaft und sind mittlerweile zum Hauptmotor des Wirtschaftswachstums geworden. Die Informations- und Kommunikationstechnologien (IKT) bilden das Rückgrat der komplexen Systeme, die alltägliche gesellschaftliche Tätigkeiten unterstützen und unsere Volkswirtschaften in Schlüsselsektoren wie Gesundheit, Energie, Finanzen und Verkehr aufrechterhalten und die insbesondere dafür sorgen, dass der Binnenmarkt reibungslos funktioniert.

(2) Die Nutzung von Netz- und Informationssystemen durch Bürger, Organisationen und Unternehmen ist mittlerweile in der Union allgegenwärtig. Digitalisierung und Konnektivität entwickeln sich zu Kernmerkmalen einer ständig steigenden Zahl von Produkten und Dienstleistungen; mit dem Aufkommen des Internets der Dinge dürften in den nächsten Jahrzehnten eine extrem hohe Zahl vernetzte digitale Geräte unionsweit Verbreitung finden. Zwar sind immer mehr Geräte mit dem Internet vernetzt, doch verfügen sie über eine nur unzureichende Cybersicherheit, da die Sicherheit und Abwehrfähigkeit dieser Geräte schon bei der Konzeption nicht ausreichend berücksichtigt wurden. In diesem Zusammenhang führt das geringe Maß an Zertifizierung dazu, dass Personen, Organisationen und Unternehmen die IKT-Produkte, -Dienste und -prozesse nutzen, nur unzureichend über deren Cybersicherheitsmerkmale informiert werden, wodurch das Vertrauen in digitale Lösungen untergraben wird. Netz- und Informationssysteme können uns das Leben in jeder Hinsicht erleichtern und das Wirtschaftswachstum der Union anzukurbeln. Sie spielen eine tragende Rolle bei der Verwirklichung des digitalen Binnenmarkts.

(3) Mit der zunehmenden Digitalisierung und Vernetzung steigen auch die Cybersicherheitsrisiken, wodurch die Gesellschaft insgesamt anfälliger für Cyberbedrohungen wird und die Gefahren zunehmen, denen Privatpersonen und insbesondere schutzbedürftige Personen wie Kinder ausgesetzt sind. Um diesen Gefahren zu begegnen, gilt es, alle für die Erhöhung der Cybersicherheit in der Union notwendigen Maßnahmen zu ergreifen, damit die Netz- und Informationssysteme, die Kommunikationsnetze und die digitalen Produkte, Dienste und Geräte, die von Bürgern, Organisationen und Unternehmen — von kleinen und mittleren Unternehmen (KMU) im Sinne der Empfehlung 2003/361/EG der Kommission ([4]) bis zu Betreibern kritischer Infrastrukturen — genutzt werden, besser vor Cyberbedrohungen geschützt sind.

([1]) ABl. C 227 vom 28.6.2018, S. 86.
([2]) ABl. C 176 vom 23.5.2018, S. 29.
([3]) Stellungnahme des Europäischen Parlaments vom 12. März 2019 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates vom 9. April 2019.
([4]) Empfehlung 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).

(4) Durch das Zurverfügungstellung einschlägiger Informationen für die Öffentlichkeit trägt die mit der Verordnung (EU) Nr. 526/2013 des Europäischen Parlaments und des Rates ([5]) errichtete Agentur der Europäischen Union für Netz- und Informationssicherheit (im Folgenden „ENISA") zur Entwicklung der Cybersicherheitsbranche in der Union, insbesondere von KMU und Start-ups, bei. Die ENISA sollte sich um eine engere Zusammenarbeit mit Universitäten und Forschungseinrichtungen bemühen, um einen Beitrag zur Verringerung der Abhängigkeit von Cybersicherheitsprodukten und -diensten von außerhalb der Union zu leisten und die Lieferketten innerhalb der Union zu stärken.

(5) Cyberangriffe nehmen zu und eine Wirtschaft und Gesellschaft, die durch ihre Vernetzung anfälliger für Cyberbedrohungen und -angriffe ist, benötigt daher einen stärkeren Schutz. Obwohl jedoch die Cyberangriffe häufig grenzüberschreitend sind, sind die Zuständigkeiten und Reaktionen der für die Cybersicherheit und für die Strafverfolgung zuständigen Behörden vor allem national. Sicherheitsvorfälle großen Ausmaßes könnten die Bereitstellung wesentlicher Dienste in der gesamten Union empfindlich stören. Notwendig sind daher effektive und koordinierte Maßnahmen sowie ein Krisenmanagement auf Unionsebene, gestützt auf gezielte Strategien, sowie ein breiter angelegtes Instrumentarium für europäische Solidarität und gegenseitige Hilfe. Zudem sind daher eine auf zuverlässigen Daten der Union basierende regelmäßige Überprüfung des Stands der Cybersicherheit und der Abwehrfähigkeit in der Union sowie eine systematische Prognose künftiger Entwicklungen, Herausforderungen und Bedrohungen — auf Unionsebene und auf globaler Ebene — für die Entscheidungsträger, die Branche und die Nutzer gleichermaßen wichtig.

(6) Angesichts immer größerer Herausforderungen, die sich der Union im Bereich der Cybersicherheit stellen, bedarf es eines umfassenden Maßnahmenpakets, das auf den bisherigen Maßnahmen der Union aufbauen und sich wechselseitig verstärkende Ziele unterstützen würde. Diese Ziele beinhalten eine weitere Stärkung der Fähigkeiten und der Abwehrbereitschaft der Mitgliedstaaten und Unternehmen sowie eine bessere Zusammenarbeit, einen besseren Informationsaustausch und Koordinierung zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der Union. Da Cyberbedrohungen an keinen Grenzen Halt machen, gilt es zudem, die Fähigkeiten auf Unionsebene zu stärken, die Maßnahmen der Mitgliedstaaten vor allem dann ergänzen könnten, wenn es zu grenzüberschreitenden Sicherheitsvorfällen und -krisen von großem Ausmaß kommt, unter Berücksichtigung der Bedeutung der Bewahrung und Verbesserung der nationalen Fähigkeiten zur Reaktion auf Cyberbedrohungen jeglichen Umfangs.

(7) Darüber hinaus sind weitere Anstrengungen notwendig, um die Bürger, Organisationen und Unternehmen für Fragen der Cybersicherheit zu sensibilisieren. Da Sicherheitsvorfälle das Vertrauen in Anbieter digitaler Dienste und in den digitalen Binnenmarkt als solchen insbesondere unter den Verbrauchern untergraben, sollte dieses Vertrauen dadurch gestärkt werden, dass auf transparente Art und Weise Informationen über das Niveau der Sicherheit von IKT-Produkten, -Diensten und -Prozessen bereitgestellt werden, wobei betont wird, dass auch eine Cybersicherheitszertifizierung auf hohem Niveau nicht garantieren kann, dass ein IKT-Produkt, -Dienst oder -Prozess völlig sicher ist. Eine Stärkung des Vertrauens kann durch eine unionsweite Zertifizierung erleichtert werden, für die über nationale Märkte und Sektoren hinaus unionsweit einheitliche Anforderungen und Bewertungskriterien für die Cybersicherheit festgelegt werden.

(8) Cybersicherheit ist nicht nur eine Frage der Technologie, sondern eine, bei der das menschliche Verhalten ebenso wichtig ist. Daher sollte die „Cyberhygiene", also einfache Routinemaßnahmen, durch die, wenn sie von Bürgern, Organisationen und Unternehmen regelmäßig umgesetzt und durchgeführt werden, die Risiken von Cyberbedrohungen so gering wie möglich gehalten werden, nachdrücklich gefördert werden.

(9) Um die Cybersicherheitsstrukturen der Union zu stärken, müssen die Fähigkeiten der Mitgliedstaaten, umfassend auf Cyberbedrohungen — einschließlich grenzüberschreitender Sicherheitsvorfälle — zu reagieren, erhalten und ausgebaut werden.

(10) Die Unternehmen und die einzelnen Verbraucher sollten über präzise Informationen darüber verfügen, auf welcher Vertrauenswürdigkeitsstufe die Sicherheit ihrer IKT-Produkte, -Dienste und -Prozesse zertifiziert wurde. Allerdings bietet kein IKT-Produkt oder -dienst hundertprozentige Cybersicherheit weshalb grundlegenden Prinzipien der Cyberhygiene verbreitet werden sollten und ihnen Vorrang eingeräumt werden sollte. Angesichts der zunehmenden Verbreitung von Geräten des Internets der Dinge kann die Privatwirtschaft zahlreiche freiwillige Maßnahmen treffen, um das Vertrauen in die Sicherheit von IKT-Produkten, -Diensten und -Prozessen zu stärken.

(11) Moderne IKT-Produkte und -Systeme weisen oft einen oder mehrere von Dritten entwickelte Technologien und Bestandteile wie Software-Module, Bibliotheken oder Programmierschnittstellen auf und sind von diesen abhängig. Diese „Abhängigkeit" könnte zusätzliche Risiken im Bereich der Cybersicherheit bergen, da sich Sicherheitslücken in Bestandteilen Dritter auch auf die Sicherheit von IKT-Produkten, -Diensten, und -Prozessen auswirken könnten. In vielen Fällen ermöglicht die Aufdeckung und Dokumentierung solcher „Abhängigkeiten" den Endnutzern von IKT-Produkten, -Diensten und -Prozessen die Verbesserung ihres Risikomanagements im Bereich der Cybersicherheit, indem beispielsweise die Behandlung von Sicherheitslücken im Bereich der Cybersicherheit durch die Nutzer und deren Abhilfeverfahren verbessert werden.

([5]) Verordnung (EU) Nr. 526/2013 des Europäischen Parlaments und des Rates vom 21. Mai 2013 über die Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA) und zur Aufhebung der Verordnung (EG) Nr. 460/2004 (ABl. L 165 vom 18.6.2013, S. 41).

(12) Organisationen, Hersteller oder Diensteanbieter, die an der Konzeption und Entwicklung von IKT-Produkten, -Diensten und -Prozessen beteiligt sind, sollten dazu angehalten werden, in den ersten Phasen der Konzeption und Entwicklung Maßnahmen durchzuführen, um die Sicherheit dieser Produkte, Dienste und Prozesse möglichst weitgehend zu schützen, in dem sie davon ausgehen, dass Cyberangriffe vorliegen, und deren Folgen vorwegzunehmen und so gering wie möglich zu halten (konzeptionsintegrierte Sicherheit — security by design). Die Sicherheit sollte während der gesamten Lebensdauer des IKT-Produkts, -Dienstes oder -Prozesses berücksichtigt werden, wobei die Konzeptions- und Entwicklungsprozesse ständig weiterentwickelt werden sollten, um das Risiko von Schäden durch eine böswillige Nutzung zu verringern.

(13) Unternehmen, Organisationen und der öffentliche Sektor sollten die von ihnen konzipierten IKT-Produkte, -Dienste oder -Prozesse so konfigurieren, dass ein höheres Maß an Sicherheit gewährleistet ist, das es dem ersten Nutzer ermöglicht, eine Standardkonfiguration mit den sichersten möglichen Einstellungen („security by default“) zu erhalten; somit wären die Nutzer in geringerem Maße der Belastung ausgesetzt, ein IKT-Produkt, -einen IKT-Dienst oder einen IKT-Prozess angemessen konfigurieren zu müssen. Die Sicherheit durch Voreinstellungen („security by default“) sollte weder eine umfangreiche Konfiguration erfordern, noch spezifische technische Kenntnisse oder ein nicht offensichtliches Verhalten seitens des Nutzers, und sie sollte dort, wo sie implementiert wurde, einfach und zuverlässig funktionieren. Wenn im Einzelfall eine Risiko- und Nutzbarkeitsanalyse zu dem Ergebnis führt, dass eine solche vordefinierte Einstellung nicht machbar ist, sollten die Nutzer aufgefordert werden, die sicherste Einstellung zu wählen.

(14) Mit der Verordnung (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates ([6]) wurde die ENISA als Beitrag zu den Zielen errichtet, innerhalb der Union eine hohe und effektive Netz- und Informationssicherheit zu gewährleisten und eine Kultur der Netz- und Informationssicherheit zu entwickeln, die Bürgern, Verbrauchern, Unternehmen und öffentlicher Verwaltung zugute kommt. Mit der Verordnung (EG) Nr. 1007/2008 des Europäischen Parlaments und des Rates ([7]) wurde das Mandat der ENISA bis März 2012 verlängert. Durch die Verordnung (EU) Nr. 580/2011 des Europäischen Parlaments und des Rates ([8]) wurde das Mandat der ENISA nochmals bis zum 13. September 2013 verlängert. Mit der Verordnung (EU) Nr. 526/2013 des Europäischen Parlaments und des Rates wurde das Mandat der ENISA bis zum 19. Juni 2020 verlängert.

(15) Die Union hat bereits wichtige Maßnahmen ergriffen, um die Cybersicherheit zu gewährleisten und das Vertrauen in die digitale Technik zu stärken. Im Jahr 2013 wurde die EU-Cybersicherheitsstrategie der Europäischen Union verabschiedet, die der Union als Orientierung für strategische Reaktionen auf Cybersicherheitsbedrohungen und -risiken dient. Im Zuge ihrer Bemühung, den Online-Schutz der Bürger zu verbessern, hat die Union im Jahr 2016 mit der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates ([9]) den ersten Rechtsakt auf dem Gebiet der Cybersicherheit erlassen. Mit der Richtlinie (EU) 2016/1148 wurden Anforderungen an die nationalen Fähigkeiten im Bereich der Cybersicherheit sowie erstmals Mechanismen zur Stärkung der strategischen und operativen Zusammenarbeit zwischen den Mitgliedstaaten festgelegt und ferner Verpflichtungen in Bezug auf die Sicherheitsmaßnahmen und die Meldung von Sicherheitsvorfällen für die Sektoren, die für die Wirtschaft und Gesellschaft lebenswichtig sind, wie Energie, Verkehr, Trinkwasserlieferung und -versorgung, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, digitale Infrastruktur sowie für Anbieter zentraler digitaler Dienste (Suchmaschinen, Cloud-Computing-Dienste und Online-Marktplätze) eingeführt.

Eine zentrale Aufgabe bei der Umsetzung dieser Richtlinie wurde dabei der ENISA zugewiesen. Darüber hinaus ist die wirksame Bekämpfung der Cyberkriminalität als ein Aspekt bei der Verfolgung des übergeordneten Ziels einer hohen Cybersicherheit ein wichtiger Schwerpunkt der Europäischen Sicherheitsagenda. Andere Rechtsakte wie die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([10]) und die Richtlinie 2002/58/EG ([11]) sowie die Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates ([12]) tragen auch zu einem hohen Maß an Cybersicherheit im digitalen Binnenmarkt bei.

([6]) Verordnung (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit (ABl. L 77 vom 13.3.2004, S. 1).

([7]) Verordnung (EG) Nr. 1007/2008 des Europäischen Parlaments und des Rates vom 24. September 2008 zur Änderung der Verordnung (EG) Nr. 460/2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit bezüglich deren Bestehensdauer (ABl. L 293 vom 31.10.2008, S. 1).

([8]) Verordnung (EU) Nr. 580/2011 des Europäischen Parlaments und des Rates vom 8. Juni 2011 zur Änderung der Verordnung (EG) Nr. 460/2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit bezüglich deren Bestehensdauer (ABl. L 165 vom 24.6.2011, S. 3).

([9]) 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).

([10]) 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).

([11]) 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).

([12]) Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) (ABl. L 321 vom 17.12.2018, S. 36).

(16) Seit der Verabschiedung der Cybersicherheitsstrategie der Europäischen Union im Jahr 2013 und der letzten Überarbeitung des Mandats der ENISA hat sich der gesamtpolitische Rahmen deutlich verändert, da das globale Umfeld nun von größeren Unwägbarkeiten und geringerer Sicherheit geprägt ist. Vor diesem Hintergrund und im Kontext der positiven Entwicklung der Rolle der ENISA als ein Bezugspunkt für Beratung und Sachkenntnis und als Vermittlerin in Bezug auf Zusammenarbeit und den Aufbau von Fähigkeiten sowie angesichts der neuen Unionspolitik im Bereich der Cybersicherheit muss das Mandat der ENISA im Hinblick auf ihre neue Rolle im veränderten Cybersicherheitsökosystem überarbeitet werden, damit sie die Union wirksam dabei unterstützen kann, auf die Herausforderungen im Bereich der Cybersicherheit zu reagieren, die sich aus der grundlegend veränderten Cyberbedrohungslandschaft ergeben und für die — wie in der Bewertung der ENISA bestätigt — das laufende Mandat nicht ausreicht.

(17) Die mit dieser Verordnung errichtete ENISA sollte Rechtsnachfolgerin der durch die Verordnung (EU) Nr. 526/2013 errichteten ENISA sein. Die ENISA sollte die Aufgaben wahrnehmen, die ihr mit dieser Verordnung und anderen Rechtsakten der Union im Bereich der Cybersicherheit übertragen werden, indem sie unter anderem Beratung bietet und Sachkenntnis bereitstellt indem sie die Rolle eines Informations- und Wissenszentrums der Union übernimmt. Sie sollte den Austausch bewährter Verfahren zwischen den Mitgliedstaaten und privaten Interessenträgern fördern, der Kommission und den Mitgliedstaaten strategische Vorschläge unterbreiten, als Bezugspunkt für sektorspezifische politische Initiativen der Union im Bereich der Cybersicherheit dienen und die operative Zusammenarbeit sowohl zwischen den Mitgliedstaaten als auch zwischen den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der Union fördern.

(18) Mit dem Einvernehmlichen Beschluss 2004/97/EG, Euratom der auf Ebene der Staats- und Regierungschefs vereinigten Vertreter der Mitgliedstaaten ([13]), legten die Vertreter der Mitgliedstaaten fest, dass die ENISA ihren Sitz in Griechenland in einer von der griechischen Regierung zu benennenden Stadt haben soll. Der Sitzmitgliedstaat der ENISA sollte die bestmöglichen Voraussetzungen für eine reibungslose und effiziente Tätigkeit der ENISA gewährleisten. Damit die ENISA ihre Aufgaben ordnungsgemäß und effizient erfüllen, Personal einstellen und binden und die Effizienz der Vernetzungsmaßnahmen steigern kann, ist es unbedingt erforderlich, sie an einem geeigneten Standort anzusiedeln, der unter anderem eine angemessene Verkehrsanbindung sowie Einrichtungen für die Ehepartner und Kinder des Personals der ENISA bietet. Die erforderlichen Modalitäten sollten in einem Abkommen zwischen der ENISA und dem Sitzmitgliedstaat festgelegt werden, das nach Billigung durch den Verwaltungsrat der ENISA geschlossen wird.

(19) Angesichts der zunehmenden Bedrohungen und Herausforderungen, mit denen die Union im Bereich der Cybersicherheit konfrontiert ist, sollten die Mittelzuweisungen für die ENISA erhöht werden, damit ihre finanzielle und personelle Ausstattung ihrer größeren Rolle und ihren umfangreicheren Aufgaben sowie ihrer wichtigen Stellung im Ökosystem der Organisationen gerecht werden kann, die das digitale Ökosystem der Union verteidigen, sodass die ENISA die ihr mit dieser Verordnung übertragenen Aufgaben wirksam erfüllen kann.

(20) Die ENISA sollte ein hohes Niveau an Sachkenntnis entwickeln und pflegen und als Bezugspunkt fungieren, wobei sie durch ihre Unabhängigkeit, die Qualität ihrer Beratung und der von ihr verbreiteten Informationen, die Transparenz ihrer Verfahren, die Transparenz ihrer Arbeitsmethoden sowie die Sorgfalt, mit der sie ihre Aufgaben erfüllt, Vertrauen in den Binnenmarkt schafft. Die ENISA sollte die Bemühungen der Mitgliedstaaten aktiv unterstützen und vorausgreifend zu den Bemühungen der Union beitragen und ihre Aufgaben in uneingeschränkter Zusammenarbeit mit den Organen, Einrichtungen und sonstigen Stellen der Union und den Mitgliedstaaten wahrnehmen, wobei Doppelarbeiten vermieden und Synergien gefördert werden sollten. Außerdem sollte sich die ENISA auf die Beiträge des Privatsektors und anderer einschlägiger Interessenträger sowie auf die Zusammenarbeit mit ihnen stützen. Mit einer Reihe von Aufgaben sollte bei gleichzeitiger Wahrung der Flexibilität in ihrer Tätigkeit vorgegeben werden, wie die ENISA ihre Ziele erreichen soll.

(21) Damit sie die operative Zusammenarbeit zwischen den Mitgliedstaaten angemessen unterstützen kann, sollte die ENISA ihre technischen und menschlichen Fähigkeiten und Fertigkeiten weiter ausbauen. Die ENISA sollte ihr Know-how und ihre Fähigkeiten vergrößern. Die ENISA und die Mitgliedstaaten könnten auf freiwilliger Basis Programme für die Entsendung von nationalen Sachverständigen an die ENISA, die Bildung von Pools von Sachverständigen und den Austausch von Personal entwickeln.

(22) Die ENISA sollte die Kommission mit Beratung, Stellungnahmen und Analysen zu allen Angelegenheiten der Union, die mit der Ausarbeitung, Aktualisierung und Überprüfung von Strategien und Rechtsvorschriften im Bereich der Cybersicherheit und den diesbezüglichen sektorenspezifischen Aspekten zusammenhängen, unterstützen, damit die Strategien und Rechtsvorschriften der Union mit einer Cybersicherheitsdimension zweckdienlicher gestaltet werden und die kohärente Umsetzung dieser Strategien und Rechtsvorschriften auf nationaler Ebene ermöglicht wird. Für sektorspezifische Strategien und Rechtsetzungsinitiativen der Union im Zusammenhang mit der Cybersicherheit sollte die ENISA als Bezugspunkt für Beratung und Sachkenntnis dienen. Die ENISA sollte dem Europäischen Parlament regelmäßig über ihre Tätigkeiten Bericht erstatten.

([13]) Einvernehmlicher Beschluss 2004/97/EG, Euratom der auf Ebene der Staats- und Regierungschefs vereinigten Vertreter der Mitgliedstaaten vom 13. Dezember 2003 über die Festlegung der Sitze bestimmter Ämter, Behörden und Agenturen der Europäischen Union (ABl. L 29 vom 3.2.2004, S. 15).

(23) Der öffentliche Kern des offenen Internets, d. h. seine wichtigsten Protokolle und Infrastrukturen, die ein globales öffentliches Gut sind, stellt die wesentlichen Funktionen des Internets als Ganzes bereit und bildet die Grundlage für dessen normalen Betrieb. Die ENISA sollte die Sicherheit und Stabilität dieses öffentlichen Kerns des offenen Internets unterstützen, unter anderem — aber nicht beschränkt auf — die wichtigsten Protokolle (insbesondere DNS, BGP und IPv6), den Betrieb des „Domain Name System" (DNS) (wie den Betrieb aller Domänen der obersten Ebene) und den Betrieb der Root-Zone.

(24) Die ENISA hat grundsätzlich die Aufgabe, die einheitliche Umsetzung des einschlägigen Rechtsrahmens, vor allem die wirksame Umsetzung der Richtlinie (EU) 2016/1148 und anderer maßgeblicher Rechtsakte zu Aspekten der Cybersicherheit, zu unterstützen, was für die Stärkung der Abwehrfähigkeit gegen Cyberangriffe unerlässlich ist. Angesichts der sich rasch weiterentwickelnden Bedrohungen für die Cybersicherheit ist klar, dass die Mitgliedstaaten beim Aufbau der Abwehrfähigkeit gegen Cyberangriffe durch ein umfassenderes und ressortübergreifendes Konzept unterstützt werden müssen.

