15.4.2024 A9-0307/2

Änderungsantrag 2
Cristian-Silviu Buşoi
im Namen des Ausschusses für Industrie, Forschung und Energie

Bericht **A9-0307/2023**
Josianne Cutajar
Verwaltete Sicherheitsdienste
(COM(2023)0208 – C9-0137/2023 – 2023/0108(COD))

Vorschlag für eine Verordnung
–

ABÄNDERUNGEN DES EUROPÄISCHEN PARLAMENTS*

zum Vorschlag der Kommission

VERORDNUNG (EU) 2024/…
DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom …

zur Änderung. der Verordnung (EU) 2019/881 im Hinblick auf verwaltete Sicherheitsdienste

(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,

* Textänderungen: Der neue bzw. geänderte Text wird durch Fett- und Kursivdruck gekennzeichnet; Streichungen werden durch das Symbol ▌ gekennzeichnet.

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

nach ***Anhörung*** des Ausschusses der Regionen,

gemäß dem ordentlichen Gesetzgebungsverfahren[2],

[1] ***ABl. C 349 vom 29.9.2023, S. 167***.

[2] ***Standpunkt des Europäischen Parlaments vom … [(ABl. …)/(noch nicht im Amtsblatt veröffentlicht)] und Beschluss des Rates vom ….***

in Erwägung nachstehender Gründe:

(1) Durch die Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates[3] wird ein Rahmen für die Schaffung europäischer Systeme für die Cybersicherheitszertifizierung eingeführt, um für ***Produkte der Informations- und Kommunikationstechnologie (IKT),*** IKT-Dienste und IKT-Prozesse in der Union ein angemessenes Maß an Cybersicherheit zu gewährleisten und eine Fragmentierung des Binnenmarkts für Zertifizierungssysteme in der EU zu verhindern.

(2) ***Um sicherzustellen, dass die Union Cyberangriffen standhalten kann, und um Schwachstellen auf dem Unionsmarkt zu verhindern, soll mit dieser Verordnung der horizontale Rechtsrahmen für die Festlegung umfassender Cybersicherheitsanforderungen für alle Produkte mit digitalen Elementen gemäß der Verordnung (EU) …/… des Europäischen Parlaments und des Rates***[4] ***(2022/0272(COD)) ergänzt werden, indem grundlegende Anforderungen für verwaltete Cybersicherheitsdienste, für deren Anwendung und für deren Vertrauenswürdigkeit festgelegt werden.***

---

3 Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (ABl. L 151 vom 7.6.2019, S. 15).

4 ***Verordnung (EU) …/… des Europäischen Parlaments und des Rates vom … über … (ABl. L …, …, ELI: …).***

(3) Verwaltete Sicherheitsdienste ***sind Dienste, die von Anbietern verwalteter Sicherheitsdienste im Sinne von Artikel 6 Nummer 40 der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates[5] erbracht werden. Deshalb sollte die Begriffsbestimmung für verwaltete Sicherheitsdienste in dieser Verordnung mit der Begriffsbestimmung für Anbieter verwalteter Sicherheitsdienste in der Richtlinie (EU) 2022/2555 im Einklang stehen. Diese*** Dienste ***bestehen*** in der Durchführung oder Unterstützung von Tätigkeiten im Zusammenhang mit dem Cybersicherheitsrisikomanagement ihrer Kunden ***und*** haben bei der Verhütung und Eindämmung von Cybersicherheitsvorfällen an Bedeutung gewonnen. Dementsprechend gelten die Anbieter dieser Dienste gemäß der Richtlinie (EU) 2022/2555 ▌ als wesentliche oder wichtige Einrichtungen, die zu einem Sektor mit hoher Kritikalität gehören. Nach Erwägungsgrund 86 der genannten Richtlinie spielen die Anbieter verwalteter Sicherheitsdienste in Bereichen wie Reaktion auf Sicherheitsvorfälle, Penetrationstests, Sicherheitsaudits und Beratung eine überaus wichtige Rolle, indem sie Einrichtungen bei deren Bemühungen um die Verhütung, Erkennung und Bewältigung von Sicherheitsvorfällen und bei der anschließenden Wiederherstellung unterstützen. Anbieter verwalteter Sicherheitsdienste sind jedoch auch selbst Ziel von Cyberangriffen geworden und stellen aufgrund ihrer engen Einbindung in die Betriebstätigkeit ihrer Kunden ein besonderes Risiko dar. Wesentliche und wichtige Einrichtungen im Sinne der Richtlinie (EU) 2022/2555 sollten daher bei der Wahl eines Anbieters verwalteter Sicherheitsdienste erhöhte Sorgfalt walten lassen.