(25) Die ENISA sollte die Mitgliedstaaten und die Organe, Einrichtungen und sonstigen Stellen der Union in ihrem Bemühen um den Auf- und Ausbau der Fähigkeiten und der Bereitschaft zur Verhütung, Erkennung und Bewältigung von Cyberbedrohungen und von Sicherheitsvorfällen im Zusammenhang mit der Netz- und Informationssicherheit unterstützen. So sollte die ENISA den Auf- und Ausbau der in der Richtlinie (EU) 2016/1148 vorgesehenen Reaktionsteams für Computersicherheitsverletzungen (im Folgenden „CSIRTs") der Mitgliedstaaten und der Union unterstützen, damit sie ein unionsweit hohes Maß an Ausgereiftheit erreichen. Die Tätigkeiten der ENISA im Zusammenhang mit den operativen Kapazitäten der Mitgliedstaaten sollten die Maßnahmen der Mitgliedstaaten zur Erfüllung ihrer Verpflichtungen aus der Richtlinie (EU) 2016/1148 aktiv unterstützen und diese daher nicht ersetzen.

(26) Zudem sollte die ENISA auf Ersuchen die Ausarbeitung und Aktualisierung von Strategien im Bereich der Netz- und Informationssysteme auf Unionsebene und, auf Anfrage, auf Ebene der Mitgliedstaaten, insbesondere der Cybersicherheit, unterstützen und sollte die Verbreitung solcher Strategien fördern und die Fortschritte bei deren Umsetzung verfolgen. Die ENISA sollte auch dazu beitragen, den Bedarf an Ausbildungsmaßnahmen und Ausbildungsmaterial, auch in Bezug auf öffentliche Stellen, zu decken, und gegebenenfalls in großem Umfang auf der Grundlage des Referenzrahmens für digitale Kompetenzen der Bürger Ausbilder weiterbilden, um die Mitgliedstaaten und die Organe, Einrichtungen und sonstigen Stellen der Union darin zu unterstützen, eigene Ausbildungskapazitäten aufzubauen.

(27) Die ENISA sollte die Mitgliedstaaten im Bereich der Sensibilisierung und Ausbildung in Bezug auf die Cybersicherheit unterstützen, indem sie eine engere Koordinierung und den Austausch von bewährten Verfahren zwischen den Mitgliedstaaten fördert. Diese Unterstützung könnte darin bestehen, dass sie ein Netz von nationalen Bildungskontaktstellen und eine Ausbildungsplattform zur Cybersicherheit entwickelt. Das Netz der nationalen Bildungskontaktstellen könnte im Rahmen des Netzes der nationalen Verbindungsbeamten betrieben werden und einen Ausgangspunkt für die zukünftige Koordinierung innerhalb der Mitgliedstaaten bilden.

(28) Die ENISA sollte die durch die Richtlinie (EU) 2016/1148 eingesetzte Kooperationsgruppe bei der Wahrnehmung ihrer Aufgaben unterstützen, indem sie vor allem ihre Sachkenntnis und Beratung zur Verfügung stellt und den Austausch bewährter Verfahren erleichtert, unter anderem was die Ermittlung von Betreibern wesentlicher Dienste durch die Mitgliedstaaten in Bezug auf Risiken und Sicherheitsvorfälle anbelangt, auch mit Blick auf grenzüberschreitende Abhängigkeiten.

(29) Die ENISA sollte als Anreiz für die Zusammenarbeit zwischen dem öffentlichen und privaten Sektor, vor allem als Beitrag zum Schutz kritischer Infrastrukturen, den Informationsaustausch in und zwischen Sektoren, vor allem in den in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren, unterstützen, indem sie bewährte Verfahren und Leitfäden zu den verfügbaren Instrumenten und Verfahren bereitstellt und aufzeigt, wie regulatorische Fragen im Zusammenhang mit der Informationsweitergabe geklärt werden können, wobei dies beispielsweise durch die Erleichterung des Aufbaus sektorbezogener Informationsaustausch- und -analysezentren (Information Sharing and Analysis Centres) erreicht werden soll.

(30) In Anbetracht der Tatsache, dass die möglichen negativen Auswirkungen von Sicherheitslücken bei IKT-Produkten, -Diensten und -Prozessen stetig zunehmen, spielen die Aufdeckung und die Behebung solcher Sicherheitslücken eine wichtige Rolle bei der Verringerung der Gesamtrisiken im Bereich der Cybersicherheit. Es hat sich gezeigt, dass die Zusammenarbeit zwischen Organisationen, Herstellern oder Anbietern besonders gefährdeter IKT-Produkte, -Dienste oder -Prozesse sowie Mitgliedern der Forschungsgemeinschaft im Bereich der Cybersicherheit und Regierungen, die diese Sicherheitslücken aufspüren, sowohl die Aufdeckung als auch die Behebung von Sicherheitslücken bei IKT-Produkten, -Diensten oder -Prozessen erheblich verbessert. Die koordinierte Offenlegung von Sicherheitslücken erfolgt in einem strukturierten Prozess der Zusammenarbeit, in dem Sicherheitslücken dem Eigentümer des Informationssystems gemeldet werden, wodurch die Organisation Gelegenheit zur Diagnose und Behebung der Sicherheitslücke erhält, bevor detaillierte Informationen über die Sicherheitslücke an Dritte oder die Öffentlichkeit weitergegeben werden. Das Verfahren sieht ferner eine Koordinierung zwischen demjenigen, der die Sicherheitslücke aufgespürt hat, und der Organisation im Hinblick auf die Veröffentlichung jener Sicherheitslücke vor. Grundsätze für die koordinierte Offenlegung von Sicherheitslücken könnten eine wichtige Rolle bei den Bemühungen der Mitgliedstaaten um die Verbesserung der Cybersicherheit spielen.

(31) Die ENISA sollte die freiwillig bereitgestellten nationalen Berichte der CSIRTs und des interinstitutionellen IT-Notfallteams für die Organe, Einrichtungen und sonstigen Stellen der Union („CERT-EU"), welche mit der zwischen dem Europäischen Parlament, dem Europäischen Rat, dem Rat der Europäischen Union, der Europäischen Kommission, dem Gerichtshof der Europäischen Union, der Europäischen Zentralbank, dem Europäischen Rechnungshof, dem Europäischen Auswärtigen Dienst, dem Europäischen Wirtschafts- und Sozialausschuss, dem Europäischen Ausschuss der Regionen und der Europäischen Investitionsbank geschlossenen Vereinbarung über die Organisation und die Funktionsweise eines IT-Notfallteams für die Organe, Einrichtungen und sonstigen Stellen der Union (CERT-EU) ([14]) errichtet wurde, zusammenstellen und auswerten, um einen Beitrag zur Aufstellung gemeinsamer Verfahren für den Informationsaustausch, zur Festlegung der Sprache und zu terminologischen Vereinbarungen zu leisten. In diesem Zusammenhang sollte die ENISA im Rahmen der Richtlinie (EU) 2016/1148, die die Grundlage für den freiwilligen Austausch technischer Informationen auf operativer Ebene innerhalb des Netzwerks von Computer-Notfallteams (im Folgenden „CSIRTs-Netz") gemäß der genannten Richtlinie geschaffen hat, auch den Privatsektor einbeziehen.

(32) Die ENISA sollte dazu beitragen, dass bei massiven grenzüberschreitenden Vorfällen und -krisen in Bezug auf Cybersicherheit eine Reaktion auf Unionsebene erfolgt. Diese Aufgabe sollte ENISA entsprechend ihrem Mandat gemäß dieser Verordnung und einem Ansatz ausführen, der von den Mitgliedstaaten im Zusammenhang mit der Empfehlung (EU) 2017/1584 ([15]) der Kommission und den Schlussfolgerungen des Rates vom 26. Juni 2018 zu einer koordinierten Reaktion auf große Cybersicherheitsvorfälle und -krisen festzulegen ist. Zu dieser Aufgabe könnte auch gehören, dass sie relevante Informationen zusammenstellt und den Kontakt zwischen dem CSIRTs-Netz und den Fachkreisen sowie den für das Krisenmanagement zuständigen Entscheidungsträgern erleichtert. Zudem sollte die ENISA die operative Zusammenarbeit zwischen den Mitgliedstaaten auf Ersuchen eines oder mehrerer Mitgliedstaaten unterstützen, indem sie die Bewältigung der Sicherheitsvorfälle aus technischer Sicht übernimmt, indem sie den Austausch entsprechender technischer Lösungen zwischen den Mitgliedstaaten erleichtert und Beiträge für die Öffentlichkeitsarbeit liefert. Die ENISA sollte die operative Zusammenarbeit unterstützen, indem sie die Modalitäten einer solchen Zusammenarbeit im Rahmen regelmäßig stattfindender Cybersicherheitsübungen testet.

(33) Zur Unterstützung der operativen Zusammenarbeit sollte die ENISA im Wege einer strukturierten Zusammenarbeit auf den bei der CERT-EU vorhandenen technischen und operativen Sachverstand zurückgreifen. Eine solche strukturierte Zusammenarbeit könnte auf der Sachkenntnis der ENISA aufbauen. Für die Festlegung der praktischen Aspekte einer solchen Kooperation und zur Vermeidung von Doppelarbeit sollten gegebenenfalls zwischen den beiden Stellen die hierfür notwendigen Modalitäten festgelegt werden.

(34) Entsprechend ihrer Aufgabe, die operative Zusammenarbeit im Rahmen des CSIRTs-Netzes zu unterstützen, sollte die ENISA in der Lage sein, die Mitgliedstaaten auf deren Ersuchen hin zu unterstützen, indem sie diese beispielsweise berät, wie sie ihre Fähigkeiten zur Verhütung, Erkennung und Bewältigung von Sicherheitsvorfällen verbessern können, die technische Bewältigung von Sicherheitsvorfällen mit beträchtlichen oder erheblichen Auswirkungen erleichtert oder sicherstellt, dass Cyberbedrohungen und Sicherheitsvorfälle analysiert werden. Die ENISA sollte die technische Bewältigung von Sicherheitsvorfällen mit beträchtlichen oder erheblichen Auswirkungen insbesondere dadurch erleichtern, dass sie den freiwilligen Austausch technischer Lösungen zwischen den Mitgliedstaaten unterstützt oder kombinierte technische Informationen — etwa über technische Lösungen, die von den Mitgliedstaaten freiwillig bereitgestellt werden — erstellt. Der Empfehlung (EU) 2017/1584 zufolge sollten die Mitgliedstaaten in gutem Glauben untereinander sowie mit der ENISA Informationen über massive Vorfälle und -krisen in Bezug auf Cybersicherheit unverzüglich austauschen. Diese Informationen würden zudem der ENISA helfen, ihre Aufgabe wahrzunehmen, die operative Zusammenarbeit zu unterstützen.

(35) Als Teil der regulären Zusammenarbeit auf technischer Ebene zur Unterstützung der EU-Lageeinschätzung sollte die ENISA auf der Grundlage öffentlich verfügbarer Informationen, ihrer eigenen Analysen und anhand von Berichten, die sie von den CSIRTs der Mitgliedstaaten oder den nationalen Anlaufstellen für die Sicherheit von Netz- und Informationssystemen gemäß der Richtlinie (EU) 2016/1148, in beiden Fällen auf freiwilliger Basis, dem Europäischen Zentrum zur Bekämpfung der Cyberkriminalität (EC3) bei Europol und dem CERT-EU sowie gegebenenfalls dem EU-Zentrum für Informationsgewinnung und -analyse (EU INTCEN) des Europäischen Auswärtigen Dienstes erhalten hat, regelmäßig und in enger Zusammenarbeit mit den Mitgliedstaaten eingehende EU-Cybersicherheitslageberichte über Sicherheitsvorfälle und Bedrohungen erstellen. Dieser Bericht sollte dem Rat, der Kommission, der Hohen Vertreterin der Union für die Gemeinsame Außen- und Sicherheitspolitik und dem CSIRTs-Netz zur Verfügung gestellt werden.

(36) Die ENISA sollte sich bei der Unterstützung von nachträglichen technischen Untersuchungen von Sicherheitsvorfällen mit beträchtlichen oder erheblichen Auswirkungen, die sie auf Ersuchen der betreffenden Mitgliedstaaten leistet, auf die Verhütung künftiger Sicherheitsvorfälle konzentrieren. Die betreffenden Mitgliedstaaten sollten die notwendigen Informationen und die erforderliche Hilfe bereitstellen, damit die ENISA die nachträgliche technische Untersuchung wirksam unterstützen kann.

([14]) ABl. C 12 vom 13.1.2018, S. 1.

([15]) Empfehlung (EU) 2017/1584 der Kommission vom 13. September 2017 für eine koordinierte Reaktion auf große Cybersicherheitsvorfälle und -krisen (ABl. L 239 vom 19.9.2017, S. 36).

(37) Die Mitgliedstaaten können die von dem Sicherheitsvorfall betroffenen Unternehmen auffordern, mit der ENISA zusammenzuarbeiten und dieser — unbeschadet ihres Rechts, sensible Geschäftsinformationen und Informationen, die für die öffentliche Sicherheit von Bedeutung sind, zu schützen — die notwendigen Informationen und Hilfen zur Verfügung stellen.

(38) Um die Herausforderungen im Bereich der Cybersicherheit besser verstehen und den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der Union langfristige strategische Beratung anbieten zu können, muss die ENISA aktuelle und neu auftretende Cybersicherheitsrisiken analysieren. Hierzu sollte die ENISA in Zusammenarbeit mit den Mitgliedstaaten und gegebenenfalls Statistikämtern und anderen Stellen einschlägige öffentlich zugängliche oder freiwillig bereitgestellte Informationen sammeln und Analysen neu entstehender Technik sowie themenspezifische Bewertungen dazu durchführen, welche gesellschaftlichen, rechtlichen, wirtschaftlichen und regulatorischen Folgen technische Innovationen für die Netz- und Informationssicherheit, insbesondere die Cybersicherheit, haben. Die ENISA sollte die Mitgliedstaaten sowie die Organe, Einrichtungen und sonstigen Stellen der Union darüber hinaus bei der Ermittlung sich abzeichnender Cybersicherheitsrisiken und bei der Vermeidung von Vorfällen unterstützen, indem sie Analysen der Cyberbedrohungen, Sicherheitslücken und Sicherheitsvorfälle durchführt.

(39) Um die Abwehrfähigkeit der Union zu stärken, sollte die ENISA Fachwissen im Bereich der Cybersicherheit der Infrastrukturen, insbesondere zur Unterstützung der in Anhang II der Richtlinie (EU) 2016/1148 aufgeführten Sektoren und der Infrastrukturen, die von den in Anhang III jener Richtlinie aufgeführten Anbietern digitaler Dienste genutzt werden, aufbauen, indem Beratung, Leitlinien zur Verfügung gestellt und bewährte Verfahren ausgetauscht werden. Um den Zugang zu besser strukturierten Informationen über Cybersicherheitsrisiken und mögliche Abhilfemaßnahmen zu erleichtern, sollte die ENISA das Informationsportal der Union aufbauen und pflegen, über das der Öffentlichkeit Informationen der Organe, Einrichtungen und sonstigen Stellen der Union und der Mitgliedstaaten zur Cybersicherheit bereitgestellt werden. Ein leichterer Zugang zu besser strukturierten Informationen über Cybersicherheitsrisiken und mögliche Abhilfemaßnahmen könnte den Mitgliedstaaten auch dabei helfen, ihre Kapazitäten auszubauen und ihre Verfahren aufeinander abzustimmen, sodass die Abwehrfähigkeit gegenüber Cyberangriffen insgesamt gestärkt wird.

(40) Die ENISA sollte dabei mitwirken, die Öffentlichkeit für Cybersicherheitsrisiken zu sensibilisieren, unter anderem durch eine unionsweite Sensibilisierungskampagne, die Förderung von Schulungen, und Leitlinien für bewährte Verfahren, die sich an Bürger, Organisationen und Unternehmen richten. Darüber hinaus sollte die ENISA einen Beitrag dazu leisten, bewährte Verfahren und Lösungen, einschließlich Cyberhygiene und Cyberkompetenz, auf der Ebene von Bürgern, Organisationen und Unternehmen zu fördern, indem sie öffentlich verfügbare Informationen über erhebliche Sicherheitsvorfälle sammelt und analysiert und Berichte und Leitlinien hierüber erstellt und veröffentlicht, die das Niveau der Abwehrbereitschaft und Abwehrfähigkeit von Bürgern, Organisationen und Unternehmen insgesamt erhöhen. Die ENISA sollte sich außerdem bemühen, Verbrauchern relevante Informationen über anwendbare Zertifizierungsschemata an die Hand zu geben, indem sie beispielsweise Leitlinien und Empfehlungen bereitstellt. Ferner sollte die ENISA gemäß dem mit der Mitteilung der Kommission vom 17. Januar 2018 aufgestellten Aktionsplan für digitale Bildung in Zusammenarbeit mit den Mitgliedstaaten und den Organen, Einrichtungen und sonstigen Stellen der Union regelmäßige öffentliche Aufklärungskampagnen durchführen, die sich an die Endnutzer richten, um sicherere Verhaltensweisen der Nutzer im Internet und digitale Kompetenz zu fördern, die Nutzer stärker für potenzielle Bedrohungen im Internet — auch für die Internetkriminalität wie das Abgreifen von Daten (Phishing), Botnets, Finanz- und Bankenbetrug sowie Datenbetrug — zu sensibilisieren und einfache Empfehlungen in Bezug auf mehrstufige Authentifizierung, Patching, Verschlüsselung, Anonymisierung und Datenschutz zu geben.

(41) Die ENISA sollte eine zentrale Rolle dabei spielen, die Sensibilisierung der Endnutzer für die Sicherheit von Geräten und die sichere Nutzung von Diensten zu forcieren und auf Unionsebene konzeptionsintegrierte Sicherheit und konzeptionsintegrierten Schutz der Privatsphäre (privacy by design) zu fördern. Dabei sollte die ENISA die verfügbaren bewährten Verfahren und die vorhandene Erfahrung insbesondere von Forschungseinrichtungen und Wissenschaftlern im Bereich IT-Sicherheit optimal nutzen.

(42) Um die im Cybersicherheitssektor tätigen Unternehmen und die Nutzer von Cybersicherheitslösungen zu unterstützen, sollte die ENISA eine „Marktbeobachtungsstelle" aufbauen und pflegen, die die wichtigsten Nachfrage- und Angebotstrends auf dem Cybersicherheitsmarkt regelmäßig analysiert und bekannt macht.

(43) Die ENISA sollte einen Beitrag zu den Bemühungen der Union um eine Zusammenarbeit mit internationalen Organisationen sowie innerhalb der einschlägigen internationalen Gremien für die Zusammenarbeit im Bereich der Cybersicherheit leisten. Insbesondere sollte die ENISA gegebenenfalls an der Zusammenarbeit mit Organisationen wie der OECD, der OSZE und der NATO mitwirken. Diese Zusammenarbeit könnte gemeinsame Cybersicherheitsübungen und eine gemeinsame Koordinierung der Reaktion auf Sicherheitsvorfälle umfassen. Diese Aktivitäten müssen unter uneingeschränkter Achtung der Grundsätze der Inklusivität, der Gegenseitigkeit und der Beschlussfassungsautonomie der Union — unbeschadet der spezifischen Merkmale der Sicherheits- und Verteidigungspolitik der einzelnen Mitgliedstaaten — erfolgen.

(44) Damit die ENISA ihre Ziele in vollem Umfang verwirklichen kann, sollte sie zu den einschlägigen Aufsichtsbehörden und anderen zuständigen Behörden in der Union und anderen zuständigen Behörden, Einrichtungen und sonstigen Stellen der Union Kontakt halten — etwa zum CERT-EU, EC3, zur Europäischen Verteidigungsagentur (EDA), zur Agentur für das Europäische zivile Satellitennavigationssystem (Europäische GNSS Agentur — GSA), zum Gremium Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK), zur Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA), zur Europäischen Zentralbank (EZB), zur Europäischen Bankenaufsichtsbehörde (EBA), zum Europäischen Datenschutzausschuss, zur Agentur für die Zusammenarbeit der Energieregulierungsbehörden (ACER), zur Europäischen Agentur für Flugsicherheit (EASA) und zu sonstigen Agenturen der Union, die sich mit Fragen der Cybersicherheit beschäftigen. Für den Austausch von Know-how und bewährten Verfahren und für die Beratung zu Fragen der Cybersicherheit, die sich auf die Arbeit von Datenschutzbehörden auswirken können, sollte die ENISA auch mit diesen in Verbindung stehen. Vertreter der Strafverfolgungs- und der Datenschutzbehörden auf nationaler Ebene und auf Unionsebene sollten als Vertreter für eine Mitwirkung in der ENISA-Beratungsgruppe in Frage kommen. Bei ihren Kontakten mit Strafverfolgungsbehörden in Bezug auf Netz- und Informationssicherheitsfragen, die sich möglicherweise auf deren Arbeit auswirken, sollte die ENISA vorhandene Informationskanäle und bestehende Netze beachten.

(45) Es könnten Partnerschaften mit Hochschulen eingerichtet werden, die in den einschlägigen Bereichen Forschungsinitiativen betreiben, und es sollten geeignete Kanäle für Beiträge von Verbraucherschutzverbänden und anderen Organisationen, die berücksichtigt werden sollten, zur Verfügung stehen.

(46) Die ENISA sollte in ihrer Rolle als Sekretariat des CSIRTs-Netzes bezüglich der in der Richtlinie (EU) 2016/1148 festgelegten einschlägigen Aufgaben des CSIRTs-Netzes die CSIRTs der Mitgliedstaaten und das CERT-EU bei der operativen Zusammenarbeit unterstützen. Zudem sollte die ENISA unter gebührender Berücksichtigung der Standardbetriebsverfahren des CSIRTs-Netzes die Zusammenarbeit zwischen den jeweiligen CSIRTs bei Sicherheitsvorfällen, Angriffen oder Störungen der von den CSIRTs verwalteten oder geschützten Netze oder Infrastrukturen, die mindestens zwei CSIRTs betreffen oder betreffen können, fördern und unterstützen.

(47) Zur Erhöhung der Abwehrbereitschaft der Union bei Cybersicherheitsvorfällen sollte die ENISA auf Unionsebene regelmäßige Cybersicherheitsübungen organisieren und die Mitgliedstaaten sowie die Organe, Einrichtungen und sonstigen Stellen der Union auf deren Ersuchen hin bei der Organisation solcher Übungen unterstützen. Eine Großübung sollte alle zwei Jahre veranstaltet werden, die technische, operative und strategische Elemente umfasst. Darüber hinaus sollte die ENISA regelmäßig weniger umfassende Übungen organisieren können, mit denen dasselbe Ziel verfolgt wird, nämlich die Abwehrbereitschaft der Union bei Sicherheitsvorfällen zu stärken.

(48) Die ENISA sollte ihre Sachkenntnis im Bereich der Cybersicherheitszertifizierung weiter ausbauen und pflegen, damit sie die Unionspolitik auf diesem Gebiet unterstützen kann. Die ENISA sollte auf bestehenden bewährten Verfahren aufbauen und die Nutzung der Cybersicherheitszertifizierung in der Union fördern, auch indem sie zum Aufbau und zur Pflege eines Rahmens für die Cybersicherheitszertifizierung auf Unionsebene (europäischer Rahmen für die Cybersicherheitszertifizierung) beiträgt, um so die Transparenz der Vertrauenswürdigkeit der Cybersicherheit von IKT-Produkten, -Diensten und -Prozessen zu erhöhen und damit das Vertrauen in den digitalen Binnenmarkt und in seine Wettbewerbsfähigkeit zu stärken.

(49) Effiziente Cybersicherheitsstrategien sollten sowohl im öffentlichen als auch im privaten Sektor auf sorgfältig entwickelten Risikobewertungsmethoden beruhen. Risikobewertungsmethoden werden auf verschiedenen Ebenen angewandt, ohne dass es eine einheitliche Vorgehensweise für deren effiziente Anwendung gibt. Durch die Förderung und Entwicklung bewährter Verfahren für die Risikobewertung und interoperabler Lösungen für das Risikomanagement innerhalb von Organisationen des öffentlichen und des privaten Sektors wird das Niveau der Cybersicherheit in der Union erhöht. Zu diesem Zweck sollte die ENISA die Zusammenarbeit zwischen Interessenträgern auf Unionsebene unterstützen und Hilfestellung bei deren Bemühungen um die Festlegung und Einführung von europäischen und internationalen Normen für das Risikomanagement und eine messbare Sicherheit in Bezug auf elektronische Produkte, Systeme, Netze und Dienste leisten, die im Zusammenwirken mit Software die Netz- und Informationssysteme bilden.

(50) Die ENISA sollte die Mitgliedstaaten, die Hersteller oder die Anbieter von IKT-Produkten, -Diensten oder -Prozessen dazu anspornen, ihre allgemeinen Sicherheitsstandards zu heben, damit alle Internetnutzer die erforderlichen Vorkehrungen für ihre persönliche Cybersicherheit treffen können und sie sollte Anreize dazu geben. So sollten Hersteller und Anbieter von IKT-Produkten, -Diensten oder -Prozessen jegliche notwendigen Aktualisierungen bereitstellen und diese IKT-Produkte, -Dienste und -Prozesse zurückrufen, vom Markt nehmen oder umrüsten, wenn sie den Cybersicherheitsstandards nicht genügen, während Einführer und Händler sicherstellen sollten, dass IKT-Produkte, -Dienste und -Prozesse, die sie in der Union vermarkten, den geltenden Anforderungen genügen und kein Risiko für die Verbraucher in der Union darstellen.

(51) In Zusammenarbeit mit den zuständigen Behörden sollte die ENISA Informationen über das Niveau der Cybersicherheit von IKT-Produkten, -Diensten oder -Prozessen verbreiten, die auf dem Binnenmarkt angeboten werden, und sollte Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen verwarnen und sie auffordern, die Sicherheit, auch die Cybersicherheit, ihrer IKT-Produkte, -Dienste oder -Prozesse zu verbessern.

(52) Die ENISA sollte die laufenden Tätigkeiten auf den Gebieten der Forschung, Entwicklung und technologischen Bewertung — insbesondere die im Rahmen der vielfältigen Forschungsinitiativen der Union durchgeführten Tätigkeiten — umfassend berücksichtigen, um die Organe, Einrichtungen und sonstigen Stellen der Union sowie gegebenenfalls die Mitgliedstaaten — auf deren Ersuchen — in Bezug auf den Forschungsbedarf und die Prioritäten im Bereich der Cybersicherheit zu beraten. Um den Bedarf und die Prioritäten im Forschungsbereich zu ermitteln, sollte die ENISA auch die einschlägigen Nutzergruppen konsultieren. Insbesondere könnte eine Zusammenarbeit mit dem Europäischen Forschungsrat und dem Europäischen Innovations- und Technologieinstitut sowie mit dem Institut der Europäischen Union für Sicherheitsstudien eingerichtet werden.

(53) Die ENISA sollte die Normungsgremien, insbesondere die europäischen Normungsgremien, bei der Ausarbeitung von europäischen Schemata für die Cybersicherheitszertifizierung regelmäßig konsultieren.

(54) Cyberbedrohungen bestehen weltweit. Um die Cybersicherheitsstandards, einschließlich der Notwendigkeit der Festlegung gemeinsamer Verhaltensnormen und der Annahme von Verhaltenskodizes, der Verwendung internationaler Normen und des Informationsaustauschs zu verbessern sowie eine zügigere internationale Zusammenarbeit bei der Abwehr und einen weltweiten gemeinsamen Ansatz für Probleme der Netz- und Informationssicherheit zu fördern, bedarf es einer engeren internationalen Zusammenarbeit. In dieser Hinsicht sollte die ENISA ein stärkeres Engagement der Union und die Zusammenarbeit mit Drittländern und internationalen Organisationen unterstützen, indem sie den einschlägigen Organen, Einrichtungen und sonstigen Stellen der Union gegebenenfalls die erforderlichen Sachkenntnisse und Analysen zur Verfügung stellt.

(55) Die ENISA sollte in der Lage sein, auf Ersuchen der Mitgliedstaaten und der Organe, Einrichtungen und sonstigen Stellen der Union um Rat und Hilfestellung zu Angelegenheiten, die durch das Mandat der ENISA abgedeckt sind, ad hoc zu reagieren.

(56) In Bezug auf die Führung der ENISA ist es vernünftig und wird empfohlen bestimmte Prinzipien umzusetzen, um der Gemeinsamen Erklärung und dem Gemeinsamen Konzept zu entsprechen, die von der Interinstitutionellen Arbeitsgruppe zu den dezentralen Einrichtungen der EU im Juli 2012 vereinbart wurden und deren Zweck darin besteht, die Aktivitäten der dezentralen Agenturen dynamischer zu gestalten und ihre Leistung zu verbessern. Die in der Gemeinsamen Erklärung und dem Gemeinsamen Konzept enthaltenen Empfehlungen sollten gegebenenfalls auch in den Arbeitsprogrammen, den Bewertungen und den Berichterstattungs- und Verwaltungsverfahren der ENISA zur Geltung kommen.

(57) Der Verwaltungsrat, der sich aus Vertretern der Mitgliedstaaten und der Kommission zusammensetzt, sollte die allgemeine Ausrichtung der Tätigkeit der ENISA festlegen und dafür sorgen, dass sie ihre Aufgaben im Einklang mit dieser Verordnung wahrnimmt. Der Verwaltungsrat sollte über die erforderlichen Befugnisse verfügen, um den Haushaltsplan zu erstellen und die Ausführung des Haushaltsplans zu überprüfen, angemessene Finanzvorschriften und transparente Verfahren für die Entscheidungsfindung der ENISA festzulegen, das einheitliche Programmplanungsdokument der ENISA anzunehmen, sich eine Geschäftsordnung zu geben, den Exekutivdirektor zu ernennen und über die Verlängerung sowie die Beendigung der Amtszeit des Exekutivdirektors zu beschließen.

(58) Damit die ENISA ihre Aufgaben ordnungsgemäß und effizient wahrnehmen kann, sollten die Kommission und die Mitgliedstaaten sicherstellen, dass die Personen, die als Mitglieder des Verwaltungsrats ernannt werden, über angemessenes Fachwissen und geeignete Erfahrung verfügen. Die Kommission und die Mitgliedstaaten sollten sich auch darum bemühen, die Fluktuation bei ihren jeweiligen Vertretern im Verwaltungsrat zu verringern, um die Kontinuität seiner Arbeit sicherzustellen.

(59) Damit die ENISA reibungslos funktioniert, ist es erforderlich, dass ihr Exekutivdirektor aufgrund seiner Verdienste und nachgewiesenen Verwaltungs- und Managementfähigkeiten ernannt wird und über einschlägige Sachkenntnis und Erfahrungen auf dem Gebiet der Cybersicherheit verfügt. Die Aufgaben des Exekutivdirektors sollten in völliger Unabhängigkeit wahrgenommen werden. Der Exekutivdirektor sollte nach Anhörung der Kommission einen Vorschlag für das jährliche Arbeitsprogramm der ENISA ausarbeiten und alle erforderlichen Maßnahmen zu dessen ordnungsgemäßer Durchführung ergreifen. Der Exekutivdirektor sollte einen dem Verwaltungsrat vorzulegenden Jahresbericht, in dem auch die Umsetzung des jährlichen Arbeitsprogramms der ENISA behandelt wird, ausarbeiten, einen Entwurf eines Voranschlags für die Einnahmen und Ausgaben der ENISA erstellen und den Haushaltsplan ausführen. Der Exekutivdirektor sollte zudem die Möglichkeit haben, Ad-hoc-Arbeitsgruppen einzusetzen, die sich mit wissenschaftlichen, technischen, rechtlichen oder sozioökonomischen Einzelfragen befassen. Insbesondere im Zusammenhang mit der Ausarbeitung eines möglichen europäischen Schemas für die Cybersicherheitszertifizierung (im Folgenden „mögliches Schema“) wird die Einrichtung einer Ad-hoc-Arbeitsgruppe für notwendig

erachtet. Der Exekutivdirektor sollte dafür sorgen, dass die Mitglieder der Ad-hoc-Arbeitsgruppen höchsten fachlichen Ansprüchen genügen, ein ausgewogenes Verhältnis von Frauen und Männern besteht und dass je nach behandelter Einzelfrage gegebenenfalls ein angemessenes Gleichgewicht zwischen öffentlichen Verwaltungen der Mitgliedstaaten, den Organen, Einrichtungen und sonstigen Stellen der Union und dem Privatsektor einschließlich der Wirtschaft, der Nutzer und wissenschaftlicher Sachverständiger für Netz- und Informationssicherheit gewahrt wird.

(60) Der Exekutivrat sollte dazu beitragen, dass der Verwaltungsrat effektiv arbeiten kann. Im Rahmen seiner vorbereitenden Arbeiten für die Beschlüsse des Verwaltungsrats sollte der Exekutivrat die einschlägigen Informationen im Detail prüfen und die sich bietenden Optionen sondieren; zudem sollte er die einschlägigen Beschlüsse des Verwaltungsrats vorbereiten, indem er Beratung und Lösungen anbietet.

(61) Die ENISA sollte über eine ENISA-Beratungsgruppe als Beratungsgremium verfügen, um einen regelmäßigen Dialog mit dem Privatsektor, den Verbraucherorganisationen und sonstigen relevanten Interessenträgern sicherzustellen. Die vom Verwaltungsrat auf Vorschlag des Exekutivdirektors eingesetzte ENISA-Beratungsgruppe sollte hauptsächlich Fragen behandeln, die die Beteiligten betreffen, und diese der ENISA zur Kenntnis bringen. Die ENISA-Beratungsgruppe sollte vor allem im Hinblick auf den Entwurf des jährlichen Arbeitsprogramms der ENISA hinzugezogen werden. Die Zusammensetzung der ENISA-Beratungsgruppe und die dieser Gruppe übertragenen Aufgaben, sollten gewährleisten, dass die Interessenträger bei der Tätigkeit der ENISA ausreichend vertreten sind.

(62) Die Gruppe der Interessenträger für die Cybersicherheitszertifizierung sollte eingesetzt werden, um der ENISA und der Kommission die Konsultation der maßgeblichen Interessenträger zu erleichtern. Die Gruppe der Interessenträger für die Cybersicherheitszertifizierung sollte sich in ausgewogenem Verhältnis aus Branchenvertretern sowohl der Nachfrage- als auch der Angebotsseite in Bezug auf IKT-Produkte und -Dienste zusammensetzen; insbesondere sollten KMU, Anbieter digitaler Dienste, europäische und internationale Normungsgremien, nationale Akkreditierungsstellen, Datenschutz-Aufsichtsbehörden, Konformitätsbewertungsstellen gemäß der Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates ([16]) und die Wissenschaft sowie Verbraucherorganisationen vertreten sein.

(63) Die ENISA sollte über Vorschriften zur Vermeidung und Handhabung von Interessenkonflikten verfügen. Die ENISA sollte die einschlägigen Bestimmungen der Union in Bezug auf den Zugang der Öffentlichkeit zu Dokumenten gemäß der Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates ([17]) anwenden. Die Verarbeitung personenbezogener Daten durch die ENISA sollte nach der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([18]) erfolgen. Die ENISA sollte die für die Organe, Einrichtungen und sonstigen Stellen der Union geltenden Bestimmungen über den Umgang mit Informationen, insbesondere mit sensiblen Informationen und Verschlusssachen der Europäischen Union (EUCI), sowie die entsprechenden nationalen Rechtsvorschriften befolgen.

(64) Damit die volle Autonomie und Unabhängigkeit der ENISA gewährleistet ist und sie zusätzliche Aufgaben — auch nicht vorhergesehene Aufgaben in Notfällen — erfüllen kann, sollte die ENISA über einen ausreichenden und eigenständigen Haushalt verfügen, der hauptsächlich durch einen Beitrag der Union und durch Beiträge von Drittländern, die sich an der Arbeit der ENISA beteiligen, finanziert werden sollte. Ein angemessen ausgestatteter Haushaltsplan ist von entscheidender Bedeutung dafür, dass die ENISA ausreichende Kapazitäten hat, um ihren wachsenden Aufgaben zu erfüllen und ihre Ziele zu erreichen. Die Mehrheit der Agenturbediensteten sollte unmittelbar mit der operativen Umsetzung des Mandats der ENISA befasst sein. Dem Sitzmitgliedstaat und anderen Mitgliedstaaten sollte es erlaubt sein, freiwillige Beiträge zum Haushaltsplan der ENISA zu leisten. Sämtliche Zuschüsse aus dem Gesamthaushaltsplan der Europäischen Union sollten dem Haushaltsverfahren der Union unterliegen. Ferner sollte die Rechnungsführung der ENISA durch den Rechnungshof geprüft werden, um Transparenz und Rechenschaftspflicht sicherzustellen.

(65) Die Cybersicherheitszertifizierung spielt eine große Rolle, wenn es darum geht, das Vertrauen in IKT-Produkte, -Dienste und -Prozesse zu stärken und deren Sicherheit zu erhöhen. Die Entwicklung des digitalen Binnenmarkts und insbesondere der Datenwirtschaft und des Internets der Dinge kommt nur voran, wenn in der breiten Öffentlichkeit das Vertrauen vorhanden ist, dass diese Produkte, Dienste und Prozesse ein gewisses Maß an Cybersicherheit gewährleisten. Vernetzte und automatisierte Fahrzeuge, elektronische medizinische Geräte, die automatischen Steuerungssysteme der Industrie und intelligente Netze sind, sind nur einige Beispiele von Sektoren, in denen die Zertifizierung bereits breiten Einsatz findet oder in naher Zukunft eingesetzt werden soll. Die unter die Richtlinie (EU) 2016/1148 fallenden Sektoren sind zudem Sektoren, in denen die Cybersicherheitszertifizierung ein maßgeblicher Faktor ist.

([16]) Verordnung (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten und zur Aufhebung der Verordnung (EWG) Nr. 339/93 des Rates (ABl. L 218 vom 13.8.2008, S. 30).

([17]) Verordnung (EG) Nr. 1049/2001 des Europäischen Parlaments und des Rates vom 30. Mai 2001 über den Zugang der Öffentlichkeit zu Dokumenten des Europäischen Parlaments, des Rates und der Kommission (ABl. L 145 vom 31.5.2001, S. 43).

([18]) Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG ABl. L 295 vom 21.11.2018, S. 39).

(66) In ihrer Mitteilung aus dem Jahr 2016 mit dem Titel „Stärkung der Abwehrfähigkeit Europas im Bereich der Cybersicherheit und Förderung einer wettbewerbsfähigen und innovativen Cybersicherheitsbranche“ unterstrich die Kommission die Notwendigkeit hochwertiger, erschwinglicher und interoperabler Produkte und Lösungen für die Cybersicherheit. Allerdings ist das Angebot an IKT-Produkten, -Diensten und -Prozessen im Binnenmarkt nach wie vor geografisch stark zersplittert. Das liegt daran, dass sich die Cybersicherheitsbranche in Europa überwiegend aufgrund der Nachfrage der nationalen Regierungen entwickelt hat. Zudem gehört der Mangel an interoperablen Lösungen (technischen Normen), Verfahrensweisen und unionsweiten Zertifizierungsmechanismen zu den Defiziten, die den Binnenmarkt im Bereich der Cybersicherheit beeinträchtigen. Dies macht es für europäische Unternehmen schwerer, im nationalen, unionsweiten und weltweiten Wettbewerb zu bestehen. Es verringert sich dadurch auch das Angebot an tragfähiger und einsetzbarer Cybersicherheitstechnik, auf die Privatpersonen und Unternehmen zugreifen können. Auch in der Mitteilung des Jahres 2017 zur Halbzeitbewertung der Umsetzung der Strategie für den digitalen Binnenmarkt — Ein vernetzter digitaler Binnenmarkt für alle — unterstrich die Kommission die Bedeutung sicherer vernetzter Produkte und Systeme und verwies darauf, dass die Schaffung eines europäischen Rahmens für die IKT-Sicherheit, auf dessen Grundlage Vorschriften für die Organisation der IKT-Sicherheitszertifizierung in der Union festgelegt werden, dafür sorgen kann, dass das Vertrauen in den Binnenmarkt erhalten bleibt und die derzeitige Fragmentierung des Binnenmarkts eingedämmt wird.

(67) Derzeit werden IKT-Produkte, -Dienste und -Prozesse, im Hinblick auf ihre Cybersicherheit kaum zertifiziert. Wenn dies doch der Fall ist, geschieht es meist auf Ebene der Mitgliedstaaten oder im Rahmen brancheneigener Programme. So wird ein von einer nationalen Behörde für die Cybersicherheitszertifizierung ausgestelltes Zertifikat nicht grundsätzlich auch in anderen Mitgliedstaaten anerkannt. Unternehmen müssen somit ihre IKT-Produkte, -Dienste und -Prozesse möglicherweise in mehreren Mitgliedstaaten, in denen sie tätig sind, zertifizieren lassen, um beispielsweise an einer nationalen Ausschreibung teilzunehmen, was ihre Kosten erhöht. Auch wenn immer neue Systeme entstehen, scheint es kein kohärentes und ganzheitliches Konzept zu geben, das sich mit horizontalen Fragen der Cybersicherheit, etwa im Bereich des Internets der Dinge, befasst. Die vorhandenen Systeme weisen im Hinblick auf Produkterfassung, Vertrauenswürdigkeitsstufen, wesentliche Kriterien und tatsächliche Nutzung erhebliche Mängel und Unterschiede auf, was die Verfahren zur gegenseitigen Anerkennung in der Union behindert.

(68) Einige Anstrengungen wurden bereits unternommen, um eine gegenseitige Anerkennung der Zertifikate in der Union zu gewährleisten. Diese waren jedoch nur zum Teil erfolgreich. Das in dieser Hinsicht wichtigste Beispiel ist die in der Gruppe hoher Beamter für die Sicherheit der Informationssysteme (SOG-IS) getroffene Vereinbarung über die gegenseitige Anerkennung (MRA). Auch wenn diese Vereinbarung das wichtigste Vorbild für die Zusammenarbeit und gegenseitige Anerkennung auf dem Gebiet der Sicherheitszertifizierung ist, umfasst die SOG-IS nur einige der Mitgliedstaaten. Dies hat aus Binnenmarktsicht zur Folge, dass die Vereinbarungen der Gruppe nur begrenzt wirksam sind.

(69) Daher ist es notwendig, einen gemeinsamen Ansatz zu verfolgen und einen europäischen Rahmen für die Cybersicherheitszertifizierung aufzubauen, auf dessen Grundlage die Anforderungen an die zu entwickelnden europäischen Schemata für die Cybersicherheitszertifizierung festgelegt werden, damit die europäischen Cybersicherheitszertifikate und EU-Konformitätserklärungen für IKT-Produkte, -Dienste oder -Prozesse in allen Mitgliedstaaten anerkannt und verwendet werden können. Dabei ist es wichtig, auf vorhandenen nationalen und internationalen Schemata sowie auf Systemen der gegenseitigen Anerkennung, insbesondere der SOG-IS, aufzubauen und einen reibungslosen Übergang von vorhandenen Schemata im Rahmen solcher Systeme zu Schemata auf der Grundlage des neuen europäischen Rahmens für die Cybersicherheitszertifizierung zu ermöglichen. Mit einem europäischen Rahmen für die Cybersicherheitszertifizierung sollten zwei Ziele verfolgt werden: erstens sollte er dazu beitragen, das Vertrauen in IKT-Produkte, -Dienste und -Prozesse zu erhöhen, die nach Schemata für die europäische Cybersicherheitszertifizierung zertifiziert wurden. Zweitens sollte er dazu beitragen, dass sich vielfältige, sich widersprechende oder überlappende nationale Schemata für die Cybersicherheitszertifizierung vermeiden lassen, und so die Kosten für auf dem digitalen Binnenmarkt tätige Unternehmen senken. Die europäischen Schemata für die Cybersicherheitszertifizierung sollten nichtdiskriminierend sein und sich auf europäische oder internationale Normen stützen, sofern diese Normen nicht unwirksam oder unangemessen im Hinblick auf die Erreichung der legitimen Ziele der Union in diesem Bereich sind.

(70) Der europäische Rahmen für die Cybersicherheitszertifizierung sollte in einheitlicher Weise in allen Mitgliedstaaten eingeführt werden, damit es nicht aufgrund unterschiedlicher Anforderungsniveaus zwischen den Mitgliedstaaten zu einem „Zertifizierungsshopping“ kommt.

(71) Europäische Schemata für die Cybersicherheitszertifizierung sollten auf dem auf internationaler und nationaler Ebene bereits Vorhandenen und erforderlichenfalls auf den von Gremien und Konsortien erstellten technischen Spezifikationen aufbauen, wobei die derzeitigen Stärken genutzt und Schwachstellen bewertet und behoben werden sollten.

(72) Es bedarf flexibler Cybersicherheitslösungen, damit die Branche den Cyberbedrohungen immer einen Schritt voraus ist und daher sollte jedes Zertifizierungsschema so gestaltet werden, dass das Risiko eines schnellen Veraltens vermieden wird.

(73) Die Kommission sollte befugt sein, für bestimmte Gruppen von IKT-Produkten, -Diensten und -Prozessen europäische Schemata für die Cybersicherheitszertifizierung anzunehmen. Diese Schemata sollten von nationalen Behörden für die Cybersicherheitszertifizierung umgesetzt und überwacht werden, und die im Rahmen dieser Schemata erteilten Zertifikate sollten unionsweit gültig sein und anerkannt werden. Die von der Industrie oder sonstigen privaten Organisationen betriebenen Zertifizierungsschemata sollten nicht in den Anwendungsbereich dieser Verordnung fallen. Die Stellen, die solche Schemata betreiben, sollten der Kommission jedoch vorschlagen können, ihre Systeme als Grundlage für ein europäisches Schema für die Cybersicherheitszertifizierung in Betracht zu ziehen und sie als ein solches zu genehmigen.

(74) Die Rechtsvorschriften der Union, in denen bestimmte Vorschriften zur Zertifizierung von IKT-Produkten, -Diensten und -Prozessen festgelegt sind, bleiben von den Bestimmungen dieser Verordnung unberührt. Insbesondere enthält die Verordnung (EU) 2016/679 Bestimmungen zur Einführung von Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen, die dem Nachweis dienen, dass die für die Datenverarbeitung Verantwortlichen und die Auftragsverarbeiter bei der Verarbeitung von Daten die Bestimmungen der genannten Verordnung einhalten. Solche Zertifizierungsverfahren sowie Datenschutzsiegel und -prüfzeichen sollten den betroffenen Personen einen raschen Überblick über das Datenschutzniveau einschlägiger IKT-Produkte, -Dienste und -Prozesse ermöglichen. Die Zertifizierung von Datenverarbeitungsvorgängen, die unter die Verordnung (EU) 2016/679 fallen, auch wenn solche Vorgänge in IKT-Produkte, -Dienste und -Prozesse eingebettet sind, bleibt von der vorliegenden Verordnung unberührt.