---

5 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) (ABl. L 333 vom 27.12.2022, S. 80).

(4) Die Begriffsbestimmung für verwaltete Sicherheitsdienste gemäß dieser Verordnung umfasst eine nicht erschöpfende Liste verwalteter Sicherheitsdienste, die für Zertifizierungssysteme infrage kommen könnten, darunter etwa die Bewältigung von Sicherheitsvorfällen, Penetrationstests, Sicherheitsaudits und Beratung im Zusammenhang mit technischer Unterstützung. Verwaltete Sicherheitsdienste könnten Cybersicherheitsdienste umfassen, die die Abwehrbereitschaft sowie die Prävention, Erkennung, Analyse und Eindämmung von, die Reaktion auf und die Wiederherstellung nach Cybersicherheitsvorfällen unterstützen. Auch die Bereitstellung von Informationen über Cyberbedrohungen und Risikoabschätzungen im Zusammenhang mit technischer Unterstützung könnten als verwaltete Sicherheitsdienste eingestuft werden. Für einzelne verwaltete Sicherheitsdienste kann es verschiedene europäische Systeme für die Cybersicherheitszertifizierung geben. Die gemäß diesen Systemen ausgestellten europäischen Cybersicherheitszertifikate sollten sich auf bestimmte verwaltete Sicherheitsdienste eines bestimmten Anbieters dieser Dienste beziehen.

(5) Die Anbieter verwalteter Sicherheitsdienste ***können*** auch eine wichtige Rolle mit Blick auf ***Maßnahmen der Union spielen, mit denen*** die Reaktion und sofortige Wiederherstellung im Falle von schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes ***unterstützt wird, wobei sie sich auf Dienste vertrauenswürdiger privater Anbieter und – auf der Grundlage von EU-Risikobewertungen – auf die Prüfung kritischer Einrichtungen auf potenzielle Schwachstellen stützen***. ***Die Zertifizierung verwalteter Sicherheitsdienste kann bei der Auswahl vertrauenswürdiger Anbieter eine Rolle spielen.***

(6) Die Zertifizierung verwalteter Sicherheitsdienste ist nicht nur für das Auswahlverfahren zur Bildung der EU-Cybersicherheitsreserve von Bedeutung, sondern ist auch ein wesentlicher Qualitätsindikator für private und öffentliche Einrichtungen, die solche Dienste nutzen wollen. Angesichts der Kritikalität der verwalteten Sicherheitsdienste und der Sensibilität der von ihnen verarbeiteten Daten könnte die Zertifizierung den potenziellen Kunden wichtige Orientierungshilfen und Sicherheit in Bezug auf die Vertrauenswürdigkeit dieser Dienste bieten. Europäische Zertifizierungssysteme für verwaltete Sicherheitsdienste tragen dazu bei, eine Fragmentierung des Binnenmarkts zu verhindern. Diese Verordnung zielt daher darauf ab, das Funktionieren des Binnenmarkts zu verbessern.

(7) ***Europäische Zertifizierungssysteme für verwaltete Sicherheitsdienste sollten bewirken, dass diese Dienste angenommen werden und der Wettbewerb zwischen Anbietern verwalteter Sicherheitsdienste zunimmt. Unbeschadet des Ziels, für ein hinreichendes und angemessenes Maß an einschlägigem technischem Wissen und beruflicher Integrität dieser Anbieter zu sorgen, sollten Zertifizierungssysteme deshalb den Markteintritt und das Anbieten verwalteter Sicherheitsdienste erleichtern, indem sie den potenziellen Regelungs-, Verwaltungs- und Finanzaufwand, mit dem Anbieter und insbesondere Kleinstunternehmen oder kleine und mittlere Unternehmen (KMU) konfrontiert sein könnten, wenn sie verwaltete Sicherheitsdienste anbieten, nach Möglichkeit verringern. Außerdem sollten die Systeme mit dem Ziel, die Einführung von verwalteten Sicherheitsdiensten zu erleichtern und die Nachfrage nach ihnen anzuregen, dazu beitragen, dass insbesondere kleinere Akteure wie etwa Kleinstunternehmen und KMU sowie lokale und regionale Gebietskörperschaften mit begrenzten Kapazitäten und Ressourcen, die jedoch anfälliger für Cyberangriffe mit finanziellen, rechtlichen, rufschädigenden und operativen Folgen sind, Zugang zu diesen Diensten haben.***