(75) Mit den europäischen Schemata für die Cybersicherheitszertifizierung sollte gewährleistet werden, dass die nach solchen Systemen zertifizierten IKT-Produkte, -Dienste und -Prozesse bestimmten Anforderungen genügen, deren Ziel es ist, die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten, Funktionen oder Dienste, die von diesen Produkten, Diensten und Prozessen angeboten oder über diese zugänglich gemacht werden, während deren gesamten Lebenszyklus zu schützen. In dieser Verordnung können nicht alle Anforderungen an die Cybersicherheit sämtlicher IKT-Produkte, -Dienste und -Prozesse im Einzelnen festgelegt werden. Die Vielfalt der IKT-Produkte, -Dienste und -Prozesse und der damit zusammenhängenden Anforderungen an die Cybersicherheit ist so groß, dass es sehr schwierig ist, allgemeine Anforderungen an die Cybersicherheit zu entwickeln, die unter allen Umständen gültig sind. Es gilt daher, ein breit gefasstes und allgemeines Konzept der Cybersicherheit für die Zwecke der Zertifizierung zu verabschieden, das durch besondere Cybersicherheitsziele ergänzt werden sollte, die bei der Konzeption der europäischen Schemata für die Cybersicherheitszertifizierung berücksichtigt werden müssen. Die Modalitäten, wie diese Ziele für bestimmte IKT-Produkte, -Dienste und -Prozesse erreicht werden sollen, sollten dann weiter im Einzelnen auf der Grundlage des jeweiligen von der Kommission angenommenen Zertifizierungsschemas festgelegt werden, etwa durch Verweise auf Normen oder technische Spezifikationen, wenn keine angemessenen Normen verfügbar sind.

(76) Die in europäischen Schemata für die Cybersicherheitszertifizierung zu verwendenden technischen Spezifikationen sollten unter Beachtung der in Anhang II der Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates ([19]) festgelegten Anforderungen bestimmt werden. Gewisse Abweichungen von diesen Anforderungen könnten jedoch in hinreichend begründeten Fällen als notwendig erachtet werden, wenn diese technischen Spezifikationen in einem europäischen Schema für die Cybersicherheitszertifizierung in der Vertrauenswürdigkeitsstufe „hoch" verwendet werden sollen. Die Gründe für solche Abweichungen sollten öffentlich zugänglich gemacht werden.

(77) Eine Konformitätsbewertung ist ein Verfahren, mit dem bewertet wird, ob bestimmte Anforderungen an ein IKT-Produkt, einen IKT-Dienst oder einen IKT-Prozess erfüllt werden. Dieses Verfahren wird von einem unabhängigen Dritten, bei dem es sich nicht um den Hersteller oder den Anbieter der IKT-Produkte, -Dienste oder -Prozesse, welche bewertet werden, handelt, durchgeführt. Ein europäisches Cybersicherheitszertifikat sollte nach der erfolgreichen Bewertung eines IKT-Produkts, -Dienstes oder -Prozesses ausgestellt werden. Ein europäisches Cybersicherheitszertifikat sollte als Bestätigung gelten, dass die Bewertung ordnungsgemäß durchgeführt wurde. Je nach Vertrauenswürdigkeitsstufe sollte im europäischen Schema für die Cybersicherheitszertifizierung angegeben werden, ob ein europäisches Cybersicherheitszertifikat von einer privaten oder einer öffentlichen Stelle auszustellen ist. Die Konformitätsbewertung und die Zertifizierung an sich können nicht garantieren, dass die zertifizierten IKT-Produkte, -Dienste und -Prozesse cybersicher sind. Es handelt sich vielmehr um Verfahren und technische Methoden, um zu bescheinigen, dass die IKT-Produkte, -Dienste und -Prozesse geprüft wurden und bestimmte Anforderungen an die Cybersicherheit erfüllen, wie sie anderweitig, beispielsweise in technischen Normen, festgelegt sind.

(78) Die Auswahl der angemessenen Zertifizierung und der dazugehörigen Sicherheitsanforderungen durch die Nutzer der europäischen Cybersicherheitszertifizierung sollte auf der Grundlage einer Risikoanalyse der Verwendung des IKT-Produkts, -Dienstes oder -Prozesses erfolgen. Dementsprechend sollte die Vertrauenswürdigkeitsstufe das mit der beabsichtigten Verwendung eines IKT-Produkts, -Dienstes oder -Prozesses verbundene Risiko widerspiegeln.

([19]) Verordnung (EU) Nr. 1025/2012 des Europäischen Parlaments und des Rates vom 25. Oktober 2012 zur europäischen Normung, zur Änderung der Richtlinien 89/686/EWG und 93/15/EWG des Rates sowie der Richtlinien 94/9/EG, 94/25/EG, 95/16/EG, 97/23/EG, 98/34/EG, 2004/22/EG, 2007/23/EG, 2009/23/EG und 2009/105/EG des Europäischen Parlaments und des Rates und zur Aufhebung des Beschlusses 87/95/EWG des Rates und des Beschlusses Nr. 1673/2006/EG des Europäischen Parlaments und des Rates (ABl. L 316 vom 14.11.2012, S. 12).

(79) Europäische Schemata für die Cybersicherheitszertifizierung könnten eine Konformitätsbewertung vorsehen, die unter der alleinigen Verantwortung des Herstellers oder Anbieters von IKT-Produkten, -Diensten und -Prozessen durchzuführen wäre (im Folgenden „Selbstbewertung der Konformität"). In diesen Fällen sollte es ausreichen, dass der Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen selbst alle Überprüfungen vornimmt, um sicherzustellen, dass die IKT-Produkte, -Dienste oder -Prozesse mit dem europäischen Schema für die Cybersicherheitszertifizierung konform sind. Die Selbstbewertung der Konformität sollte für IKT-Produkte, -Dienste oder -Prozesse von geringer Komplexität, die ein geringes Risiko für die Öffentlichkeit darstellen, wie bei einfacher Konzeption und einfachem Herstellungsmechanismus, als angemessen angesehen werden. Zudem sollte die Selbstbewertung der Konformität nur dann für IKT-Produkte, IKT-Dienste oder IKT-Prozesse erlaubt sein, wenn sie der Vertrauenswürdigkeitsstufe „niedrig" entsprechen.

(80) Europäische Schemata für die Cybersicherheitszertifizierung könnten sowohl die Selbstbewertung der Konformität als auch die Zertifizierung von IKT-Produkten, -Diensten oder -Prozessen zulassen. In einem solchen Fall sollten im System klare und verständliche Instrumente für Verbraucher oder andere Nutzer vorgesehen werden, mit denen sie zwischen IKT-Produkten, -Diensten oder -Prozessen, die unter der Verantwortung des Herstellers oder Anbieters von IKT-Produkten, -Diensten oder -Prozessen bewertet werden, und IKT-Produkten, -Diensten oder -Prozessen, die von einem Dritten zertifiziert werden, unterscheiden können.

(81) Ein Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen, der eine Selbstbewertung der Konformität durchführt, sollte die EU-Konformitätserklärung im Rahmen des Konformitätsbewertungsverfahrens abfassen und unterzeichnen können. Eine EU-Konformitätserklärung ist ein Dokument, welches bestätigt, dass das betreffende IKT-Produkt, der betreffende IKT-Dienst oder der betreffende IKT-Prozess die Anforderungen des Schemas erfüllt. Durch die Abfassung und Unterzeichnung der EU-Konformitätserklärung übernimmt der Hersteller oder Anbieter die Verantwortung dafür, dass das IKT-Produkt, der IKT-Dienst oder der IKT-Prozess die rechtlichen Anforderungen des europäischen Schemas für die Cybersicherheitszertifizierung erfüllt. Eine Kopie der EU-Konformitätserklärung sollte der nationalen Behörde für die Cybersicherheitszertifizierung und der ENISA vorgelegt werden.

(82) Hersteller oder Anbieter von IKT-Produkten, -Diensten und -Prozessen sollten die EU-Konformitätserklärung, die technische Dokumentation und alle weiteren einschlägigen Informationen in Bezug auf die Konformität der IKT-Produkte, -Dienste oder -Prozesse mit einem System während eines Zeitraums, der im einschlägigen europäischen Schema für die Cybersicherheitszertifizierung festgelegt ist, für die zuständige nationale Behörde für die Cybersicherheitszertifizierung bereithalten. In der technischen Dokumentation sollten die in diesem System geltenden Anforderungen aufgeführt werden und die Konzeption, Herstellung und Funktionsweise des IKT-Produkts, -Dienstes oder -Prozesses erfasst werden. Die technische Dokumentation sollte so erstellt werden, dass es möglich ist, die Konformität eines IKT-Produkts oder -Dienstes mit den in diesem System geltenden Anforderungen zu bewerten.

(83) Bei der Gestaltung des Rahmens des europäischen Schemas für die Cybersicherheitszertifizierung sollte die Einbeziehung der Mitgliedstaaten sowie eine angemessene Einbeziehung der Interessenträger berücksichtigt werden; ferner sollte die Rolle der Kommission während der Planung und Vorlage eines europäischen Schemas für die Cybersicherheitszertifizierung, der Erteilung des entsprechenden Auftrags sowie der Ausarbeitung, der Annahme und der Überprüfung eines europäischen Schemas für die Cybersicherheitszertifizierung festgelegt werden.

(84) Die Kommission sollte mit Unterstützung der Europäischen Gruppe für die Cybersicherheitszertifizierung und der Gruppe der Interessenträger für die Cybersicherheitszertifizierung im Anschluss an eine offene und umfassende Konsultation ein fortlaufendes Arbeitsprogramm der Union für europäische Schemata für die Cybersicherheitszertifizierung ausarbeiten und in Form eines nicht verbindlichen Instruments veröffentlichen. Das fortlaufende Arbeitsprogramm der Union sollte ein strategisches Dokument sein und insbesondere der Branche, den nationalen Behörden und den Normungsgremien ermöglichen, sich auf die künftigen Europäischen Schemata für die Cybersicherheitszertifizierung vorzubereiten. Das fortlaufende Arbeitsprogramm der Union sollte eine mehrjährige Übersicht über die Aufträge für die Ausarbeitung möglicher Systeme umfassen, die die Kommission der ENISA aus bestimmten Gründen zu erteilen beabsichtigt. Die Kommission sollte dieses fortlaufende Arbeitsprogramm der Union im Rahmen des fortlaufenden Plans für die IKT-Normung und bei der Erstellung ihrer Normungsaufträge an die europäischen Normungsorganisationen berücksichtigen. Wegen der raschen Einführung und Übernahme neuer Technologien sowie die Entstehung bislang unbekannter Cybersicherheitsrisiken und Gesetzgebungs- und Marktentwicklungen sollte die Kommission oder die Europäische Gruppe für die Cybersicherheitszertifizierung befugt sein, die ENISA mit der Ausarbeitung möglicher Zertifizierungsschemata, die nicht im fortlaufenden Arbeitsprogramm der Union enthalten waren, zu beauftragen. In solchen Fällen sollten die Kommission und die Europäische Gruppe für die Cybersicherheitszertifizierung auch die Notwendigkeit eines solchen Auftrags bewerten, wobei die allgemeinen Zielsetzungen und Vorgaben dieser Verordnung und die Notwendigkeit der Kontinuität bei der Planung der ENISA und der Nutzung der Ressourcen durch die ENISA zu berücksichtigen sind.

Im Anschluss an einen solchen Auftrag sollte die ENISA ohne ungebührliche Verzögerung mögliche Zertifizierungsschemata für bestimmte IKT- Produkte -Dienste und -Prozesse, ausarbeiten. Die Kommission sollte die positiven und negativen Auswirkungen ihres Auftrags auf den spezifischen Markt und insbesondere auf KMU, Innovation, die Schranken für den Eintritt in diesen Markt und die Kosten für die Endverbraucher bewerten. Die Kommission sollte befugt sein, auf der Grundlage des von der ENISA vorbereiteten möglichen Schemas das europäische Schema für die Cybersicherheitszertifizierung mittels eines Durchführungsrechtsakts anzunehmen. Unter Berücksichtigung des allgemeinen Zwecks dieser Verordnung und der in ihr festgelegten Sicherheitsziele sollten in den von der Kommission angenommenen europäischen Schemata für die Cybersicherheitszertifizierung Mindestbestimmungen in Bezug auf den Gegenstand, den Anwendungsbereich und die Funktionsweise des einzelnen Schemas festgelegt werden. Unter diese Bestimmungen sollte unter anderem Folgendes fallen: Anwendungsbereich und Ziel der Cybersicherheitszertifizierung, darunter auch die Kategorien von IKT-Produkten, -Diensten und -Prozessen, detaillierte Spezifikationen der Anforderungen an die Cybersicherheit, etwa durch Verweise auf Normen oder technische Spezifikationen, die jeweiligen Bewertungskriterien und -verfahren sowie die beabsichtigte Vertrauenswürdigkeitsstufe („niedrig“, „mittel“ oder „hoch“) sowie gegebenenfalls die Bewertungsniveaus. Die ENISA sollte einen Auftrag der Europäischen Gruppe für die Cybersicherheitszertifizierung ablehnen können. Solche Entscheidungen sollten gebührend begründet und vom Verwaltungsrat getroffen werden.

(85) Die ENISA sollte eine eigene Website unterhalten, auf der sie über die europäischen Schemata für die Cybersicherheitszertifizierung informiert und für diese wirbt und auf der unter anderem die Aufträge für die Ausarbeitung eines möglichen Schemas und die Rückmeldungen im Rahmen des Konsultationsverfahrens, das von der ENISA in der Ausarbeitungsphase durchgeführt wird, zur Verfügung stehen. Auf der Website sollten auch Informationen über die europäischen Cybersicherheitszertifikate und die nach dieser Verordnung ausgestellten EU-Konformitätserklärungen einschließlich Informationen zum Widerruf und Ablauf solcher europäischen Cybersicherheitszertifikate und EU-Konformitätserklärungen bereitgestellt werden. Auf der Website sollten auch diejenigen nationalen Schemata für die Cybersicherheitszertifizierung angegeben werden, die durch ein europäisches Schema für die Cybersicherheitszertifizierung ersetzt wurden.

(86) Die Vertrauenswürdigkeit eines europäischen Zertifizierungsschemas ist die Grundlage für das Vertrauen, dass ein IKT-Produkt, -Dienst oder -Prozess den Sicherheitsanforderungen eines spezifischen europäischen Schemas für die Cybersicherheitszertifizierung genügt. Um die Kohärenz des Rahmens für ein europäisches Schema für die Cybersicherheitszertifizierung zu gewährleisten, sollte ein europäisches Schema für die Cybersicherheitszertifizierung die Vertrauenswürdigkeitsstufen für europäische Cybersicherheitszertifikate und EU-Konformitätserklärungen, die im Rahmen dieses Schemas ausgestellt werden, angeben können. Jedes europäische Cybersicherheitszertifikat könnte sich auf eine der Vertrauenswürdigkeitsstufen „niedrig“, „mittel“ oder „hoch“ beziehen, wohingegen sich die EU-Konformitätserklärung nur auf die Vertrauenswürdigkeitsstufe „niedrig“ beziehen könnte. Die Vertrauenswürdigkeitsstufen würden die entsprechende Strenge und Gründlichkeit für die Bewertung des IKT-Produkts, -Dienstes oder -Prozesses vorgeben und durch Bezugnahme auf die diesbezüglichen technischen Spezifikationen, Normen und Verfahren einschließlich technischer Prüfungen, deren Zweck in der Minderung oder Prävention der Gefahr von Vorfällen besteht, gekennzeichnet sein. Jede Vertrauenswürdigkeitsstufe sollte in den verschiedenen Bereichen der Sektoren, in denen die Zertifizierung angewandt wird, einheitlich sein.

(87) In einem europäischen Schema für die Cybersicherheitszertifizierung können je nach Strenge und Gründlichkeit der verwendeten Evaluierungsmethode mehrere Bewertungsniveaus angegeben werden. Die Evaluierungsstufen sollten jeweils einer der Vertrauenswürdigkeitsstufen entsprechen und mit einer entsprechenden Kombination von Vertrauenswürdigkeitskomponenten verknüpft sein sollten. Für alle Vertrauenswürdigkeitsstufen sollte das IKT-Produkt, der IKT-Dienst oder der IKT-Prozess eine Reihe sicherer Funktionen enthalten, die im jeweiligen System festgelegt sind, so unter anderem eine voreingestellte sichere Konfiguration, einen signierten Code, ein sicheres Aktualisierungsverfahren und die Reduzierung von Exploits sowie eine vollständige Absicherung von Stapelspeicher (Stack) oder dynamischem Speicher (Heap). Diese Funktionen sollten weiterentwickelt und gepflegt werden, wobei sicherheitsorientierte Entwicklungskonzepte und dazugehörige Instrumente zu verwenden sind, um sicherzustellen, dass wirksame Software- und Hardware-Mechanismen zuverlässig integriert werden.

(88) Bei der Vertrauenswürdigkeitsstufe „niedrig“ sollte sich die Bewertung mindestens auf die folgenden Vertrauenswürdigkeitskomponenten stützen: Die Bewertung sollte mindestens eine Überprüfung der technischen Dokumentation des IKT-Produkts -Dienstes oder -Prozesses durch die Konformitätsbewertungsstelle umfassen. Schließt die Zertifizierung IKT-Prozesse ein, sollte auch das Verfahren zur Konzipierung, Entwicklung und Pflege eines IKT-Produkts oder -Dienstes einer technischen Überprüfung unterzogen werden. Ist in einem europäischen Schema für die Cybersicherheitszertifizierung eine Selbstbewertung der Konformität vorgesehen, so sollte es genügen, wenn der Hersteller oder Anbieter von IKT- Produkten, Diensten oder Prozessen eine Selbstbewertung der Konformität des IKT-Produkts, -Dienstes oder -Prozesses, mit dem Zertifizierungsschema vornimmt.

(89) Bei der Vertrauenswürdigkeitsstufe „mittel“ sollte sich die Bewertung — zusätzlich zu den Anforderungen bei der Vertrauenswürdigkeitsstufe „niedrig“ — mindestens auf eine Überprüfung der Konformität der Sicherheitsfunktionen des IKT-Produkts, -Dienstes oder -Prozesses mit seiner technischen Dokumentation stützen.

(90) Bei der Vertrauenswürdigkeitsstufe „hoch“ sollte sich die Bewertung — zusätzlich zu den Anforderungen bei der Vertrauenswürdigkeitsstufe „mittel“ — mindestens auf einen Wirksamkeitstest stützen, bei dem die Widerstandsfähigkeit der Sicherheitsfunktionen des IKT-Produkts, -Dienstes oder -Prozesses gegen gründlich vorbereitete Cyberattacken bewertet wird, die von Akteuren mit umfangreichen Fähigkeiten und Ressourcen durchgeführt wird.

(91) Der Rückgriff auf eine europäische Cybersicherheitszertifizierung und eine EU-Konformitätserklärung sollte freiwillig bleiben, sofern im Unionsrecht oder in entsprechend dem Unionsrecht erlassenen Rechtsvorschriften der Mitgliedstaaten nichts anderes festgelegt ist. Falls es keine harmonisierten Unionsrechtsvorschriften gibt, können die Mitgliedstaaten nationale technische Vorschriften gemäß der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates ([20]) erlassen. Die Mitgliedstaaten können auch im Zusammenhang mit öffentlichen Ausschreibungen und der Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates ([21]) auf eine europäische Cybersicherheitszertifizierung zurückgreifen.

(92) In einigen Bereichen könnte es künftig notwendig werden, bestimmte Anforderungen an die Cybersicherheit und die entsprechende Zertifizierung für bestimmte IKT-Produkte, -Dienste oder -Prozesse verbindlich vorzuschreiben, um das Niveau der Cybersicherheit in der Union zu erhöhen. Die Kommission sollte die Auswirkungen der angenommenen europäischen Schemata für die Cybersicherheitszertifizierung auf die Verfügbarkeit sicherer IKT-Produkte, -Dienste und -Prozesse im Binnenmarkt regelmäßig überwachen und sollte regelmäßig bewerten, inwieweit die Zertifizierungsschemata durch die Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen in der Union genutzt werden. Die Effizienz der europäischen Schemata für die Cybersicherheitszertifizierung und die Frage, ob bestimmte Systeme verbindlich vorgeschrieben werden sollten, sollte anhand der Rechtsvorschriften der Union im Bereich der Cybersicherheit, insbesondere der Richtlinie (EU) 2016/1148, unter Berücksichtigung der Sicherheit der von Betreibern wesentlicher Dienste genutzten Netz- und Informationssysteme bewertet werden.

(93) Die europäischen Cybersicherheitszertifikate und die EU-Konformitätserklärung sollten den Endnutzern dabei helfen, kundige Entscheidungen zu treffen. Daher sollten IKT-Produkte, -Dienste und -Prozesse, die zertifiziert wurden oder für die eine EU-Konformitätserklärung ausgestellt wurde, strukturierte Informationen beigegeben werden, die an das erwartete technische Niveau des vorgesehenen Endnutzers angepasst sind. Alle diese Informationen sollten online verfügbar sein, und gegebenenfalls physisch bereitgestellt werden. Der Endnutzer sollte Zugang zu Informationen über die Kennnummer des Zertifizierungsschemas, die Vertrauenswürdigkeitsstufe, die Beschreibung der Cybersicherheitsrisiken in Verbindung mit dem IKT-Produkt, -Dienst oder -Prozess sowie die ausstellende Stelle haben oder eine Kopie des europäischen Cybersicherheitszertifikats erhalten können. Darüber hinaus sollten die Endnutzer über die Politik des Herstellers oder Anbieters von IKT-Produkten, -Diensten oder -Prozessen zur Förderung der Cybersicherheit, d. h. darüber, wie lange ein Endnutzer Aktualisierungen oder Patches im Bereich der Cybersicherheit erwarten kann, informiert sein. Gegebenenfalls sollten Leitlinien über Maßnahmen oder Einstellungen, die der Endnutzer von IKT-Produkten oder -Diensten zur Aufrechterhaltung oder Verbesserung der Cybersicherheit vornehmen kann, und Kontaktinformationen einer zentralen Anlaufstelle zur Meldung von Cyberangriffen und zur Unterstützung im Fall von Cyberangriffen (neben der automatischen Berichterstattung) zur Verfügung gestellt werden. Diese Informationen sollten regelmäßig auf den neuesten Stand gebracht werden und auf einer Website, die Informationen über das europäische Schema für die Cybersicherheitszertifizierung bereitstellt, zur Verfügung stehen.

(94) Mit Blick auf die Ziele dieser Verordnung und zur Vermeidung einer Fragmentierung des Binnenmarkts sollten nationale Schemata oder Verfahren für die Cybersicherheitszertifizierung für die IKT-Produkte, -Dienste oder -Prozesse, die unter ein europäisches Schema für die Cybersicherheitszertifizierung fallen, ab einem Zeitpunkt unwirksam werden, den die Kommission in Durchführungsrechtsakten festlegt. Zudem sollten die Mitgliedstaaten keine neuen nationalen Schemata für die Cybersicherheitszertifizierung der IKT-Produkte, -Dienste oder -Prozesse einführen, die bereits unter ein geltendes europäisches Schema für die Cybersicherheitszertifizierung fallen. Allerdings sollte es den Mitgliedstaaten freistehen, aus Gründen der nationalen Cybersicherheit nationale Cyberzertifizierungsschemata einzuführen oder beizubehalten. Die Mitgliedstaaten sollten die Kommission und die Europäische Gruppe für die Cybersicherheitszertifizierung über ihre Absicht unterrichten, neue nationale Schemata für die Cybersicherheitszertifizierung auszuarbeiten. Die Kommission und die Europäische Gruppe für die Cybersicherheitszertifizierung sollten die Auswirkungen des neuen nationalen Schemas für die Cybersicherheitszertifizierung auf das ordnungsgemäße Funktionieren des Binnenmarkts und im Hinblick auf das strategische Interesse bewerten, stattdessen einen Auftrag für ein europäisches Schema für die Cybersicherheitszertifizierung zu erteilen.