(8) ***Es ist wichtig, Kleinstunternehmen sowie kleine und mittlere Unternehmen bei der Durchführung dieser Verordnung und bei der Einstellung von Personal mit den erforderlichen Kompetenzen und dem erforderlichen Fachwissen im Bereich Cybersicherheit zu unterstützen, damit sie im Einklang mit den Anforderungen dieser Verordnung verwaltete Sicherheitsdienste anbieten können. Das Programm „Digitales Europa“ und andere einschlägige Unionsprogramme sehen vor, dass die Kommission finanzielle und technische Unterstützung leistet, die es diesen Unternehmen ermöglicht, zum Wachstum der Wirtschaft in Europa und zur Stärkung des gemeinsamen europäischen Cybersicherheitsniveaus innerhalb der Union beizutragen, indem beispielsweise die finanzielle Unterstützung aus dem Programm „Digitales Europa“ und anderen einschlägigen Unionsprogrammen auf dieses Ziel ausgerichtet wird und Kleinstunternehmen und KMU unterstützt werden.***

(9) ***Das Zertifizierungssystem der Union für verwaltete Sicherheitsdienste sollte zur Verfügbarkeit sicherer und hochwertiger Dienste, die einen sicheren digitalen Übergang gewährleisten, und zur Erreichung der im Politikprogramm für die digitale Dekade festgelegten Ziele beitragen, und zwar insbesondere im Hinblick auf die Ziele, dass 75 % der Unternehmen in der Union mit der Nutzung der Cloud, von KI oder Massendaten beginnen, dass mehr als 90 % der Kleinstunternehmen und der KMU zumindest eine grundlegende digitale Intensität erreichen und dass wesentliche öffentliche Dienstleistungen online angeboten werden.***

(10) Neben der Einführung von IKT-Produkten, -Diensten oder -Prozessen bieten verwaltete Sicherheitsdienste häufig noch zusätzliche Dienstleistungen an, die sich auf die Kompetenzen, Fachkenntnis und Erfahrung ihres Personals stützen. Ein sehr hohes Niveau solcher Kompetenzen, Fachkenntnis und Erfahrung sowie geeignete interne Verfahren sollten Teil der Sicherheitsziele sein, um eine sehr hohe Qualität der verwalteten Sicherheitsdienste zu gewährleisten. Damit alle Aspekte verwalteter Sicherheitsdienste von ***speziellen Zertifizierungssystemen*** erfasst werden können, ist es daher erforderlich, die Verordnung (EU) 2019/881 zu ändern. ***Den Ergebnissen und Empfehlungen der in der Verordnung (EU) 2019/881 vorgesehenen Bewertung und Überarbeitung sollte Rechnung getragen werden.***

(11) ***Damit das Wachstum eines verlässlichen Unionsmarkts gefördert werden kann und man zudem Partnerschaften mit gleichgesinnten Drittstaaten eingehen kann, sollte das Zertifizierungsverfahren, das mit dem durch diese Verordnung geschaffenen Rahmen eingerichtet wird, gestrafft sein, damit seine internationale Anerkennung und die Abstimmung auf internationale Normen erleichtert werden.***