(95) Die europäischen Schemata für die Cybersicherheitszertifizierung sollen dabei helfen, die Cybersicherheitsverfahren in der Union zu harmonisieren. Sie müssen dazu beitragen, das Niveau der Cybersicherheit in der Union zu erhöhen. Das Design der europäischen Schemata für die Cybersicherheitszertifizierung sollte weitere Innovationen im Bereich der Cybersicherheit berücksichtigen und ermöglichen werden.

([20]) 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.)

([21]) Richtlinie 2014/24/EU des Europäischen Parlaments und des Rates vom 26. Februar 2014 über die öffentliche Auftragsvergabe und zur Aufhebung der Richtlinie 2004/18/EG (ABl. L 94 vom 28.3.2014, S. 65).

(96) Die europäischen Schemata für die Cybersicherheitszertifizierung sollten die derzeitigen Methoden der Software- und Hardware-Entwicklung und insbesondere die Auswirkungen häufiger Software- oder Firmware-Aktualisierungen zu einzelnen europäischen Cybersicherheitszertifikaten berücksichtigen. Bei den europäischen Schemata für die Cybersicherheitszertifizierung sollten die Bedingungen angegeben werden, unter denen eine Aktualisierung erfordern kann, dass ein IKT-Produkt, ein IKT-Dienst oder ein IKT-Prozess neu zertifiziert werden muss oder dass der Umfang des spezifischen europäische Cybersicherheitszertifikats eingeschränkt werden muss, wobei die möglichen nachteiligen Auswirkungen der Aktualisierung auf die Einhaltung der Sicherheitsanforderungen des Zertifikats zu berücksichtigen sind.

(97) Sobald ein europäisches Schema für die Cybersicherheitszertifizierung eingeführt worden ist, sollten die Hersteller oder die Anbieter von IKT-Produkten, -Diensten oder -Prozessen die Zertifizierung ihrer IKT-Produkte, -Dienste oder -Prozesse bei einer nationalen Konformitätsbewertungsstelle ihrer Wahl an einem beliebigen Ort in der Union beantragen können. Die Konformitätsbewertungsstellen sollten, sofern sie bestimmten in dieser Verordnung festgelegten Anforderungen genügen, von einer nationalen Akkreditierungsstelle akkreditiert werden. Die Akkreditierung sollte für eine Höchstdauer von fünf Jahren erfolgen und unter denselben Bedingungen verlängert werden können, sofern die Konformitätsbewertungsstelle die Anforderungen weiterhin erfüllt. Die nationalen Akkreditierungsstellen sollten die einer Konformitätsbewertungsstelle erteilte Akkreditierung beschränken, aussetzen oder widerrufen, wenn die Voraussetzungen für die Akkreditierung nicht erfüllt wurden oder nicht mehr erfüllt werden oder wenn die Konformitätsbewertungsstelle gegen diese Verordnung verstößt.

(98) Verweise im nationalen Recht, die sich auf nationale Normen beziehen, die aufgrund des Inkrafttretens eines europäischen Schemas für die Cybersicherheitszertifizierung keine Rechtswirkung mehr haben, können zu Verwirrung führen. Daher sollten die Mitgliedstaaten der Annahme eines europäischen Schemas für die Cybersicherheitszertifizierung in ihren nationalen Rechtsvorschriften Rechnung zu tragen.

(99) Zur Erreichung gleichwertiger Standards in der gesamten Union, zur Erleichterung der gegenseitigen Anerkennung und zur Förderung der allgemeinen Akzeptanz der Europäischen Cybersicherheitszertifikate und EU-Konformitätserklärungen bedarf es eines Systems der gegenseitigen Begutachtung der nationalen Behörden für die Cybersicherheitszertifizierung. Die gegenseitige Begutachtung sollte Verfahren für Folgendes umfassen: Überwachung der Übereinstimmung der IKT-Produkte, -Dienste und -Prozesse mit den europäischen Cybersicherheitszertifikaten, Überwachung der Verpflichtungen der Hersteller oder Anbieter von IKT-Produkten, -Diensten und -Prozessen, die eine Selbstbewertung der Konformität vornehmen, Überwachung der Konformitätsbewertungsstellen sowie Angemessenheit des Fachwissens des Personals der Einrichtungen, die Zertifikate für die Vertrauenswürdigkeitsstufe „hoch“ ausstellen. Die Kommission sollte im Wege von Durchführungsrechtsakten mindestens einen Fünfjahresplan für gegenseitige Begutachtungen sowie Kriterien und Methoden für die Abwicklung der gegenseitigen Begutachtungen festlegen können.

(100) Unbeschadet des allgemeinen Systems der gegenseitigen Begutachtung, das zwischen allen nationalen Behörden für die Cybersicherheitszertifizierung im Rahmen der europäischen Cybersicherheitszertifizierung eingerichtet werden soll, können bestimmte Schemata für die europäische Cybersicherheit ein Verfahren zur gegenseitigen Begutachtung der Stellen für die Ausstellung europäischer Cybersicherheitszertifikate für IKT-Produkte, -Dienste und -Prozesse auf der Vertrauenswürdigkeitsstufe „hoch“ im Rahmen solcher Schemata umfassen. Die Gruppe für die Cybersicherheitszertifizierung sollte die Umsetzung der Verfahren der gegenseitigen Begutachtung unterstützen. Bei solchen gegenseitigen Begutachtungen sollte insbesondere bewertet werden, ob die betreffenden Stellen ihre Aufgaben einheitlich ausführen; zudem können sie Einspruchsmöglichkeiten umfassen. Die Ergebnisse der gegenseitigen Begutachtungen sollten veröffentlicht werden. Die betreffenden Stellen können entsprechend geeignete Maßnahmen ergreifen, um ihre Verfahren und Sachkenntnisse anzupassen.

(101) Die Mitgliedstaaten sollten eine oder mehrere nationale Behörden für die Cybersicherheitszertifizierung benennen, die die Einhaltung der sich aus dieser Verordnung ergebenden Verpflichtungen beaufsichtigen. Eine nationale Behörde für die Cybersicherheitszertifizierung kann eine bereits bestehende oder eine neue Behörde sein. Ein Mitgliedstaat sollte im gegenseitigen Einvernehmen mit einem anderen Mitgliedstaat auch eine oder mehrere nationale Behörden für die Cybersicherheitszertifizierung im Hoheitsgebiet dieses anderen Mitgliedstaats benennen können.

(102) Die nationalen Behörden für die Cybersicherheitszertifizierung sollten insbesondere die Verpflichtungen der in ihrem jeweiligen Hoheitsgebiet niedergelassenen Hersteller oder Anbieter von IKT-Produkten, -Diensten oder -Prozessen in Bezug auf die EU-Konformitätserklärung überwachen und durchsetzen, die nationalen Akkreditierungsstellen bei der Überwachung und Beaufsichtigung der Tätigkeiten der Konformitätsbewertungsstellen durch Bereitstellung von Sachkenntnis und einschlägigen Informationen unterstützen, Konformitätsbewertungsstellen ermächtigen, ihre Aufgaben wahrzunehmen, wenn diese in einem europäischen Schema für die Cybersicherheitszertifizierung festgelegte zusätzliche Anforderungen erfüllen, und einschlägige Entwicklungen auf dem Gebiet der Cybersicherheitszertifizierung verfolgen. Die nationalen Behörden für die Cybersicherheitszertifizierung sollten auch Beschwerden bearbeiten, die von natürlichen oder juristischen Personen in Bezug auf die von diesen Behörden ausgestellten europäischen Cybersicherheitszertifikate oder die in Verbindung mit den europäischen Cybersicherheitszertifikaten von Konformitätsbewertungsstellen ausgestellten Zertifikate für die Vertrauenswürdigkeitsstufe

„hoch“ eingereicht werden, den Beschwerdegegenstand, soweit angemessen, untersuchen und den Beschwerdeführer über die Fortschritte und das Ergebnis der Untersuchung innerhalb einer angemessenen Frist unterrichten. Darüber hinaus sollten die nationalen Behörden für die Cybersicherheitszertifizierung mit anderen nationalen Behörden für die Cybersicherheitszertifizierung und anderen öffentlichen Stellen zusammenarbeiten, auch indem sie Informationen über die etwaige Nichtkonformität von IKT-Produkten, -Diensten und -Prozessen mit den Anforderungen dieser Verordnung oder bestimmten europäischen Schemata für die Cybersicherheitszertifizierung austauschen. Die Kommission sollte diesen Informationsaustausch erleichtern, indem sie ein allgemeines elektronisches Informationssystem zur Unterstützung bereitstellt, zum Beispiel das internetgestützte Informations- und Kommunikationssystem zur europaweiten Marktüberwachung (Information and Communication System on Market Surveillance — ICSMS) und das gemeinschaftliche System zum raschen Austausch von Informationen über die Gefahren bei der Verwendung von Konsumgütern (Community system for the rapid exchange of information on dangers arising from the use of consumer products — RAPEX), die in Übereinstimmung mit der Verordnung (EG) Nr. 765/2008 bereits von Marktüberwachungsbehörden genutzt werden.

(103) Für eine einheitliche Anwendung des europäischen Rahmens für die Cybersicherheitszertifizierung sollte eine europäische Gruppe für die Cybersicherheitszertifizierung eingesetzt werden, die sich aus Vertretern der nationalen Behörden für die Cybersicherheitszertifizierung oder anderer zuständiger nationaler Behörden zusammensetzt. Die Gruppe für die Cybersicherheitszertifizierung sollte vor allem die Kommission bei ihren Tätigkeiten zur Gewährleistung einer einheitlichen Umsetzung und Anwendung des europäischen Rahmens für die Cybersicherheitszertifizierung beraten und unterstützen, die ENISA bei der Ausarbeitung der möglichen Cybersicherheitszertifizierungsschemata unterstützen und mit ihr eng zusammenarbeiten, in entsprechend begründeten Fällen die ENISA mit der Ausarbeitung eines möglichen Schemas beauftragen, an die ENISA gerichtete Stellungnahmen zu möglichen Schemata annehmen, und an die Kommission gerichtete Stellungnahmen zur Pflege und Überprüfung vorhandener europäischer Schemata für die Cybersicherheitszertifizierung annehmen. Die Gruppe für die Cybersicherheitszertifizierung sollte den Austausch von bewährten Verfahren und Sachkenntnissen zwischen den verschiedenen nationalen Behörden für die Cybersicherheitszertifizierung, die für die Ermächtigung der Konformitätsbewertungsstellen und die Ausstellung von Europäischen Cybersicherheitszertifikaten zuständig sind, erleichtern.

(104) Zur Sensibilisierung und um die Akzeptanz künftiger europäischer Schemata für die Cybersicherheitssicherheit zu erhöhen, kann die Kommission allgemeine und sektorspezifische Cybersicherheitsleitlinien herausgeben, die sich beispielsweise auf bewährte Verfahren oder verantwortungsvolles Verhalten im Bereich der Cybersicherheit beziehen, und dabei die Vorteile der Verwendung zertifizierter IKT-Produkte, -Dienste und -Prozesse hervorheben.

(105) Da die IKT-Lieferketten weltumspannend sind, kann die Union zur weiteren Erleichterung des Handels gemäß Artikel 218 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) Abkommen über die gegenseitige Anerkennung von europäischen Cybersicherheitszertifikaten schließen. Die Kommission kann unter Berücksichtigung der Ratschläge der ENISA und der europäischen Gruppe für die Cybersicherheitszertifizierung die Aufnahme entsprechender Verhandlungen empfehlen. In jedem europäischen Schema für die Cybersicherheitszertifizierung sollten spezifische Bedingungen für diese Abkommen über die gegenseitige Anerkennung bei Drittländern vorgesehen werden.

(106) Zur Gewährleistung einheitlicher Bedingungen für die Durchführung dieser Verordnung sollten der Kommission Durchführungsbefugnisse übertragen werden. Diese Befugnisse sollten nach Maßgabe der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates ([22]) ausgeübt werden.

(107) Das Prüfverfahren sollte für die Annahme der Durchführungsrechtsakte über die europäischen Schemata für die Cybersicherheitszertifizierung von IKT-Produkten, -Diensten oder -Prozessen, für die Annahme von Durchführungsrechtsakten über die Modalitäten für die Durchführung von Umfragen durch die ENISA, für die Annahme von Durchführungsrechtsakten über einen Plan für die gegenseitige Begutachtung der nationalen Behörden für die Cybersicherheitszertifizierung sowie für die Annahme von Durchführungsrechtsakten über die Umstände, Formate und Verfahren der Notifikation akkreditierter Konformitätsbewertungsstellen durch die nationalen Behörden für die Cybersicherheitszertifizierung bei der Kommission verwendet werden.

(108) Die Tätigkeit der ENISA sollte regelmäßig und unabhängig bewertet werden. Diese Bewertung sollte sich darauf beziehen, inwieweit die ENISA ihre Ziele erreicht, wie sie arbeitet und inwieweit ihre Aufgaben relevant sind, insbesondere ihre Aufgaben bezüglich der operativen Zusammenarbeit auf Unionsebene. Zudem sollten Wirkung, Wirksamkeit und Effizienz des europäischen Rahmens für Cybersicherheitszertifizierung bewertet werden. Im Falle einer Überprüfung sollte die Kommission bewerten, wie die Rolle der ENISA als Bezugspunkt für Beratung und Sachkenntnis verstärkt werden kann und sollte ebenfalls die Möglichkeit einer Rolle der ENISA bei der Unterstützung der Bewertung von IKT-Produkten, -Diensten und -Prozessen aus Drittländern, die auf den Unionsmarkt gelangen und gegen die Unionsvorschriften verstoßen, bewerten.

([22]) Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren (ABl. L 55 vom 28.2.2011, S. 13).

(109) Da die Ziele dieser Verordnung von den Mitgliedstaaten nicht ausreichend verwirklicht werden können, sondern vielmehr wegen ihres Umfangs und ihrer Wirkungen auf Unionsebene besser zu verwirklichen sind, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union (EUV) verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Verordnung nicht über das für die Verwirklichung dieser Ziele erforderliche Maß hinaus.

(110) Die Verordnung (EU) Nr. 526/2013 sollte aufgehoben werden —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

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 europäischen 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)

KAPITEL I

Mandat und Ziele

Artikel 3

Mandat

(1) Die ENISA nimmt die ihr mit dieser Verordnung zugewiesenen Aufgaben mit dem Ziel wahr, ein hohes gemeinsames Maß an Cybersicherheit in der gesamten Union zu erreichen, unter anderem indem sie die Mitgliedstaaten und die Organe, Einrichtungen und sonstigen Stellen der Union bei der Verbesserung der Cybersicherheit unterstützt. Die ENISA dient den Organen, Einrichtungen und sonstigen Stellen der Union sowie anderen maßgeblichen Interessenträgern der Union als Bezugspunkt für Beratung und Sachkenntnis im Bereich Cybersicherheit.

Die ENISA trägt durch die Wahrnehmung der ihr mit dieser Verordnung zugewiesenen Aufgaben zur Verringerung der Fragmentierung im Binnenmarkt bei.

(2) Die ENISA nimmt die ihr durch Rechtsakte der Union zugewiesenen Aufgaben wahr, mit denen die Rechts- und Verwaltungsvorschriften der Mitgliedstaaten auf dem Gebiet der Cybersicherheit angeglichen werden sollen.

(3) Die ENISA handelt bei der Wahrnehmung ihrer Aufgaben unabhängig, vermeidet Überschneidungen mit den Tätigkeiten der Mitgliedstaaten und berücksichtigt die bereits vorhandene Sachkenntnis der Mitgliedstaaten.

(4) Die ENISA entwickelt ihre eigenen Ressourcen, einschließlich technischer und menschlicher Fähigkeiten und Fertigkeiten, die erforderlich sind, um die ihr mit dieser Verordnung zugewiesenen Aufgaben wahrzunehmen.

Artikel 4

Ziele

(1) Die ENISA dient aufgrund ihrer Unabhängigkeit, der wissenschaftlichen und technischen Qualität der von ihr geleisteten Beratung und Unterstützung, der von ihr bereitgestellten Informationen, ihrer operativen Verfahren, ihrer Arbeitsmethoden sowie der Sorgfalt bei der Wahrnehmung ihrer Aufgaben als Kompetenzzentrum in Fragen der Cybersicherheit.

(2) Die ENISA unterstützt die Organe, Einrichtungen und sonstigen Stellen der Union sowie die Mitgliedstaaten bei der Ausarbeitung und Umsetzung von Strategien der Union im Zusammenhang mit der Cybersicherheit, wozu auch sektorbezogene Strategien zur Cybersicherheit gehören.

(3) Die ENISA fördert unionsweit den Kapazitätsaufbau und die Abwehrbereitschaft, indem sie die Organe, Einrichtungen und sonstigen Stellen der Union, die Mitgliedstaaten sowie öffentliche und private Interessenträger dabei unterstützt, den Schutz ihrer Netz- und Informationssysteme zu verbessern, Fähigkeiten zur Abwehr von Cyberangriffen und Reaktionskapazitäten aufzubauen und zu verbessern und Fähigkeiten und Kompetenzen auf dem Gebiet der Cybersicherheit aufzubauen.

(4) Die ENISA fördert auf Unionsebene die Zusammenarbeit einschließlich des Informationsaustauschs und die Koordinierung zwischen den Mitgliedstaaten, den Organen, Einrichtungen und sonstigen Stellen der Union sowie den einschlägigen privaten und öffentlichen Interessenträgern in Fragen, die im Zusammenhang mit der Cybersicherheit stehen.

(5) Die ENISA trägt zum Ausbau der Cybersicherheitskapazitäten auf Unionsebene bei, um — insbesondere bei grenzüberschreitenden Sicherheitsvorfällen — die Maßnahmen zu unterstützen, die die Mitgliedstaaten zur Vermeidung von Cyberbedrohungen oder als Reaktion darauf ergreifen.

(6) Die ENISA fördert die Nutzung der europäischen Cybersicherheits-Zertifizierung, um der Fragmentierung des Binnenmarkts vorzubeugen. Die ENISA trägt zum Aufbau und zur Pflege eines Cybersicherheitszertifizierungsrahmens im Sinne des Titels III dieser Verordnung bei, um die auf mehr Transparenz gestützte Vertrauenswürdigkeit der Cybersicherheit von IKT-Produkten, -Diensten und -Prozessen zu erhöhen und damit das Vertrauen in den digitalen Binnenmarkt sowie dessen Wettbewerbsfähigkeit zu stärken.

(7) Die ENISA fördert ein hohes Maß der Sensibilisierung für die Cybersicherheit, einschließlich der Cyberhygiene und der Cyberkompetenz von Bürgern, Organisationen und Unternehmen.

KAPITEL II

Aufgaben

Artikel 5

Entwicklung und Umsetzung der Unionspolitik und des Unionsrechts

Die ENISA trägt zur Entwicklung und Umsetzung der Unionspolitik und des Unionsrechts bei, indem sie

1. insbesondere durch unabhängige Stellungnahmen und Analysen sowie durch vorbereitende Arbeiten zur Ausarbeitung und Überprüfung der Unionspolitik und des Unionsrechts auf dem Gebiet der Cybersicherheit Beratung und Unterstützung gewährt und indem sie sektorspezifische Strategien und Rechtsetzungsinitiativen im Bereich der Cybersicherheit vorlegt;

2. die Mitgliedstaaten darin unterstützt, die Unionspolitik und das Unionsrecht auf dem Gebiet der Cybersicherheit, vor allem im Zusammenhang mit der Richtlinie (EU) 2016/1148, kohärent umzusetzen, auch durch die Abgabe von Stellungnahmen, Herausgabe von Leitlinien, Anbieten von Beratung und bewährten Verfahren zu Themen wie Risikomanagement, Meldung von Sicherheitsvorfällen und Informationsaustausch, und indem sie den Austausch bewährter Verfahren in diesem Bereich zwischen den zuständigen Behörden erleichtert;

3. die Mitgliedstaaten und die Organe, Einrichtungen und sonstigen Stellen der Union bei der Entwicklung und Förderung von Strategien im Zusammenhang mit der Cybersicherheit unterstützt, die die allgemeine Verfügbarkeit oder Integrität des öffentlichen Kerns des offenen Internets bewahren;

4. ihre Sachkenntnis und Unterstützung in die Arbeit der nach Artikel 11 der Richtlinie (EU) 2016/1148 eingesetzten Kooperationsgruppe einbringt;

5. Folgendes unterstützt:

   a) die Entwicklung und Umsetzung der Unionspolitik im Bereich der elektronischen Identität und Vertrauensdienste, vor allem durch Beratung und die Herausgabe technische Leitlinien sowie durch die Erleichterung des Austauschs bewährter Verfahren zwischen den zuständigen Behörden;

   b) die Förderung eines höheren Sicherheitsniveaus in der elektronischen Kommunikation, auch indem sie Beratung und Sachkenntnis anbietet und den Austausch bewährter Verfahren zwischen den zuständigen Behörden erleichtert;

   c) die Mitgliedstaaten bei der Umsetzung bestimmter auf die Cybersicherheit bezogener Aspekte der Politik und des Rechts der Union im Bereich des Datenschutzes und des Schutzes der Privatsphäre, was — auf dessen Ersuchen die Beratung des Europäischen Datenschutzausschusses einschließt;

6. die regelmäßige Überprüfung der Unionspolitik unterstützt und dazu einen Jahresbericht über den Stand der Umsetzung des jeweiligen Rechtsrahmens in Bezug auf Folgendes erstellt:

   a) Informationen über Meldungen von Sicherheitsvorfällen durch die Mitgliedstaaten über die zentrale Anlaufstelle der Kooperationsgruppe nach Artikel 10 Absatz 3 der Richtlinie (EU) 2016/1148;

   b) Zusammenfassungen von Meldungen von Sicherheitsverletzungen oder Integritätsverlusten von Vertrauensdiensteanbietern, die der ENISA auf der Grundlage des Artikels 19 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates ([23]) von den Aufsichtsstellen übermittelt werden;

   c) die Meldungen von Sicherheitsvorfällen durch Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugängliche elektronische Kommunikationsdienste, die der ENISA von den zuständigen Behörden auf der Grundlage des Artikels 40 der Richtlinie (EU) 2018/1972 übermittelt werden.

([23]) 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) gefördert werden und zur Aufhebung der Richtlinie 1999/93/EG (ABl. L 257 vom 28.8.2014, S. 73).

Artikel 6

Kapazitätsaufbau

(1) Die ENISA unterstützt

a) die Mitgliedstaaten bei ihren Bemühungen zur Verhütung, Erkennung und Analyse und zur Stärkung ihrer Fähigkeiten bei der Bewältigung von Cyberbedrohungen und Cybersicherheitsvorfällen, indem sie ihnen Wissen und Sachkenntnisse zur Verfügung stellt;

b) die Mitgliedstaaten und die Organe, Einrichtungen und sonstigen Stellen der Union bei der Aufstellung und Umsetzung von Strategien für eine Offenlegung von Sicherheitslücken auf freiwilliger Basis;

c) die Organe, Einrichtungen und sonstigen Stellen der Union bei ihren Bemühungen zur Verhütung, Erkennung und Analyse von Cyberbedrohungen und Cybersicherheitsvorfällen und zur Verbesserung ihrer Fähigkeiten bei der Bewältigung derartiger Cyberbedrohungen und Cybersicherheitsvorfällen, indem sie insbesondere das CERT-EU angemessen unterstützt;

d) die Mitgliedstaaten auf deren Ersuchen beim Aufbau nationaler CSIRTs nach Artikel 9 Absatz 5 der Richtlinie (EU) 2016/1148;

e) die Mitgliedstaaten auf Ersuchen bei der Ausarbeitung nationaler Strategien für die Sicherheit von Netz- und Informationssystemen nach Artikel 7 Absatz 2 der Richtlinie (EU) 2016/1148 und fördert die unionsweite Verbreitung dieser Strategien und stellt die Fortschritte bei deren Umsetzung fest, um bewährte Verfahren bekannt zu machen;

f) die Organe der Union bei der Ausarbeitung und Überprüfung von Unionsstrategien zur Cybersicherheit, fördert deren Verbreitung und verfolgt die Fortschritte bei deren Umsetzung;

g) die CSIRTs der Mitgliedstaaten und der Union bei der Anhebung des Niveaus ihrer Fähigkeiten, auch durch die Förderung des Dialogs und Informationsaustauschs, damit jedes CSIRT entsprechend dem Stand der Technik einen gemeinsamen Bestand an Minimalfähigkeiten hat und entsprechend der bewährten Praxis arbeitet;

h) die Mitgliedstaaten durch die regelmäßige Veranstaltung der mindestens alle zwei Jahre stattfindenden Cybersicherheitsübungen auf Unionsebene nach Artikel 7 Absatz 5 und durch die Abgabe von Empfehlungen, die sie aus der Auswertung der Übungen und der bei diesen gemachten Erfahrungen ableitet;

i) einschlägige öffentliche Stellen, indem sie diesen, gegebenenfalls in Zusammenarbeit mit Interessenträgern, Fortbildungen zur Cybersicherheit anbietet;

j) die Kooperationsgruppe beim Austausch bewährter Verfahren, vor allem zur Ermittlung der Betreiber wesentlicher Dienste durch die Mitgliedstaaten nach Artikel 11 Absatz 3 Buchstabe l der Richtlinie (EU) 2016/1148, auch im Zusammenhang mit grenzüberschreitenden Abhängigkeiten, im Hinblick auf Risiken und Sicherheitsvorfälle.

(2) Die ENISA unterstützt den Informationsaustausch in und zwischen den Sektoren, vor allem in den in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren, indem sie bewährte Verfahren und Leitlinien zu den verfügbaren Instrumenten und Verfahren sowie zur Bewältigung rechtlicher Fragen im Zusammenhang mit dem Informationsaustausch bereitstellt.

Artikel 7

Operative Zusammenarbeit auf Unionsebene

(1) Die ENISA unterstützt die operative Zusammenarbeit zwischen den Mitgliedstaaten und Organen, Einrichtungen und sonstigen Stellen der Union untereinander und zwischen den Interessenträgern.

(2) Die ENISA arbeitet auf operativer Ebene mit den Organen, Einrichtungen und sonstigen Stellen der Union zusammen und entwickelt Synergien mit diesen Stellen, zu denen auch das CERT-EU sowie die für Cyberkriminalität und die Aufsicht über den Datenschutz zuständigen Stellen zählen, um Fragen von gemeinsamem Interesse anzugehen, unter anderem durch

a) den Austausch von Know-how und bewährten Verfahren;

b) die Bereitstellung von Beratung und die Veröffentlichung von Leitlinien zu einschlägigen Fragen im Zusammenhang mit der Cybersicherheit;

c) die Festlegung praktischer Modalitäten für die Wahrnehmung besonderer Aufgaben nach Konsultation der Kommission.

(3) Die ENISA führt die Sekretariatsgeschäfte des CSIRTs-Netzes nach Artikel 12 Absatz 2 der Richtlinie (EU) 2016/1148 und unterstützt in dieser Eigenschaft aktiv den Informationsaustausch und die Zusammenarbeit zwischen den Mitgliedern des CSIRTs-Netzes.

(4) Die ENISA unterstützt die Mitgliedstaaten bei der operativen Zusammenarbeit innerhalb des CSIRTs-Netzes, indem sie

a) diese berät, wie sie ihre Fähigkeiten zur Verhütung, Erkennung und Bewältigung von Sicherheitsvorfällen verbessern können, und auf Ersuchen eines oder mehrerer Mitgliedstaaten Beratung in Bezug auf eine spezifische Cyberbedrohung leistet;

b) auf Ersuchen eines oder mehrerer Mitgliedstaaten bei der Bewertung von Sicherheitsvorfällen mit beträchtlichen oder erheblichen Auswirkungen Hilfe leistet, indem sie Sachkenntnisse bereitstellt und die technische Bewältigung solcher Vorfälle erleichtert, insbesondere auch durch die Unterstützung der freiwilligen Weitergabe maßgeblicher Informationen und technischer Lösungen zwischen den Mitgliedstaaten;

c) Sicherheitslücken und Sicherheitsvorfälle auf der Grundlage von öffentlich verfügbaren Informationen oder freiwillig von den Mitgliedstaaten zu diesem Zweck bereitgestellten Informationen analysiert und

d) auf Ersuchen eines oder mehrerer Mitgliedstaaten die nachträglichen technischen Untersuchungen von Sicherheitsvorfällen mit beträchtlichen oder erheblichen Auswirkungen im Sinne der Richtlinie (EU) 2016/1148 unterstützt.

Bei der Wahrnehmung dieser Aufgaben arbeiten die ENISA und das CERT-EU in strukturierter Weise zusammen, um Synergien nutzen zu können und Doppelarbeit zu vermeiden.

(5) Die ENISA veranstaltet auf Unionsebene regelmäßig Cybersicherheitsübungen und unterstützt die Mitgliedstaaten und die Organe, Einrichtungen und sonstigen Stellen der Union auf deren Ersuchen hin bei der Organisation solcher Cybersicherheitsübungen. Diese Cybersicherheitsübungen auf Unionsebene können technische, operative oder strategische Elemente umfassen. Alle zwei Jahre veranstaltet die ENISA eine umfassende Großübung.

Die ENISA unterstützt gemeinsam mit den betreffenden Organisationen gegebenenfalls auch die Organisation sektorspezifischer Cybersicherheitsübungen, zu denen sie beiträgt, wobei diese Organisationen an den Cybersicherheitsübungen auf Unionsebene teilnehmen können.

(6) Die ENISA erstellt in enger Zusammenarbeit mit den Mitgliedstaaten regelmäßig einen eingehenden technischen EU-Cybersicherheitslagebericht über Sicherheitsvorfälle und Bedrohungen auf der Grundlage von öffentlich zugänglichen Informationen, eigenen Analysen und Berichten, die ihr unter anderem von den CSIRTs der Mitgliedstaaten () oder den zentralen Anlaufstellen im Sinne der Richtlinie (EU) 2016/1148 (in beiden Fällen auf freiwilliger Basis) sowie dem EC3 und dem CERT-EU übermittelt werden.

(7) Die ENISA trägt zur Entwicklung gemeinsamer Maßnahmen bei, mit denen auf Ebene der Union und der Mitgliedstaaten auf massive, grenzüberschreitende Cybersicherheitsvorfälle oder Cyberkrisen reagiert werden kann, indem sie insbesondere:

a) öffentlich verfügbare oder auf freiwilliger Grundlage bereitgestellte Berichte aus nationalen Quellen als Beitrag zu einer gemeinsamen Lageerfassung zusammenstellt und analysiert;

b) für einen effizienten Informationsfluss und Mechanismen sorgt, die zwischen dem CSIRTs-Netz und den fachlichen und politischen Entscheidungsträgern auf EU-Ebene eine abgestufte Vorgehensweise ermöglichen;

c) auf Ersuchen die technische Bewältigung dieser Sicherheitsvorfälle oder Krisen erleichtert, insbesondere auch durch die Unterstützung der freiwilligen Weitergabe technischer Lösungen zwischen den Mitgliedstaaten;

d) die Organe, Einrichtungen und sonstigen Stellen der Union und auf deren Ersuchen die Mitgliedstaaten bei der öffentlichen Kommunikation im Umfeld solcher Sicherheitsvorfälle oder der Krisen unterstützt;

e) die Kooperationspläne für die Reaktion auf solche Sicherheitsvorfälle oder Krisen auf Ebene der Union testet und auf deren Ersuchen die Mitgliedstaaten bei der Erprobung solcher Pläne auf nationaler Ebene unterstützt.

Artikel 8

Markt, Cybersicherheitszertifizierung und Normung

(1) Die ENISA unterstützt und fördert die Entwicklung und Umsetzung der Unionspolitik auf dem Gebiet der Cybersicherheitszertifizierung von IKT-Produkten, -Diensten und -Prozessen, wie in Titel III dieser Verordnung festgelegt, indem sie

a) die Entwicklungen in damit zusammenhängenden Normungsbereichen fortlaufend überwacht und in Fällen, in denen keine Normen zur Verfügung stehen, geeignete technische Spezifikationen für die Entwicklung europäischer Schemata für die Cybersicherheitszertifizierung nach Artikel 54 Absatz 1 Buchstabe c empfiehlt;

b) mögliche europäische Schemata für die Cybersicherheitszertifizierung (im Folgenden „mögliche Schemata“) von IKT-Produkten, -Diensten und -Prozessen nach Artikel 49 ausarbeitet;

c) angenommene europäische Schemata für die Cybersicherheitszertifizierung nach Artikel 49 Absatz 8 evaluiert;

d) sich an gegenseitigen Begutachtungen nach Artikel 59 Absatz 4 beteiligt;

e) die Kommission bei der Wahrnehmung der Sekretariatsgeschäfte der nach Artikel 62 Absatz 5 eingesetzten Europäischen Gruppe für die Cybersicherheitszertifizierung unterstützt.

(2) Die ENISA nimmt die Sekretariatsgeschäfte der nach Artikel 22 Absatz 4 eingesetzten Gruppe der Interessenträger für die Cybersicherheitszertifizierung wahr.

(3) Die ENISA stellt in Zusammenarbeit mit den nationalen Behörden für die Cybersicherheitszertifizierung und der Branche auf formelle, strukturierte und transparente Art und Weise Leitlinien zusammen und veröffentlicht diese und entwickelt bewährte Verfahren im Zusammenhang mit den Anforderungen an die Cybersicherheit von IKT-Produkten, -Diensten und -Prozessen.

(4) Die ENISA trägt zu einem hinreichenden Kapazitätsaufbau im Zusammenhang mit den Bewertungs- und Zertifizierungsverfahren bei, indem sie Leitlinien erstellt und veröffentlicht und die Mitgliedstaaten auf deren Ersuchen hin unterstützt.

(5) Die ENISA erleichtert die Ausarbeitung und Übernahme europäischer und internationaler Normen für das Risikomanagement und die Sicherheit von IKT-Produkten, -Diensten und -Prozessen.

(6) Die ENISA bietet nach Artikel 19 Absatz 2 der Richtlinie (EU) 2016/1148 in Zusammenarbeit mit den Mitgliedstaaten und der Branche Beratung an und erstellt Leitlinien für die technischen Bereiche, die sich auf die Sicherheitsanforderungen für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste beziehen, sowie für bereits vorhandene Normen, auch nationale Normen der Mitgliedstaaten.

(7) Die ENISA führt regelmäßig Analysen der wichtigsten Angebots- und Nachfragetrends auf dem Cybersicherheitsmarkt durch, um den Cybersicherheitsmarkt in der Union zu fördern.

Artikel 9

Wissen und Informationen

Die ENISA

a) führt Analysen neu entstehender Technik durch und bietet themenspezifische Bewertungen der von den technischen Innovationen zu erwartenden gesellschaftlichen, rechtlichen, wirtschaftlichen und regulatorischen Auswirkungen auf die Cybersicherheit;

b) führt langfristige strategische Analysen der Cyberbedrohungen und Sicherheitsvorfälle durch, um neu auftretende Trends erkennen und dazu beitragen zu können, Sicherheitsvorfälle zu vermeiden;

c) stellt in Zusammenarbeit mit den Sachverständigen der Behörden der Mitgliedstaaten und den maßgeblichen Interessenträgern Beratung, Leitlinien und bewährte Verfahren für die Sicherheit der Netz- und Informationssysteme zur Verfügung, vor allem für die Sicherheit der Infrastrukturen, die die in Anhang II der Richtlinie (EU) 2016/1148 aufgeführten Sektoren unterstützen, und der Infrastrukturen, die von den Anbietern der in Anhang III der genannten Richtlinie aufgeführten digitaler Dienste genutzt werden;

d) bündelt die von den Organen, Einrichtungen und sonstigen Stellen der Union bereitgestellten Informationen zur Cybersicherheit und die auf freiwilliger Grundlage von den Mitgliedstaaten und privaten und öffentlichen Interessenträgern bereitgestellten Informationen zur Cybersicherheit, ordnet diese Informationen und stellt sie über ein eigenes Portal der Öffentlichkeit zur Verfügung;

e) erhebt und analysiert öffentlich verfügbare Informationen über signifikante Sicherheitsvorfälle und stellt Berichte mit dem Ziel zusammen, den Bürgern, Organisationen und Unternehmen unionsweite Leitlinien bereitzustellen.

Artikel 10

Sensibilisierung und Ausbildung

Die ENISA

a) sensibilisiert die Öffentlichkeit für Cybersicherheitsrisiken und stellt Leitlinien für bewährte Verfahren für einzelne Nutzer zur Verfügung, die sich an Bürger, Organisationen und Unternehmen richten und auch Cyberhygiene und Cyberkompetenz umfassen;

b) organisiert in Zusammenarbeit mit den Mitgliedstaaten, den Organen, Einrichtungen und sonstigen Stellen der Union und der Branche regelmäßige Aufklärungskampagnen, um die Cybersicherheit und ihre Sichtbarkeit in der Union zu erhöhen und eine umfassende öffentliche Debatte anzuregen;

c) unterstützt die Mitgliedstaaten bei ihren Anstrengungen zur Sensibilisierung in Bezug auf Cybersicherheit und zur Förderung der Ausbildung im Bereich Cybersicherheit;

d) unterstützt die engere Koordinierung und den Austausch bewährter Verfahren zwischen den Mitgliedstaaten in Bezug auf Sensibilisierung und Ausbildung im Bereich Cybersicherheit.

Artikel 11

Forschung und Innovation

Die ENISA, in Zusammenhang mit der Forschung und Innovation,

a) berät die Organe, Einrichtungen und sonstigen Stellen der Union und die Mitgliedstaaten zum Forschungsbedarf und zu den Forschungsprioritäten im Bereich Cybersicherheit, damit die Voraussetzung für wirksame Reaktionen auf die gegenwärtigen oder sich abzeichnenden Risiken und Cyberbedrohungen, auch in Bezug auf neue und aufkommende Informations- und Kommunikationstechnologien (IKT), geschaffen und die Techniken zur Risikovermeidung genutzt werden können;

b) beteiligt sich dort, wo die Kommission ihr die einschlägigen Befugnisse übertragen hat, an der Durchführungsphase von Förderprogrammen für Forschung und Innovation oder als Begünstige;

c) trägt im Bereich der Cybersicherheit zur strategischen Forschungs- und Innovationsagenda auf Unionsebene bei.

Artikel 12

Internationale Zusammenarbeit

Die ENISA unterstützt die Bemühungen der Union um Zusammenarbeit mit Drittländern und internationalen Organisationen sowie innerhalb der einschlägigen Rahmen für internationale Zusammenarbeit, um die internationale Zusammenarbeit in Angelegenheiten der Cybersicherheit zu fördern, indem sie

a) soweit zweckmäßig — bei der Organisation von internationalen Übungen als Beobachterin mitwirkt, die Ergebnisse solcher Übungen analysiert und sie dem Verwaltungsrat vorlegt;

b) auf Ersuchen der Kommission den Austausch bewährter Verfahren erleichtert;

c) der Kommission auf deren Ersuchen mit Sachkenntnis zur Seite steht;

d) die Kommission in Zusammenarbeit mit der nach Artikel 62 eingesetzten Europäischen Gruppe für die Cybersicherheitszertifizierung bei Fragen zu Abkommen über die gegenseitige Anerkennung von Cybersicherheitszertifikaten mit Drittländern berät und unterstützt.

KAPITEL III

Organisation der ENISA

Artikel 13

Struktur der ENISA

Die Verwaltungs- und Leitungsstruktur der ENISA besteht aus

a) einem Verwaltungsrat;

b) einem Exekutivrat;

c) einem Exekutivdirektor;

d) einer EINSA-Beratungsgruppe; und

e) einem Netz der nationalen Verbindungsbeamten.

Abschnitt 1

Verwaltungsrat

Artikel 14

Zusammensetzung des Verwaltungsrats

(1) Dem Verwaltungsrat gehören je ein von jedem Mitgliedstaat ernanntes Mitglied und zwei von der Kommission ernannte Mitglieder an. Alle Mitglieder haben Stimmrecht.

(2) Jedes Mitglied des Verwaltungsrats hat einen Stellvertreter. Dieser Stellvertreter vertritt das Mitglied im Fall seiner Abwesenheit.

(3) Die Mitglieder des Verwaltungsrats und ihre Stellvertreter werden aufgrund ihrer Kenntnisse auf dem Gebiet der Cybersicherheit ernannt, wobei ihren einschlägigen Management-, Verwaltungs- und Haushaltsführungskompetenzen Rechnung zu tragen ist. Die Kommission und die Mitgliedstaaten bemühen sich, die Fluktuation bei ihren Vertretern im Verwaltungsrat gering zu halten, um die Kontinuität der Arbeit des Verwaltungsrats sicherzustellen. Die Kommission und die Mitgliedstaaten setzen sich für ein ausgewogenes Geschlechterverhältnis im Verwaltungsrat ein.

(4) Die Amtszeit der Mitglieder des Verwaltungsrats und ihrer Stellvertreter beträgt vier Jahre. Sie kann verlängert werden.

Artikel 15

Aufgaben des Verwaltungsrats

(1) Der Verwaltungsrat

a) legt die allgemeine Ausrichtung der Tätigkeit der ENISA fest und sorgt auch dafür, dass die ENISA ihre Geschäfte gemäß der in dieser Verordnung festgelegten Vorschriften und Grundsätze führt. Er sorgt zudem für die Abstimmung der Arbeit der ENISA mit den Tätigkeiten, die von den Mitgliedstaaten und auf Unionsebene durchgeführt werden;

b) nimmt den Entwurf des in Artikel 24 genannten einheitlichen Programmplanungsdokuments der ENISA an, bevor dieser der Kommission zur Stellungnahme vorgelegt wird;

c) nimmt — unter Berücksichtigung der Stellungnahme der Kommission — das einheitliche Programmplanungsdokument der ENISA an;

d) überwacht die Umsetzung der im einheitlichen Programmplanungsdokument enthaltenen mehrjährigen und jährlichen Programmplanung;

e) stellt den jährlichen Haushaltsplan der Agentur fest und übt andere Funktionen in Bezug auf den Haushalt der ENISA gemäß Kapitel IV aus;

f) bewertet und genehmigt den konsolidierten Jahresbericht über die Tätigkeiten der ENISA einschließlich des Jahresabschlusses und der Ausführungen darüber, inwiefern die ENISA die vorgegebenen Leistungsindikatoren erfüllt hat, und übermittelt den Bericht zusammen mit seiner Bewertung bis zum 1. Juli des folgenden Jahres dem Europäischen Parlament, dem Rat, der Kommission und dem Rechnungshof, und macht ihn der Öffentlichkeit zugänglich;

g) erlässt nach Artikel 32 die für die ENISA geltende Finanzregelung;

h) nimmt eine Betrugsbekämpfungsstrategie an, die den diesbezüglichen Risiken entspricht und an einer Kosten-Nutzen-Analyse der durchzuführenden Maßnahmen orientiert ist;

i) erlässt Vorschriften zur Unterbindung und Bewältigung von Interessenkonflikten bei seinen Mitgliedern;

j) sorgt ausgehend von den Erkenntnissen und Empfehlungen, die sich aus den Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) und den verschiedenen internen und externen Prüfberichten und Bewertungen ergeben haben, für angemessene Folgemaßnahmen;

k) gibt sich eine Geschäftsordnung einschließlich Regelungen zu den vorläufigen Beschlüssen zur Übertragung bestimmter Aufgaben gemäß Artikel 19 Absatz 7;

l) nimmt gemäß Absatz 2 des vorliegenden Artikels in Bezug auf das Personal der ENISA die Befugnisse wahr, die der Anstellungsbehörde durch das Statut der Beamten der Europäischen Union (im Folgenden „Statut der Beamten") bzw. der Stelle, die zum Abschluss der Dienstverträge ermächtigt ist, durch die Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Union (im Folgenden „Beschäftigungsbedingungen für die sonstigen Bediensteten der Europäischen Union") nach der Verordnung (EWG, Euratom, EGKS) Nr. 259/68 des Rates ([24]) übertragen wurden (im Folgenden „Befugnisse der Anstellungsbehörde");

m) erlässt gemäß dem Verfahren des Artikels 110 des Statuts der Beamten Durchführungsbestimmungen zum Statut der Beamten und zu den Beschäftigungsbedingungen für die sonstigen Bediensteten;

n) ernennt den Exekutivdirektor und verlängert gegebenenfalls dessen Amtszeit oder enthebt ihn nach Artikel 36 seines Amtes;

o) ernennt einen Rechnungsführer, bei dem es sich um den Rechnungsführer der Kommission handeln kann, der in der Wahrnehmung seiner Aufgaben völlig unabhängig ist;

p) fasst unter Berücksichtigung der Tätigkeitserfordernisse der ENISA und unter Beachtung der Grundsätze einer wirtschaftlichen Haushaltsführung alle Beschlüsse über die Schaffung und, falls notwendig, Änderung der Organisationsstruktur der Agentur;

q) genehmigt das Treffen von Arbeitsvereinbarungen bezüglich Artikel 7;

r) genehmigt das Treffen oder den Abschluss von Arbeitsvereinbarungen nach Artikel 42.

(2) Der Verwaltungsrat fasst gemäß nach Artikel 110 des Statuts der Beamten, einen Beschluss auf der Grundlage von Artikel 2 Absatz 1 des Statuts der Beamten und von Artikel 6 der Beschäftigungsbedingungen für die sonstigen Bediensteten, mit dem er die einschlägigen Befugnisse der Anstellungsbehörde dem Exekutivdirektor überträgt und die Bedingungen festlegt, unter denen die Befugnisübertragung ausgesetzt werden kann. Der Exekutivdirektor kann diese Befugnisse einer nachgeordneten Ebene übertragen.

([24]) Verordnung (EWG, Euratom, EGKS) Nr. 259/68 des Rates vom 29. Februar 1968 zur Festlegung des Statuts der Beamten der Europäischen Gemeinschaften und der Beschäftigungsbedingungen für die sonstigen Bediensteten dieser Gemeinschaften sowie zur Einführung von Sondermaßnahmen, die vorübergehend auf die Beamten der Kommission anwendbar sind (ABl. L 56 vom 4.3.1968, S. 1).

(3) Wenn außergewöhnliche Umstände dies erfordern, kann der Verwaltungsrat durch Beschluss die Übertragung der Befugnisse der Anstellungsbehörde auf den Exekutivdirektor sowie jegliche von diesem vorgenommene Weiterübertragung von Befugnissen der Anstellungsbehörde vorübergehend aussetzen und die Befugnisse selbst ausüben oder sie stattdessen einem seiner Mitglieder oder einem anderen Bediensteten als dem Exekutivdirektor übertragen.