(12) Wie die Kommission in ihrer Mitteilung vom 18. April 2023 über die Akademie für Cybersicherheitskompetenzen festgestellt hat, ist die Union mit einem Fachkräftemangel konfrontiert, der durch einen Mangel an qualifizierten Arbeitskräften und eine sich schnell entwickelnde Bedrohungslage gekennzeichnet ist. Bildungsressourcen und die Formen formaler Ausbildungen variieren und Wissen kann auf unterschiedliche Weise erworben werden, und zwar entweder formal, etwa an Hochschulen oder mit Kursen, oder nicht-formal, beispielsweise durch das Lernen am Arbeitsplatz oder eine lange Berufserfahrung in dem einschlägigen Bereich. Deshalb muss die Zusammenarbeit zwischen den Mitgliedstaaten, der Kommission, der ENISA und Interessenträgern unter anderem aus der Privatwirtschaft und der Wissenschaft im Wege des Aufbaus öffentlich-privater Partnerschaften, der Unterstützung von Forschungs- und Innovationsinitiativen, der Ausarbeitung und gegenseitigen Anerkennung von gemeinsamen Normen und der Zertifizierung von Cybersicherheitskompetenzen etwa mittels des europäischen Rahmens für Cybersicherheitskompetenzen intensiviert werden, sodass hochwertige grundlegende verwaltete Sicherheitsdienste einfacher eingerichtet werden können und ein besserer Überblick über die Zusammensetzung des Arbeitskräfteangebots der Union im Bereich Cybersicherheit erlangt wird. Diese Zusammenarbeit würde außerdem die Mobilität von Fachkräften im Bereich Cybersicherheit innerhalb der Union sowie die Aufnahme von Kenntnissen und Schulungen in diesem Bereich in Bildungsprogramme fördern und den Zugang junger Menschen, darunter auch Menschen, die in benachteiligten Regionen wie Inseln, dünn besiedelten, ländlichen und entlegenen Gegenden leben, zu Ausbildungen und Praktika sicherstellen. Diese Maßnahmen müssen darauf ausgerichtet sein, mehr Frauen und Mädchen für diesen Bereich zu gewinnen, und einen Beitrag zur Beseitigung des Geschlechtergefälles in Mathematik, Informatik, Naturwissenschaften und Technik leisten, und die Privatwirtschaft muss sich darum bemühen, eine Ausbildung am Arbeitsplatz anzubieten, die sich auf die am stärksten gefragten Kompetenzen konzentriert und in die sowohl die öffentliche Verwaltung als auch Start-ups, Kleinstunternehmen und KMU einbezogen werden. Zudem müssen die Anbieter und die Mitgliedstaaten zusammenarbeiten und zur Erhebung von Daten zur Lage und zur Entwicklung des Cybersicherheits-Arbeitsmarkts beitragen.

(13) Die ENISA spielt eine wichtige Rolle, wenn es gilt, mögliche europäische Zertifizierungssysteme auszuarbeiten. Bei der Ausarbeitung des Entwurfs des Gesamthaushaltsplans der Union sollte die Kommission gemäß dem in Artikel 29 der Verordnung (EU) 2019/881 festgelegten Verfahren die erforderlichen Haushaltsmittel für den Stellenplan der ENISA abschätzen.

(14) In der vorliegenden Verordnung sind gezielte Änderungen der Verordnung (EU) 2019/881 vorgesehen, damit die Möglichkeit geschaffen wird, Systeme für die Cybersicherheitszertifizierung für Anbieter verwalteter Sicherheitsdienste einzurichten. Diesbezüglich werden in der vorliegenden Verordnung außerdem bestimmte Vorschriften ausgeführt und erläutert, die sich mit der Ausarbeitung und Funktionsweise sämtlicher europäischer Systeme für die Cybersicherheitszertifizierung befassen, damit für ihre Transparenz und Offenheit gesorgt ist. Die letztgenannten Änderungen, die sich auf die Ausführung oder Erläuterungen der Verordnung (EU) 2019/881 beschränken – insbesondere die Änderungen der Artikel 49 und 49a –, sollten keinesfalls die gemäß Artikel 67 der genannten Verordnung erforderliche generelle Bewertung und Überarbeitung der genannten Verordnung vorwegnehmen, insbesondere die Bewertung der Auswirkungen, der Wirksamkeit und der Effizienz des Titels der genannten Verordnung in Bezug auf Systeme für die Cybersicherheitszertifizierung. Diese Bewertung und Überarbeitung des Titels in Bezug auf Systeme für die Cybersicherheitszertifizierung sollte auf einer umfassenden Konsultation der Interessenträger und einer ausführlichen und sorgfältigen Analyse der betreffenden Verfahren beruhen.

(15) ***Da das Ziel dieser Verordnung, nämlich die Schaffung der Möglichkeit, europäische Systeme für die Cybersicherheitszertifizierung für verwaltete Sicherheitsdienste einzurichten, von den Mitgliedstaaten nicht ausreichend verwirklicht werden kann, sondern vielmehr wegen seines Umfangs und seiner Wirkungen auf Unionsebene besser zu verwirklichen ist, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Verordnung nicht über das für die Verwirklichung dieses Ziels erforderliche Maß hinaus.***

(16) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates[6] angehört und hat am ***10. Januar 2024*** eine Stellungnahme[7] abgegeben —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

---

[6] ***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).***

[7] ***ABl. C …/….***

Artikel 1

Änderungen der Verordnung (EU) 2019/881

Die Verordnung (EU) 2019/881 wird wie folgt geändert:

1. Artikel 1 Absatz 1 Unterabsatz 1 Buchstabe b erhält folgende Fassung:

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

2. Artikel 2 wird wie folgt geändert:

a) Die Nummern 9, 10 und 11 erhalten folgende Fassung:

„9. ‚europäisches System 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 und verwalteten Sicherheitsdiensten gelten;

10. ‚nationales System 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 und verwalteten Sicherheitsdiensten gelten, die von diesem System erfasst werden;

11. ‚europäisches Cybersicherheitszertifikat' bezeichnet ein von einer maßgeblichen Stelle ausgestelltes Dokument, in dem bescheinigt wird, dass ein bestimmtes IKT-Produkt, ein bestimmter IKT-Dienst, ein bestimmter IKT-Prozess oder ein bestimmter verwalteter Sicherheitsdienst im Hinblick auf die Erfüllung besonderer Sicherheitsanforderungen, die in einem europäischen System für die Cybersicherheitszertifizierung festgelegt sind, bewertet wurde;"

b) Folgende Nummer 14a wird eingefügt:

„14a. ‚verwalteter Sicherheitsdienst' bezeichnet einen ***für einen Dritten erbrachten*** Dienst, der in der Durchführung oder Unterstützung von Tätigkeiten im Zusammenhang mit dem Cybersicherheitsrisikomanagement besteht und unter anderem die ***Bewältigung von Sicherheitsvorfällen***, Penetrationstests, Sicherheitsaudits und Beratung ***– auch von Sachverständigen – zur technischen Unterstützung*** umfasst;"

c) Die Nummern 20, 21 und 22 erhalten folgende Fassung:

„20. ‚technische Spezifikationen‘ bezeichnet ein Dokument, das die technischen Anforderungen, denen ein IKT-Produkt, -Dienst oder -Prozess oder ein verwalteter Sicherheitsdienst genügen muss, oder ein diesbezügliches Konformitätsbewertungsverfahren vorschreibt;

21. ‚Vertrauenswürdigkeitsstufe‘ bezeichnet die Grundlage für das Vertrauen darin, dass ein IKT-Produkt, -Dienst oder -Prozess oder ein verwalteter Sicherheitsdienst den Sicherheitsanforderungen eines spezifischen europäischen Systems für die Cybersicherheitszertifizierung genügt, und gibt an, auf welchem Niveau das IKT-Produkt, der IKT-Dienst, der IKT-Prozess oder der verwaltete Sicherheitsdienst bei der Bewertung eingestuft wurde, ist jedoch als solche kein Maß für die Sicherheit des jeweiligen IKT-Produkts, -Dienstes oder -Prozesses oder verwalteten Sicherheitsdienstes;

22. ‚Selbstbewertung der Konformität' bezeichnet eine Maßnahme eines Herstellers oder Anbieters von IKT-Produkten, -Diensten und -Prozessen oder verwalteten Sicherheitsdiensten zur Bewertung, ob diese IKT-Produkte, -Dienste und -Prozesse oder verwalteten Sicherheitsdienste die Anforderungen, die in einem bestimmten europäischen System für die Cybersicherheitszertifizierung festgelegt sind, erfüllen."

3. Artikel 4 Absatz 6 erhält folgende Fassung:

„(6) Die ENISA fördert die Nutzung der europäischen Cybersicherheitszertifizierung, um der Fragmentierung des Binnenmarkts vorzubeugen. Die ENISA trägt zum Aufbau und zur Pflege eines europäischen Zertifizierungsrahmens für die Cybersicherheit im Sinne des Titels III dieser Verordnung bei, um die Transparenz der Cybersicherheit von IKT-Produkten, -Diensten und -Prozessen und verwalteten Sicherheitsdiensten zu erhöhen und damit das Vertrauen in den digitalen Binnenmarkt sowie dessen Wettbewerbsfähigkeit zu stärken."