Artikel 16

Vorsitz des Verwaltungsrats

Der Verwaltungsrat wählt aus dem Kreis seiner Mitglieder mit der Zweidrittelmehrheit seiner Mitglieder einen Vorsitzenden und einen stellvertretenden Vorsitzenden. Ihre Amtszeit beträgt vier Jahre, wobei eine einmalige Wiederwahl zulässig ist. Endet jedoch ihre Mitgliedschaft im Verwaltungsrat während ihrer Amtszeit, so endet auch ihre Amtszeit automatisch am selben Tag. Der stellvertretende Vorsitzende tritt im Fall der Verhinderung des Vorsitzenden von Amts wegen an dessen Stelle.

Artikel 17

Sitzungen des Verwaltungsrats

(1) Der Verwaltungsrat wird von seinem Vorsitzenden einberufen.

(2) Der Verwaltungsrat tritt mindestens zweimal jährlich zu einer ordentlichen Sitzung zusammen. Auf Antrag des Vorsitzenden, der Kommission oder mindestens eines Drittels seiner Mitglieder tritt er darüber hinaus zu außerordentlichen Sitzungen zusammen.

(3) Der Exekutivdirektor nimmt an den Sitzungen des Verwaltungsrats teil, hat jedoch kein Stimmrecht.

(4) Die Mitglieder der ENISA-Beratungsgruppe können auf Einladung des Vorsitzes an den Sitzungen des Verwaltungsrats teilnehmen, haben jedoch kein Stimmrecht.

(5) Die Mitglieder des Verwaltungsrats und ihre Stellvertreter können sich nach Maßgabe der Geschäftsordnung des Verwaltungsrats von Beratern oder Sachverständigen bei den Sitzungen des Verwaltungsrats unterstützen lassen.

(6) Die Sekretariatsgeschäfte des Verwaltungsrats werden von der ENISA wahrgenommen.

Artikel 18

Vorschriften für die Abstimmung im Verwaltungsrat

(1) Der Verwaltungsrat fasst seine Beschlüsse mit der Mehrheit seiner Mitglieder.

(2) Für die Annahme des einheitlichen Programmplanungsdokuments und des jährlichen Haushaltsplans sowie für die Ernennung, die Verlängerung der Amtszeit oder die Abberufung des Exekutivdirektors ist eine Mehrheit von zwei Dritteln der Mitglieder des Verwaltungsrats erforderlich.

(3) Jedes Mitglied hat eine Stimme. In Abwesenheit eines Mitglieds kann sein Stellvertreter das Stimmrecht des Mitglieds ausüben.

(4) Der Vorsitzende des Verwaltungsrats nimmt an den Abstimmungen teil.

(5) Der Exekutivdirektor nimmt nicht an den Abstimmungen teil.

(6) Die näheren Einzelheiten der Abstimmungsregeln, insbesondere die Voraussetzungen, unter denen ein Mitglied im Namen eines anderen Mitglieds handeln kann, werden in der Geschäftsordnung des Verwaltungsrats festgelegt.

Abschnitt 2

Exekutivrat

Artikel 19

Exekutivrat

(1) Der Verwaltungsrat wird von einem Exekutivrat unterstützt.

(2) Der Exekutivrat

a) bereitet die Beschlussvorlagen für den Verwaltungsrat vor;

b) stellt zusammen mit dem Verwaltungsrat sicher, dass ausgehend von den Ergebnissen und Empfehlungen im Rahmen der Untersuchungen des OLAF und der externen oder internen Prüfberichte und Bewertungen angemessene Folgemaßnahmen getroffen werden;

c) unterstützt und berät unbeschadet der Aufgaben des Exekutivdirektors nach Artikel 20 den Exekutivdirektor bei der Umsetzung der verwaltungs- und haushaltsbezogenen Beschlüsse des Verwaltungsrats nach Artikel 20.

(3) Der Exekutivrat besteht aus fünf Mitgliedern. Die Mitglieder des Exekutivrats werden aus den Reihen der Mitglieder des Verwaltungsrats ernannt. Eines der Mitglieder ist der Vorsitzende des Verwaltungsrats, der zugleich auch Vorsitzender des Exekutivrats sein kann, und ein weiteres ist einer der Vertreter der Kommission. Bei den Ernennungen der Mitglieder des Exekutivrats wird die Sicherstellung eines ausgewogenen Geschlechterverhältnisses im Exekutivrat angestrebt. Der Exekutivdirektor nimmt an den Sitzungen des Exekutivrats, hat jedoch kein Stimmrecht.

(4) Die Amtszeit der Mitglieder des Exekutivrats beträgt vier Jahre. Sie kann verlängert werden.

(5) Der Exekutivrat tritt mindestens einmal alle drei Monate zusammen. Der Vorsitzende des Exekutivrats beruft auf Antrag der Mitglieder zusätzliche Sitzungen ein.

(6) Der Verwaltungsrat legt die Geschäftsordnung des Exekutivrats fest.

(7) Ist dies aufgrund der Dringlichkeit notwendig, so kann der Exekutivrat im Namen des Verwaltungsrats bestimmte vorläufige Beschlüsse fassen, vor allem in Verwaltungsangelegenheiten, einschließlich der Aussetzung der Übertragung der Befugnisse der Anstellungsbehörde, und in Haushaltsangelegenheiten. über Diese vorläufigen Beschlüsse werden dem Verwaltungsrat unverzüglich mitgeteilt. Der Verwaltungsrat entscheidet sodann spätestens drei Monate, nachdem der Beschluss gefasst wurde, ob er den vorläufigen Beschluss genehmigt oder ob er ihn nicht genehmigt. Der Exekutivrat fasst keine Beschlüsse im Namen des Verwaltungsrats, die mit einer Mehrheit von zwei Dritteln der Mitglieder des Verwaltungsrats angenommen werden müssen.

Abschnitt 3

Exekutivdirektor

Artikel 20

Pflichten des Exekutivdirektors

(1) Die ENISA wird von ihrem Exekutivdirektor geleitet, der bei der Wahrnehmung seiner Aufgaben unabhängig ist. Der Exekutivdirektor ist gegenüber dem Verwaltungsrat rechenschaftspflichtig.

(2) Der Exekutivdirektor erstattet dem Europäischen Parlament über die Erfüllung seiner Aufgaben Bericht, wenn er dazu aufgefordert wird. Der Rat kann den Exekutivdirektor auffordern, über die Erfüllung seiner Aufgaben Bericht zu erstatten.

(3) Der Exekutivdirektor ist dafür verantwortlich,

a) die laufenden Geschäfte der ENISA zu führen;

b) die vom Verwaltungsrat gefassten Beschlüsse umzusetzen;

c) den Entwurf des einheitlichen Programmplanungsdokuments auszuarbeiten und dem Verwaltungsrat vor der Übermittlung an die Kommission vorzulegen;

d) das einheitliche Programmplanungsdokument umzusetzen und dem Verwaltungsrat hierüber Bericht zu erstatten;

e) den konsolidierten Jahresbericht über die Tätigkeit der ENISA, einschließlich der Umsetzung des jährlichen Arbeitsprogramms der ENISA, auszuarbeiten und dem Verwaltungsrat zur Bewertung und Annahme vorzulegen;

f) einen Aktionsplan mit Folgemaßnahmen zu den Schlussfolgerungen der nachträglichen Bewertungen auszuarbeiten und alle zwei Jahre der Kommission über die erzielten Fortschritte Bericht zu erstatten;

g) einen Aktionsplan mit Folgemaßnahmen zu den Schlussfolgerungen interner oder externer Prüfberichte sowie der Untersuchungen des OLAF auszuarbeiten und der Kommission zweimal jährlich und dem Verwaltungsrat regelmäßig über die erzielten Fortschritte Bericht zu erstatten;

h) den Entwurf der für die ENISA geltenden Finanzregelung nach Artikel 32 auszuarbeiten;

i) den Entwurf des Voranschlags der Einnahmen und Ausgaben der ENISA auszuarbeiten und ihren Haushaltsplan auszuführen;

j) die finanziellen Interessen der Union durch vorbeugende Maßnahmen gegen Betrug, Korruption und sonstige rechtswidrige Handlungen, durch wirksame Kontrollen und, falls Unregelmäßigkeiten festgestellt werden, durch Einziehung zu Unrecht gezahlter Beträge sowie gegebenenfalls durch Verhängung wirksamer, verhältnismäßiger und abschreckender verwaltungsrechtlicher und finanzieller Sanktionen zu schützen;

k) eine Betrugsbekämpfungsstrategie für die ENISA auszuarbeiten und dem Verwaltungsrat zur Genehmigung vorzulegen;

l) Kontakte zur Wirtschaft und zu Verbraucherorganisationen im Hinblick auf einen regelmäßigen Dialog mit den einschlägigen Interessenträgern aufzubauen und zu pflegen;

m) einen regelmäßigen Gedanken- und Informationsaustausch mit den Organen, Einrichtungen und sonstigen Stellen der Union über deren Tätigkeiten im Bereich Cybersicherheit zu führen, um die Kohärenz bei der Weiterentwicklung und Umsetzung der Unionspolitik sicherzustellen;

n) sonstige dem Exekutivdirektor durch diese Verordnung übertragene Aufgaben wahrzunehmen.

(4) Soweit erforderlich sowie entsprechend den Zielen und Aufgaben der ENISA kann der Exekutivdirektor der ENISA Ad-hoc-Arbeitsgruppen aus Sachverständigen — auch von den zuständigen Behörden der Mitgliedstaaten — einsetzen. Der Exekutivdirektor unterrichtet den Verwaltungsrat hiervon vorab. Die Verfahren, die insbesondere die Zusammensetzung dieser Arbeitsgruppen, die Bestellung der Sachverständigen der Arbeitsgruppen durch den Exekutivdirektor und die Arbeitsweise der Arbeitsgruppen betreffen, werden in den internen Verfahrensvorschriften der ENISA festgelegt.

(5) Der Exekutivdirektor kann auf der Grundlage einer angemessenen Kosten-Nutzen-Analyse erforderlichenfalls beschließen, eine oder mehrere Außenstellen in einem oder mehreren Mitgliedstaaten einzurichten, damit die ENISA ihre Aufgaben effizient und wirksam wahrnehmen kann. Bevor er über die Einrichtung einer Außenstelle beschließt, ersucht der Exekutivdirektor den/die betreffenden Mitgliedstaat(en), einschließlich des Mitgliedstaats, in dem die ENISA ihren Sitz hat, um eine Stellungnahme, und er holt die vorherige Zustimmung der Kommission und des Verwaltungsrats ein. Im Falle von Meinungsverschiedenheiten bei der Konsultation zwischen dem Exekutivdirektor und den betreffenden Mitgliedstaaten werden die strittigen Fragen dem Rat zur Erörterung vorgelegt. Die Gesamtzahl der Mitarbeiter in allen Außenstellen ist möglichst gering zu halten und darf insgesamt nicht 40 % der Gesamtzahl der Mitarbeiter der ENISA ii dem Mitgliedstaat, in dem die ENISA ihren Sitz hat, überschreiten. Die Anzahl der Mitarbeiter in jeder Außenstelle darf nicht 10 % der Gesamtzahl der Mitarbeiter der Agentur im Mitgliedstaat, in dem die ENISA ihren Sitz hat, überschreiten.

In dem Beschluss zur Einrichtung einer Außenstelle wird der Umfang der in der Außenstelle auszuübenden Tätigkeiten so festgelegt, dass unnötige Kosten und eine Überschneidung der Verwaltungsfunktionen mit denen der ENISA vermieden werden.

Abschnitt 4

ENISA-Beratungsgruppe, Gruppe der Interessenträger für die Cybersicherheitszertifizierung und Netz der nationalen Verbindungsbeamten

Artikel 21

ENISA-Beratungsgruppe

(1) Der Verwaltungsrat setzt auf Vorschlag des Exekutivdirektors auf transparente Art und Weise eine ENISA-Beratungsgruppe ein, die sich aus anerkannten Sachverständigen als Vertreter der einschlägigen Interessenträger zusammensetzt, darunter die IKT-Branche, Anbieter öffentlich zugänglicher elektronischer Kommunikationsnetze oder -dienste, KMU, Betreiber wesentlicher Dienste, Verbrauchergruppen, wissenschaftliche Sachverständige aus dem Bereich der Cybersicherheit sowie Vertreter der zuständigen Behörden, die nach der Richtlinie (EU) 2018/1972 notifiziert wurden, europäische Normungsorganisationen sowie Strafverfolgungsbehörden und Datenschutz-Aufsichtsbehörden. Der Verwaltungsrat strebt ein angemessenes Gleichgewicht zwischen den Geschlechtern, ein angemessenes geographisches Gleichgewicht und ein angemessenes Gleichgewicht zwischen den verschiedenen Interessengruppen an.

(2) Die Verfahren für die ENISA-Beratungsgruppe, die insbesondere ihre Zusammensetzung, den Vorschlag des in Absatz 1 genannten Exekutivdirektors, die Anzahl und die Ernennung der Mitglieder und die Arbeitsweise der ENISA-Beratungsgruppe betreffen, werden in den internen Verfahrensvorschriften der ENISA festgelegt und öffentlich bekannt gemacht.

(3) Den Vorsitz der ENISA-Beratungsgruppe führt der Exekutivdirektor oder eine jeweils vom Exekutivdirektor ernannte Person.

(4) Die Amtszeit der Mitglieder der ENISA-Beratungsgruppe beträgt zweieinhalb Jahre. Mitglieder des Verwaltungsrats dürfen nicht Mitglieder der ENISA-Beratungsgruppe sein. Sachverständige der Kommission und aus den Mitgliedstaaten können an den Sitzungen der ENISA-Beratungsgruppe teilnehmen und an ihrer Arbeit mitwirken. Vertreter anderer Stellen, die vom Exekutivdirektor für relevant erachtet werden und die der ENISA-Beratungsgruppe nicht angehören, können zur Teilnahme an den Sitzungen der ENISA-Beratungsgruppe und zur Mitarbeit an ihrer Arbeit eingeladen werden.

(5) Die ENISA-Beratungsgruppe berät die ENISA bei der Durchführung ihrer Aufgaben, ausgenommen der Anwendung der Bestimmungen des Titels III dieser Verordnung. Sie berät insbesondere den Exekutivdirektor bei der Ausarbeitung eines Vorschlags für das Jahresarbeitsprogramms der ENISA und bei der Sicherstellung der Kommunikation mit den einschlägigen Interessenträgern bezüglich Fragen im Zusammenhang mit dem Jahresarbeitsprogramm.

(6) Die ENISA-Beratungsgruppe unterrichtet den Verwaltungsrat regelmäßig über ihre Tätigkeiten.

Artikel 22

Gruppe der Interessenträger für die Cybersicherheitszertifizierung

(1) Es wird eine Gruppe der Interessenträger für die Cybersicherheitszertifizierung eingesetzt.

(2) Die Mitglieder der Gruppe der Interessenträger für die Cybersicherheitszertifizierung werden unter anerkannten Sachverständigen als Vertreter der einschlägigen Interessenträger ausgewählt. Die Kommission wählt die Mitglieder der Gruppe der Interessenträger für die Cybersicherheitszertifizierung auf Vorschlag der ENISA im Wege eines transparenten und offenen Auswahlverfahrens aus, durch das ein Gleichgewicht zwischen den verschiedenen Interessengruppen sowie ein angemessenes Gleichgewicht zwischen den Geschlechtern und ein angemessenes geographisches Gleichgewicht sichergestellt wird.

(3) Die Gruppe der Interessenträger für die Cybersicherheitszertifizierung:

a) berät die Kommission in strategischen Fragen im Zusammenhang mit dem europäischen Rahmen für die Cybersicherheitszertifizierung;

b) berät auf Ersuchen die ENISA in allgemeinen und strategischen Fragen im Zusammenhang mit den Aufgaben der ENISA in Bezug auf den Markt, die Cybersicherheitszertifizierung und die Normung;

c) unterstützt die Kommission bei der Ausarbeitung des in Artikel 47 genannten fortlaufenden Arbeitsprogramms der Union;

d) nimmt zum fortlaufenden Arbeitsprogramm der Union gemäß Artikel 47 Absatz 4 Stellung und

e) berät in dringenden Fällen die Kommission und die Europäische Gruppe für die Cybersicherheitszertifizierung in Bezug auf die Notwendigkeit zusätzlicher Zertifizierungsschemata, die nicht Teil des fortlaufenden Arbeitsprogramms der Union sind, wie in Artikel 47 und 48 beschrieben.

(4) Den Vorsitz der Gruppe der Interessenträger für die Cybersicherheitszertifizierung führen die Vertreter der Kommission und der ENISA gemeinsam, und die Sekretariatsgeschäfte werden von der ENISA wahrgenommen.

Artikel 23

Netz der nationalen Verbindungsbeamten

(1) Der Verwaltungsrat richtet auf Vorschlag des Exekutivdirektors ein Netz der nationalen Verbindungsbeamten ein, das sich aus Vertretern der Mitgliedstaaten zusammensetzt (im Folgenden „nationale Verbindungsbeamten"). Jeder Mitgliedstaat ernennt einen Vertreter im Netz der nationalen Verbindungsbeamten. Die Sitzungen des Netzes der nationalen Verbindungsbeamten können in verschiedenen Sachverständigenzusammensetzungen abgehalten werden.

(2) Das Netz der nationalen Verbindungsbeamten erleichtert vor allem den Informationsaustausch zwischen der ENISA und den Mitgliedstaaten und unterstützt die ENISA dabei, ihre Tätigkeiten, Erkenntnisse und Empfehlungen bei den einschlägigen Interessenträgern in der gesamten Union bekannt zu machen.

(3) Die nationalen Verbindungsbeamten dienen als Kontaktstelle auf nationaler Ebene, um die Zusammenarbeit zwischen der ENISA und den nationalen Sachverständigen im Rahmen der Durchführung des Jahresarbeitsprogramms der ENISA zu erleichtern.

(4) Während die nationalen Verbindungsbeamten eng mit den Vertretern ihres jeweiligen Mitgliedstaats im Verwaltungsrat zusammenarbeiten, darf das Netz der nationalen Verbindungsbeamten selbst nicht dieselbe Arbeit leisten wie der Verwaltungsrat oder andere Gremien der Union.

(5) Die Funktionen und Verfahren des Netzes der nationalen Verbindungsbeamten werden in den internen Verfahrensvorschriften der ENISA festgelegt und der Öffentlichkeit zugänglich gemacht.

Abschnitt 5

Arbeitsweise

Artikel 24

Einheitliches Programmplanungsdokument

(1) Die ENISA führt ihre Geschäfte in Übereinstimmung mit einem einheitlichen Programmplanungsdokument, das ihre jährliche und mehrjährige Programmplanung mit allen ihren geplanten Tätigkeiten enthält.

(2) Jedes Jahr erstellt der Exekutivdirektor einen Entwurf des einheitlichen Programmplanungsdokuments mit der jährlichen und mehrjährigen Programmplanung und der entsprechenden Finanz- und Personalplanung nach Artikel 32 der Delegierten Verordnung (EU) Nr. 1271/2013 der Kommission ([25]) und unter Berücksichtigung der von der Kommission festgelegten Leitlinien.

(3) Bis zum 30. November eines jeden Jahres nimmt der Verwaltungsrat das in Absatz 1 genannte einheitliche Programmplanungsdokument an und übermittelt es bis zum 31. Januar des Folgejahres dem Europäischen Parlament, dem Rat und der Kommission, sowie jede spätere Aktualisierung dieses Dokuments.

(4) Das einheitliche Programmplanungsdokument wird nach der endgültigen Feststellung des Gesamthaushaltsplans der Union endgültig und ist erforderlichenfalls entsprechend anzupassen.

([25]) Delegierte Verordnung (EU) Nr. 1271/2013 der Kommission vom 30. September 2013 über die Rahmenfinanzregelung für Einrichtungen gemäß Artikel 208 der Verordnung (EU, Euratom) Nr. 966/2012 des Europäischen Parlaments und des Rates (ABl. L 328 vom 7.12.2013, S. 42).

(5) Das Jahresarbeitsprogramm enthält detaillierte Ziele und Angaben zu den erwarteten Ergebnissen, einschließlich Erfolgsindikatoren. Es enthält zudem eine Beschreibung der zu finanzierenden Maßnahmen sowie Angaben zur Höhe der für die einzelnen Maßnahmen vorgesehenen finanziellen und personellen Ressourcen gemäß den Grundsätzen der maßnahmenbezogenen Aufstellung des Haushaltsplans und des maßnahmenbezogenen Managements. Das Jahresarbeitsprogramm muss mit dem mehrjährigen Arbeitsprogramm nach Absatz 7 im Einklang stehen. Es ist klar darin anzugeben, welche Aufgaben im Vergleich zum vorangegangenen Haushaltsjahr hinzugefügt, verändert oder gestrichen wurden.

(6) Der Verwaltungsrat ändert das angenommene Jahresarbeitsprogramm, wenn der ENISA eine neue Aufgabe übertragen wird. Wesentliche Änderungen des jährlichen Arbeitsprogramms werden nach demselben Verfahren angenommen wie das ursprüngliche jährliche Arbeitsprogramm. Der Verwaltungsrat kann dem Exekutivdirektor die Befugnis übertragen, nicht wesentliche Änderungen am Jahresarbeitsprogramm vorzunehmen.

(7) Im mehrjährigen Arbeitsprogramm der Agentur wird die strategische Gesamtplanung einschließlich der Ziele, erwarteten Ergebnisse und Leistungsindikatoren festgelegt. Es umfasst auch die Ressourcenplanung mit einem mehrjährigen Finanz- und Personalplan.

(8) Die Ressourcenplanung wird jährlich aktualisiert. Die strategische Programmplanung ist zu aktualisieren, wann immer dies geboten erscheint und insbesondere, wenn dies notwendig ist, um dem Ergebnis der in Artikel 67 genannten Bewertung Rechnung zu tragen.

Artikel 25

Interessenerklärung

(1) Die Mitglieder des Verwaltungsrats, der Exekutivdirektor und die von den Mitgliedstaaten auf Zeit abgeordneten Beamten geben eine Verpflichtungserklärung und eine Interessenerklärung ab, aus der hervorgeht, ob direkte oder indirekte Interessen bestehen, die ihre Unabhängigkeit beeinträchtigen könnten. Die Erklärungen müssen der Wahrheit entsprechen und vollständig sein; sie werden jedes Jahr schriftlich abgegeben und, wann immer erforderlich, aktualisiert.

(2) Die Mitglieder des Verwaltungsrats, der Exekutivdirektor und externe Sachverständige, die in den Ad-hoc-Arbeitsgruppen mitwirken, geben spätestens zu Beginn jeder Sitzung eine wahrheitsgetreue und vollständige Erklärung über alle Interessen ab, die ihre Unabhängigkeit in Bezug auf die Tagesordnungspunkte beeinträchtigen könnten, und beteiligen sich nicht an den Diskussionen und den Abstimmungen über solche Punkte.

(3) Die ENISA legt in ihren internen Verfahrensvorschriften die praktischen Einzelheiten der Vorschriften über Interessenerklärungen nach den Absätzen 1 und 2 fest.

Artikel 26

Transparenz

(1) Die ENISA übt ihre Tätigkeiten mit einem hohen Maß an Transparenz und im Einklang mit Artikel 28 aus.

(2) Die ENISA stellt sicher, dass die Öffentlichkeit sowie interessierte Kreise angemessene, objektive, zuverlässige und leicht zugängliche Informationen, insbesondere zu ihren eigenen Arbeitsergebnissen, erhalten. Ferner veröffentlicht sie die nach Artikel 25 abgegebenen Interessenerklärungen.