4. Artikel 8 wird wie folgt geändert:

a) Absatz 1 erhält folgende Fassung:

„(1) Die ENISA unterstützt und fördert die Entwicklung und Umsetzung der Unionspolitik auf dem Gebiet der Cybersicherheitszertifizierung von IKT-Produkten, -Diensten und -Prozessen und verwalteten Sicherheitsdiensten, 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 Systeme für die Cybersicherheitszertifizierung nach Artikel 54 Absatz 1 Buchstabe c empfiehlt,

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

c) angenommene europäische Systeme für die Cybersicherheitszertifizierung nach Artikel 49 Absatz 8 bewertet,

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.“

b) Absatz 3 erhält folgende Fassung:

„(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 zu den Anforderungen an die Cybersicherheit von IKT-Produkten, -Diensten und -Prozessen und verwalteten Sicherheitsdiensten zusammen, veröffentlicht diese und entwickelt bewährte Verfahren hierzu.“

c) Absatz 5 erhält folgende Fassung:

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

5. Artikel 46 Absätze 1 und 2 erhalten folgende Fassung:

„(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 und verwaltete Sicherheitsdienste ein harmonisierter Ansatz auf Unionsebene für europäische Systeme für die Cybersicherheitszertifizierung ermöglicht wird.

(2) Im europäischen Zertifizierungsrahmen für die Cybersicherheit ist ein Mechanismus festgelegt, mit dem europäische Systeme für die Cybersicherheitszertifizierung geschaffen werden. Damit wird bescheinigt, dass die nach einem solchen System bewerteten IKT-Produkte, -Dienste und -Prozesse den festgelegten Sicherheitsanforderungen genügen, um die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit von gespeicherten, übermittelten oder verarbeiteten Daten oder der Funktionen oder Dienste, die von diesen Produkten, Diensten und Prozessen angeboten oder über diese zugänglich gemacht werden, während deren gesamten Lebenszyklus zu schützen. Außerdem wird damit bescheinigt, dass verwaltete Sicherheitsdienste, die nach solchen Systemen bewertet wurden, den festgelegten Sicherheitsanforderungen zum Schutz der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten entsprechen, auf die im Zusammenhang mit der Erbringung dieser Dienste zugegriffen wird bzw. die in diesem Zusammenhang verarbeitet, gespeichert oder übermittelt werden, und dass diese Dienste kontinuierlich mit der erforderlichen Kompetenz, Sachkenntnis und Erfahrung von Personal mit einem ***hinreichenden und angemessenen*** Maß an einschlägigen Fachkenntnissen und beruflicher Integrität erbracht werden.“

6. Artikel 47 Absätze 2 und 3 erhalten folgende Fassung:

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

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

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

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

c) Nachfrage auf dem Markt;

ca) technologische Entwicklungen sowie Verfügbarkeit und Entwicklung internationaler Systeme für die Cybersicherheitszertifizierung und internationaler und allgemeiner Normen;

d) Entwicklungen in der Cyberbedrohungslandschaft;

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

7. Artikel 49 ***wird wie folgt geändert:***

a) Die Absätze 1, 2, 3 und 4 erhalten folgende Fassung:

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

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

(3) Bei der Ausarbeitung eines möglichen Systems konsultiert die ENISA zeitnah alle infrage kommenden Interessenträger im Wege eines förmlichen, offenen, transparenten und inklusiven Konsultationsprozesses. Wenn die ENISA der Kommission das mögliche System gemäß Artikel 49 Absatz 6 vorlegt, stellt sie Informationen darüber bereit, inwiefern sie dieser Verpflichtung nachgekommen ist.

(4) Für jedes mögliche System setzt die ENISA eine Ad-hoc-Arbeitsgruppe nach Artikel 20 Absatz 4 ein, damit sie der ENISA spezifische Beratung und Sachkenntnis bereitstellt. Den zu diesem Zweck eingesetzten Ad-hoc-Arbeitsgruppen gehören gegebenenfalls und unbeschadet der Verfahren und des Ermessensspielraums gemäß Artikel 20 Absatz 4 Sachverständige der öffentlichen Verwaltungsbehörden der Mitgliedstaaten, der Organe, Einrichtungen und sonstigen Stellen der Union und der Privatwirtschaft an.“

b) Absatz 7 erhält folgende Fassung:

„(7) Auf der Grundlage des von der ENISA ausgearbeiteten möglichen Systems kann die Kommission Durchführungsrechtsakte erlassen, in denen für IKT-Produkte, -Dienste und -Prozesse und verwaltete Sicherheitsdienste, die die Anforderungen der Artikel 51, ***51a,*** 52 und 54 erfüllen, ein europäisches System für die Cybersicherheitszertifizierung festgelegt wird. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 66 Absatz 2 genannten Prüfverfahren erlassen.“

8. Folgender Artikel 49a wird eingefügt:

„Artikel 49a

Informationen und Konsultationen über die europäischen Systeme für die Cybersicherheitszertifizierung

(1) Die Kommission veröffentlicht Informationen darüber, dass sie die ENISA damit beauftragt hat, ein mögliches System auszuarbeiten oder ein bestehendes europäisches System für die Cybersicherheitszertifizierung nach Artikel 48 zu überarbeiten.