(3) Der Verwaltungsrat kann auf Vorschlag des Exekutivdirektors gestatten, dass interessierte Kreise als Beobachter an bestimmten Tätigkeiten der ENISA teilnehmen.

(4) Die ENISA legt in ihren internen Verfahrensvorschriften die praktischen Einzelheiten für die Anwendung der in den Absätzen 1 und 2 genannten Transparenzregelungen fest.

Artikel 27

Vertraulichkeit

(1) Unbeschadet des Artikels 28 gibt die Agentur Informationen, die bei ihr eingehen oder von ihr verarbeitet werden und die auf begründetes Ersuchen vertraulich behandelt werden sollen, nicht an Dritte weiter.

(2) Die Mitglieder des Verwaltungsrats, der Exekutivdirektor, die Mitglieder der ENISA-Beratungsgruppe, die externen Sachverständigen der Ad-hoc-Arbeitsgruppen sowie das Personal der ENISA, einschließlich der von den Mitgliedstaaten auf Zeit abgeordneten Beamten, unterliegen auch nach Beendigung ihrer Tätigkeit den Vertraulichkeitsbestimmungen des Artikels 339 AEUV.

(3) Die ENISA legt in ihren internen Verfahrensvorschriften die praktischen Einzelheiten für die Anwendung der in den Absätzen 1 und 2 genannten Vertraulichkeitsregelungen fest.

(4) Soweit es zur Erfüllung der Aufgaben der ENISA erforderlich ist, beschließt der Verwaltungsrat, die ENISA zum Umgang mit Verschlusssachen zu ermächtigen. In diesem Fall nimmt die ENISA im Einvernehmen mit den Dienststellen der Kommission Sicherheitsvorschriften zur Anwendung der Sicherheitsgrundsätze an, die in den Beschlüssen (EU, Euratom) 2015/443 ([26]) und (EU, Euratom) 2015/444 ([27]) der Kommission festgelegt sind. Diese Sicherheitsvorschriften betreffen unter anderem die Bestimmungen über den Austausch, die Verarbeitung und die Speicherung von Verschlusssachen.

Artikel 28

Zugang zu Dokumenten

(1) Die Verordnung (EG) Nr. 1049/2001 findet Anwendung auf die Dokumente der ENISA.

(2) Der Verwaltungsrat legt bis zum 28. Dezember 2019 Maßnahmen zur Durchführung der Verordnung (EG) Nr. 1049/2001 fest.

(3) Gegen Entscheidungen der ENISA gemäß Artikel 8 der Verordnung (EG) Nr. 1049/2001 kann nach Maßgabe des Artikels 228 AEUV bzw. 263 AEUV Beschwerde beim Europäischen Bürgerbeauftragten eingelegt oder Klage beim Gerichtshof der Europäischen Union erhoben werden.

KAPITEL IV

Aufstellung und Gliederung des Haushaltsplans der ENISA

Artikel 29

Aufstellung des Haushaltsplans der ENISA

(1) Der Exekutivdirektor erstellt jedes Jahr den Entwurf des Voranschlags der Einnahmen und Ausgaben der ENISA für das folgende Haushaltsjahr und übermittelt ihn dem Verwaltungsrat zusammen mit dem Entwurf des Stellenplans vor. Einnahmen und Ausgaben müssen ausgeglichen sein.

(2) Der Verwaltungsrat erstellt jedes Jahr auf der Grundlage des Entwurfs des Voranschlags einen Voranschlag der Einnahmen und Ausgaben der ENISA für das folgende Haushaltsjahr.

(3) Der Verwaltungsrat übermittelt jedes Jahr bis zum 31. Januar der Kommission und den Drittländern, mit denen die Union Abkommen nach Artikel 42 Absatz 2 geschlossen hat, den Voranschlag, der Teil des Entwurfs des einheitlichen Programmplanungsdokuments ist.

(4) Die Kommission setzt aufgrund dieses Voranschlags die von ihr für erforderlich erachteten Mittelansätze für den Stellenplan und den Betrag des Zuschusses aus dem Gesamthaushaltsplan der Union in den Haushaltsplanentwurf der Union ein, den sie nach Artikel 314 AEUV dem Europäischen Parlament und dem Rat vorlegt.

(5) Das Europäische Parlament und der Rat bewilligen die Mittel für den Beitrag der Union für die ENISA.

(6) Das Europäische Parlament und der Rat legen den Stellenplan der ENISA fest.

([26]) Beschluss (EU, Euratom) 2015/443 der Kommission vom 13. März 2015 über Sicherheit in der Kommission (ABl. L 72 vom 17.3.2015, S. 41).

([27]) Beschluss (EU, Euratom) 2015/444 der Kommission vom 13. März 2015 über die Sicherheitsvorschriften für den Schutz von EU-Verschlusssachen (ABl. L 72 vom 17.3.2015, S. 53).

(7) Der Haushaltsplan der ENISA wird zusammen mit dem einheitlichen Programmplanungsdokument vom Verwaltungsrat angenommen. Der Haushaltsplan der ENISA wird endgültig, sobald der Gesamthaushaltsplan der Union endgültig festgestellt ist. Erforderlichenfalls nimmt der Verwaltungsrat eine Anpassung des Haushaltsplans der ENISA und des einheitlichen Programmplanungsdokuments entsprechend dem Gesamthaushaltsplan der Union vor.

Artikel 30

Gliederung des Haushaltsplans der ENISA

(1) Unbeschadet sonstiger Ressourcen gliedern sich die Einnahmen der ENISA wie folgt:

a) ein Beitrag aus dem Gesamthaushalt der Union;

b) Einnahmen, die konkreten Ausgabenpositionen im Einklang mit der in Artikel 32 genannten Finanzregelung zugewiesen werden;

c) Unionsmittel in Form von Übertragungsvereinbarungen oder Ad-hoc-Finanzhilfen im Einklang mit der in Artikel 32 genannten Finanzregelung der Agentur und den Bestimmungen der einschlägigen Instrumente zur Unterstützung der Unionspolitik;

d) Beiträge von Drittländern, die sich nach Artikel 42 an der Arbeit der ENISA beteiligen;

e) freiwillige Zahlungen oder Sachleistungen von Mitgliedstaaten.

Mitgliedstaaten, die einen freiwilligen Beitrag nach Unterabsatz 1 Buchstabe e leisten, können aufgrund dessen keine bestimmten Rechte oder Dienstleistungen beanspruchen.

(2) Die Ausgaben der ENISA umfassen Aufwendungen für Personal, Verwaltung, technische Unterstützung, Infrastruktur, Betriebskosten und Ausgaben, die sich aus Verträgen mit Dritten ergeben.

Artikel 31

Ausführung des Haushaltsplans der ENISA

(1) Der Exekutivdirektor trägt die Verantwortung für die Ausführung des Haushaltsplans der ENISA.

(2) Der interne Rechnungsprüfer der Kommission übt gegenüber der ENISA dieselben Befugnisse wie gegenüber den Kommissionsdienststellen aus.

(3) Bis zum 1. März des jeweils folgenden Haushaltsjahres (1. März des Jahres n+1) übermittelt der Rechnungsführer der Agentur dem Rechnungsführer der Kommission und dem Rechnungshof den vorläufigen Jahresabschluss für das Haushaltsjahr (Jahr n).

(4) Nach Eingang der Bemerkungen des Rechnungshofes zum vorläufigen Jahresabschluss der ENISA gemäß Artikel 246 der Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates ([28]), erstellt der Rechnungsführer in eigener Verantwortung den endgültigen Jahresabschluss der ENISA und legt ihn dem Verwaltungsrat zur Stellungnahme vor.

(5) Der Verwaltungsrat gibt eine Stellungnahme zu den endgültigen Jahresabschlüssen der ENISA ab.

(6) Bis zum 31. März des Jahres n+1 übermittelt der Exekutivdirektor den Bericht über die Haushaltsführung und das Finanzmanagement dem Europäischen Parlament, dem Rat, der Kommission und dem Rechnungshof.

(7) Bis zum 1. Juli des Jahres n+1 übermittelt der Rechnungsführer der ENISA den endgültigen Jahresabschluss zusammen mit der Stellungnahme des Verwaltungsrats dem Europäischen Parlament, dem Rat, dem Rechnungsführer der Kommission und dem Rechnungshof.

([28]) Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates vom 18. Juli 2018 über die Haushaltsordnung für den Gesamthaushaltsplan der Union, zur Änderung der Verordnungen (EU) Nr. 1296/2013, (EU) Nr. 1301/2013, (EU) Nr. 1303/2013, (EU) Nr. 1304/2013, (EU) Nr. 1309/2013, (EU) Nr. 1316/2013, (EU) Nr. 223/2014, (EU) Nr. 283/2014 und des Beschlusses Nr. 541/2014/EU sowie zur Aufhebung der Verordnung (EU, Euratom) Nr. 966/2012 (ABl. L 193 vom 30.7.2018, S. 1).

(8) Gleichzeitig mit der Übermittlung des endgültigen Jahresabschlusses der ENISA leitet der Rechnungsführer der ENISA auch dem Rechnungshof eine Erklärung über die Vollständigkeit dieses endgültigen Jahresabschlusses mit Kopie an den Rechnungsführer der Kommission zu.

(9) Bis zum 15. November des Jahres n+1 veröffentlicht der Exekutivdirektor den endgültigen Jahresabschluss im *Amtsblatt der Europäischen Union*.

(10) Bis zum 30. September des Jahres n+1 übermittelt der Exekutivdirektor dem Rechnungshof eine Antwort auf dessen Bemerkungen und leitet eine Kopie dieser Antwort auch dem Verwaltungsrat und der Kommission zu.

(11) Der Exekutivdirektor unterbreitet dem Europäischen Parlament auf dessen Ersuchen nach Artikel 261 Absatz 3 der Verordnung (EU, Euratom) 2018/1046 alle für ein reibungsloses Entlastungsverfahren für das betreffende Haushaltsjahr notwendigen Informationen.

(12) Auf Empfehlung des Rates erteilt das Europäische Parlament dem Direktor vor dem 15. Mai des Jahres n+2 Entlastung zur Ausführung des Haushaltsplans für das Jahr n.

Artikel 32

Finanzregelung

Der Verwaltungsrat erlässt nach Konsultation der Kommission die für die ENISA geltende Finanzregelung. Die Finanzregelung darf von der Delegierten Verordnung (EU) Nr. 1271/2013 nur abweichen, wenn dies für den Betrieb der ENISA eigens erforderlich ist und die Kommission vorher ihre Zustimmung erteilt hat.

Artikel 33

Betrugsbekämpfung

(1) Zur Erleichterung der Bekämpfung von Betrug, Korruption und sonstigen rechtswidrigen Handlungen gemäß der Verordnung (EU, Euratom) Nr. 883/2013 des Europäischen Parlaments und des Rates ([29]) tritt die ENISA bis zum 28. Dezember 2019 der Interinstitutionellen Vereinbarung vom 25. Mai 1999 zwischen dem Europäischen Parlament, dem Rat der Europäischen Union und der Kommission der Europäischen Gemeinschaften über die internen Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) ([30]) bei. Die ENISA erlässt die einschlägigen Vorschriften, die für sämtliche Mitarbeiter der ENISA gelten, nach dem Muster im Anhang der genannten Vereinbarung.

(2) Der Rechnungshof ist befugt, bei allen Empfängern von Finanzhilfen sowie bei Auftragnehmern und Unterauftragnehmern, die Unionsmittel von der ENISA erhalten haben, Rechnungsprüfungen anhand von Belegkontrollen und Kontrollen vor Ort durchzuführen.

(3) Das OLAF kann gemäß den Bestimmungen und Verfahren der Verordnung (EU, Euratom) Nr. 883/2013 und der Verordnung (Euratom, EG) Nr. 2185/96 des Rates ([31]) Untersuchungen, einschließlich Kontrollen und Überprüfungen vor Ort, durchführen, um festzustellen, ob im Zusammenhang mit von der ENISA gewährten Finanzhilfen oder von ihr finanzierten Aufträgen ein Betrugs- oder Korruptionsdelikt oder eine sonstige rechtswidrige Handlung zum Nachteil der finanziellen Interessen der Union vorliegt.

(4) Unbeschadet der Absätze 1, 2 und 3 müssen Kooperationsvereinbarungen mit Drittländern oder internationalen Organisationen, Verträge, Finanzhilfevereinbarungen und Finanzhilfebeschlüsse der ENISA Bestimmungen enthalten, die den Rechnungshof und das OLAF ausdrücklich ermächtigen, derartige Rechnungsprüfungen und Untersuchungen im Rahmen ihrer jeweiligen Zuständigkeiten durchzuführen.

([29]) Verordnung (EU, Euratom) Nr. 883/2013 des Europäischen Parlaments und des Rates vom 11. September 2013 über die Untersuchungen des Europäischen Amtes für Betrugsbekämpfung (OLAF) und zur Aufhebung der Verordnung (EG) Nr. 1073/1999 des Europäischen Parlaments und des Rates und der Verordnung (Euratom) Nr. 1074/1999 des Rates (ABl. L 248 vom 18.9.2013, S. 1).
([30]) ABl. L 136 vom 31.5.1999, S. 15.
([31]) Verordnung (Euratom, EG) Nr. 2185/96 des Rates vom 11. November 1996 betreffend die Kontrollen und Überprüfungen vor Ort durch die Kommission zum Schutz der finanziellen Interessen der Europäischen Gemeinschaften vor Betrug und anderen Unregelmäßigkeiten (ABl. L 292 vom 15.11.1996, S. 2).

KAPITEL V

Personal

Artikel 34

Allgemeine Bestimmungen

Für das Personal der ENISA gelten das Statut der Beamten, die Beschäftigungsbedingungen für die sonstigen Bediensteten sowie die im gegenseitigen Einvernehmen der Organe der Union erlassenen Regelungen zur Durchführung der Bestimmungen des Statuts der Beamten und der Beschäftigungsbedingungen für die sonstigen Bediensteten.

Artikel 35

Vorrechte und Befreiungen

Das dem EUV und dem AEUV beigefügte Protokoll Nr. 7 über die Vorrechte und Befreiungen der Europäischen Union findet auf die ENISA und ihr Personal Anwendung.

Artikel 36

Exekutivdirektor

(1) Der Exekutivdirektor wird als Zeitbediensteter der ENISA nach Artikel 2 Buchstabe a der Beschäftigungsbedingungen für die sonstigen Bediensteten eingestellt.

(2) Der Exekutivdirektor wird vom Verwaltungsrat aus einer Liste von Kandidaten, die die Kommission im Anschluss an ein offenes und transparentes Auswahlverfahren vorgeschlagen hat, ernannt.

(3) Beim Abschluss des Arbeitsvertrags des Exekutivdirektors wird die ENISA durch den Vorsitzenden des Verwaltungsrats vertreten.

(4) Vor der Ernennung wird der vom Verwaltungsrat ausgewählte Kandidat aufgefordert, eine Erklärung vor dem zuständigen Ausschuss des Europäischen Parlaments abzugeben und Fragen der Mitglieder zu beantworten.

(5) Die Amtszeit des Exekutivdirektors beträgt fünf Jahre. Zum Ende dieses Zeitraums nimmt die Kommission eine Bewertung der Leistung des Exekutivdirektors und der künftigen Aufgaben und Herausforderungen der ENISA vor.

(6) Der Verwaltungsrat beschließt über die Ernennung, die Verlängerung der Amtszeit oder die Abberufung des Exekutivdirektors gemäß Artikel 18 Absatz 2.

(7) Der Verwaltungsrat kann auf Vorschlag der Kommission unter Berücksichtigung der Bewertung nach Absatz 5 die Amtszeit des Exekutivdirektors einmal um fünf Jahre verlängern.

(8) Der Verwaltungsrat unterrichtet das Europäische Parlament über seine Absicht, die Amtszeit des Exekutivdirektors zu verlängern. Innerhalb von drei Monaten vor der Verlängerung der Amtszeit gibt der Exekutivdirektor, sofern er dazu aufgefordert wird, vor dem zuständigen Ausschuss des Europäischen Parlaments eine Erklärung ab und beantwortet Fragen der Mitglieder.

(9) Ein Exekutivdirektor, dessen Amtszeit verlängert wurde, nimmt nicht an einem anderen Auswahlverfahren für dieselbe Stelle teil.

(10) Der Exekutivdirektor kann nur durch einen Beschluss des Verwaltungsrats auf Vorschlag der Kommission seines Amtes enthoben werden.

Artikel 37

Abgeordnete nationale Sachverständige und sonstiges Personal

(1) Die ENISA kann auf abgeordnete nationale Sachverständige oder sonstiges Personal zurückgreifen, das nicht von der ENISA selbst beschäftigt wird. Für dieses Personal gelten das Statut der Beamten und die Beschäftigungsbedingungen für die sonstigen Bediensteten nicht.

(2) Der Verwaltungsrat beschließt eine Regelung über zur ENISA abgeordnete nationale Sachverständige.

KAPITEL VI

Allgemeine Bestimmungen für die ENISA

Artikel 38

Rechtsform der ENISA

(1) Die ENISA ist eine Einrichtung der Union und besitzt Rechtspersönlichkeit.

(2) Die ENISA besitzt in jedem Mitgliedstaat die weitestgehende Rechts- und Geschäftsfähigkeit, die juristischen Personen nach nationalem Recht zuerkannt ist. Sie kann insbesondere bewegliches und unbewegliches Vermögen erwerben oder veräußern und ist vor Gericht parteifähig.

(3) Die ENISA wird vom Exekutivdirektor vertreten.

Artikel 39

Haftung der ENISA

(1) Die vertragliche Haftung der ENISA bestimmt sich nach dem für den betreffenden Vertrag geltenden Recht.

(2) Für Entscheidungen aufgrund einer Schiedsklausel in einem von der ENISA geschlossenen Vertrag ist der Gerichtshof der Europäischen Union zuständig.

(3) Im Bereich der außervertraglichen Haftung ersetzt die ENISA den durch sie selbst oder ihre Bediensteten in Ausübung ihrer Tätigkeit verursachten Schaden nach den allgemeinen Grundsätzen, die den Rechten der Mitgliedstaaten gemeinsam sind.

(4) In Streitsachen über den Schadensersatz gemäß Absatz 3 ist der Gerichtshof der Europäischen Union zuständig.

(5) Die persönliche Haftung der Bediensteten der ENISA gegenüber der ENISA bestimmt sich nach den für die Bediensteten der ENISA geltenden Beschäftigungsbedingungen.

Artikel 40

Sprachenregelung

(1) Für die ENISA gilt die Verordnung Nr. 1 des Rates ([32]). Die Mitgliedstaaten und die anderen von den Mitgliedstaaten benannten Einrichtungen können sich in einer der Amtssprachen der Organe der Union ihrer Wahl an die ENISA wenden und erhalten eine Antwort in dieser Sprache.

(2) Die für die Arbeit der ENISA erforderlichen Übersetzungsdienste werden vom Übersetzungszentrum für die Einrichtungen der Europäischen Union erbracht.

Artikel 41

Schutz personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten durch die ENISA unterliegt der Verordnung (EU) 2018/1725.

(2) Der Verwaltungsrat beschließt die Durchführungsvorschriften gemäß Artikel 45 Absatz 3 der Verordnung (EU) 2018/1725. Der Verwaltungsrat kann zusätzliche Maßnahmen, die für die Anwendung der Verordnung (EU) 2018/1725 durch die ENISA erforderlich sind, festlegen.

([32]) Verordnung Nr. 1 zur Regelung der Sprachenfrage für die Europäische Wirtschaftsgemeinschaft (ABl. 17 vom 6.10.1958, S. 385/58).

Artikel 42

Zusammenarbeit mit Drittländern und internationalen Organisationen

(1) Die ENISA kann mit den zuständigen Behörden von Drittländern und mit internationalen Organisationen zusammenarbeiten, soweit dies zur Verwirklichung der Ziele dieser Verordnung erforderlich ist. Zu diesem Zweck kann die ENISA, nach vorheriger Genehmigung durch die Kommission, Arbeitsvereinbarungen mit den Behörden von Drittländern und internationalen Organisationen treffen. Diese Arbeitsvereinbarungen begründen keine rechtlichen Verpflichtungen für die Union und ihre Mitgliedstaaten.

(2) Die ENISA steht der Beteiligung von Drittländern offen, die entsprechende Übereinkünfte mit der Europäischen Union geschlossen haben. Gemäß den einschlägigen Bestimmungen dieser Übereinkünfte werden Arbeitsvereinbarungen getroffen, die insbesondere Art, Umfang und Form einer Beteiligung dieser Drittländer an der Tätigkeit der ENISA festlegen; hierzu zählen auch Bestimmungen über die Beteiligung an den von der ENISA durchgeführten Initiativen, finanzielle Beiträge und Personal. In Personalfragen müssen derartige Arbeitsvereinbarungen in jedem Fall mit dem Statut der Beamten und den Beschäftigungsbedingungen für die sonstigen Bediensteten vereinbar sein.

(3) Der Verwaltungsrat verabschiedet eine Strategie für die Beziehungen zu Drittländern und internationalen Organisationen in Bezug auf Angelegenheiten, für die die ENISA zuständig ist. Die Kommission stellt durch den Abschluss einer entsprechenden Arbeitsvereinbarung mit dem Exekutivdirektor sicher, dass die ENISA im Rahmen ihres Mandats und des bestehenden institutionellen Rahmens handelt.

Artikel 43

Sicherheitsvorschriften für den Schutz von vertraulichen Informationen, die nicht zu den Verschlusssachen zählen und von Verschlusssachen

Nach Konsultation der Kommission legt die ENISA die Sicherheitsvorschriften fest, mit denen die in den Sicherheitsvorschriften der Kommission für den Schutz von vertraulichen Informationen, die nicht zu den Verschlusssachen zählen und von Verschlusssachen der Europäischen Union enthaltenen Sicherheitsgrundsätze angewandt werden, die in den Beschlüssen (EU, Euratom) 2015/443 und 2015/444 festgelegt sind. Die Sicherheitsvorschriften der ENISA enthalten Bestimmungen über den Austausch, die Verarbeitung und die Speicherung derartiger Informationen.

Artikel 44

Sitzabkommen und Arbeitsbedingungen

(1) Die notwendigen Regelungen über die Unterbringung der ENISA in dem Mitgliedstaat, in dem sie ihren Sitz hat, und über die Einrichtungen, die von diesem Mitgliedstaat zur Verfügung zu stellen sind, sowie die besonderen Vorschriften, die im Sitzmitgliedstaat der ENISA für den Exekutivdirektor, die Mitglieder des Verwaltungsrats, das Personal der ENISA und für Familienangehörige dieser Personen gelten, werden in einem Sitzabkommen festgelegt, das nach Billigung durch den Verwaltungsrat zwischen der ENISA und dem Sitzmitgliedstaat geschlossen wird.

(2) Der Sitzmitgliedstaat der ENISA gewährleistet die bestmöglichen Voraussetzungen für das reibungslose Funktionieren der ENISA, unter Berücksichtigung der Erreichbarkeit des Standortes, des Vorhandenseins adäquater Bildungseinrichtungen für die Kinder der Mitglieder des Personals und eines angemessenen Zugangs zu Arbeitsmarkt, Sozialversicherung und medizinischer Versorgung für Kinder und Ehegatten der Mitglieder des Personals.

Artikel 45

Verwaltungskontrolle

Die Tätigkeit der ENISA unterliegt der Aufsicht des Europäischen Bürgerbeauftragten nach Artikel 228 AEUV.

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 Cybersicherheitszertifizierung 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 Konformitätsbewertungsstellen, 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.

Geschehen zu Straßburg am 17. April 2019.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Der Präsident*
A. TAJANI	G. CIAMBA

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 erforderlichen 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.