(2) Während der Ausarbeitung eines möglichen Systems durch die ENISA gemäß Artikel 49 können das Europäische Parlament und der Rat die Kommission in ihrer Eigenschaft als Vorsitzende der Europäischen Gruppe für die Cybersicherheitszertifizierung (ECCG) und die ENISA ersuchen, vierteljährlich einschlägige Informationen über den Entwurf eines möglichen Systems vorzulegen. Auf Ersuchen des Europäischen Parlaments oder des Rates kann die ENISA im Einvernehmen mit der Kommission und unbeschadet des Artikels 27 dem Europäischen Parlament und dem Rat relevante Teile des Entwurfs eines möglichen Systems in einer dem erforderlichen Vertraulichkeitsniveau angemessenen Weise und gegebenenfalls in eingeschränkter Form zur Verfügung stellen.

(3) Um den Dialog zwischen den Unionsorganen zu fördern und zu einem formellen, offenen, transparenten und inklusiven Konsultationsprozess beizutragen, können das Europäische Parlament und der Rat die Kommission und die ENISA ersuchen, Angelegenheiten zu erörtern, die das Funktionieren der europäischen Systeme für die Cybersicherheitszertifizierung von IKT-Produkten, -Diensten und -Prozessen oder verwalteten Sicherheitsdiensten betreffen.

(4) Bei der Bewertung dieser Verordnung gemäß Artikel 67 berücksichtigt die Kommission gegebenenfalls Elemente, die sich aus den Standpunkten des Europäischen Parlaments und des Rates zu den in Absatz 3 des vorliegenden Artikels genannten Angelegenheiten ergeben.“;

9. Artikel 51 wird wie folgt geändert:

a) Der Titel erhält folgende Fassung:

„Sicherheitsziele der europäischen Systeme für die Cybersicherheitszertifizierung für IKT-Produkte, -Dienste und -Prozesse“

b) Der einleitende Satz erhält folgende Fassung:

„Es wird ein europäisches System für die Cybersicherheitszertifizierung für IKT-Produkte, -Dienste und -Prozesse konzipiert, um – soweit zutreffend – mindestens die folgenden Sicherheitsziele zu verwirklichen:“

10. Folgender Artikel 51a wird eingefügt:

„Artikel 51a
Sicherheitsziele der europäischen Systeme für die Cybersicherheitszertifizierung für verwaltete Sicherheitsdienste

Es wird ein europäisches System für die Cybersicherheitszertifizierung für verwaltete Sicherheitsdienste konzipiert, um – soweit zutreffend – mindestens die folgenden Sicherheitsziele zu verwirklichen:

a) Die verwalteten Sicherheitsdienste werden mit der erforderlichen Kompetenz, Sachkenntnis und Erfahrung erbracht, wozu auch gehört, dass das mit der Erbringung dieser Dienste betraute Personal über ein ***ausreichendes und angemessenes*** Maß an Fachkenntnissen und Kompetenzen in dem betreffenden Bereich, ausreichende und angemessene Erfahrung und ein Höchstmaß an beruflicher Integrität verfügt.

b) Der Anbieter verfügt über geeignete interne Verfahren, um sicherzustellen, dass die verwalteten Sicherheitsdienste jederzeit in ***ausreichender und angemessener*** Qualität erbracht werden.

c) Daten, auf die bei der Erbringung verwalteter Sicherheitsdienste zugegriffen wird bzw. dabei gespeicherte, übermittelte oder anderweitig verarbeitete Daten werden vor unbeabsichtigtem oder unbefugtem Zugriff und vor unbeabsichtigter oder unbefugter Speicherung, Preisgabe, Vernichtung und sonstiger Verarbeitung sowie vor Verlust, Änderung oder Nichtverfügbarkeit geschützt.

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

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

f) Es wird protokolliert und kann abgerufen werden, 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 wurden.

g) Die IKT-Produkte, -Dienste und -Prozesse, die zur Erbringung der verwalteten Sicherheitsdienste eingesetzt werden, sind durch Voreinstellungen und Technikgestaltung sicher, ***und enthalten gegebenenfalls die neuesten Sicherheitsaktualisierungen und*** weisen keine öffentlich bekannten Sicherheitslücken auf;“;

11. Artikel 52 wird wie folgt geändert:

a) Absatz 1 erhält folgende Fassung:

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

b) Absatz 3 erhält folgende Fassung:

„(3) Die den einzelnen Vertrauenswürdigkeitsstufen entsprechenden Sicherheitsanforderungen, einschließlich der entsprechenden Sicherheitsfunktionen und der entsprechenden Strenge und Gründlichkeit der Bewertung, die das IKT-Produkt, der IKT-Dienst, der IKT-Prozess oder der verwaltete Sicherheitsdienst durchlaufen muss, werden in dem jeweiligen europäischen System für die Cybersicherheitszertifizierung festgelegt.“

c) Absätze 5, 6 und 7 erhalten folgende Fassung:

„(5) Ein europäisches Cybersicherheitszertifikat oder eine EU-Konformitätserklärung für die Vertrauenswürdigkeitsstufe „niedrig“ bietet die Gewissheit, dass die IKT-Produkte, -Dienste und -Prozesse und verwalteten Sicherheitsdienste, 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 Grundrisiken für Sicherheitsvorfälle und Cyberangriffe möglichst gering zu halten. Die durchzuführende Bewertung beinhaltet mindestens eine Überprüfung der technischen Dokumentation. Ist eine solche Überprüfung 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 und verwalteten Sicherheitsdienste, 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 eine Prüfung, die zeigt, dass die IKT-Produkte, -Dienste und -Prozesse und verwalteten Sicherheitsdienste die erforderlichen Sicherheitsfunktionen korrekt durchführen. Falls diese Bewertungstätigkeiten nicht geeignet sind, werden alternative Prüfungen mit gleicher Wirkung durchgeführt.

(7) Ein europäisches Cybersicherheitszertifikat für die Vertrauenswürdigkeitsstufe „hoch“ bietet die Gewissheit, dass die IKT-Produkte, -Dienste und -Prozesse und verwalteten Sicherheitsdienste, für welche dieses Zertifikat ausgestellt wird, die entsprechenden Sicherheitsanforderungen einschließlich der Sicherheitsfunktionen erfüllen und 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 durchzuführende Bewertung beinhaltet mindestens Folgendes: eine Überprüfung, die zeigt, dass keine allgemein bekannten Sicherheitslücken vorliegen; eine Prüfung, die zeigt, dass die IKT-Produkte, -Dienste und -Prozesse oder verwalteten Sicherheitsdienste 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, werden alternative Prüfungen mit gleicher Wirkung durchgeführt.“

12. Artikel 53 Absätze 1, 2 und 3 erhalten folgende Fassung:

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

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

(3) Der Hersteller oder Anbieter von IKT-Produkten, -Diensten und -Prozessen oder verwalteten Sicherheitsdiensten hält die EU-Konformitätserklärung, die technische Dokumentation und alle weiteren einschlägigen Informationen in Bezug auf die Konformität der IKT-Produkte, -Dienste und -Prozesse oder verwalteten Sicherheitsdienste mit dem System während des Zeitraums, der in dem entsprechenden europäischen System 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.“

13. Artikel 54 Absatz 1 wird wie folgt geändert:

a) Buchstabe a erhält folgende Fassung:

„a) den Gegenstand und Umfang des Zertifizierungssystems, einschließlich der Art oder Kategorie der erfassten IKT-Produkte, -Dienste und -Prozesse und verwalteten Sicherheitsdienste;“

aa) Buchstabe g erhält folgende Fassung:

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

b) Buchstabe j erhält folgende Fassung:

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

c) Buchstabe l erhält folgende Fassung:

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

d) Buchstabe o erhält folgende Fassung:

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

e) Buchstabe q erhält folgende Fassung:

„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*** oder verwalteten Sicherheitsdiensten ▌ “;

14. Artikel 56 wird wie folgt geändert:

a) Absatz 1 erhält folgende Fassung:

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

b) Absatz 3 wird wie folgt geändert:

i) Unterabsatz 1 erhält folgende Fassung:

„Die Kommission bewertet regelmäßig die Effizienz und Nutzung der angenommenen europäischen Systeme für die Cybersicherheitszertifizierung sowie die Frage, ob ein bestimmtes europäisches System für die Cybersicherheitszertifizierung durch das einschlägige Unionsrecht verbindlich vorgeschrieben werden soll, um ein angemessenes Maß an Cybersicherheit von IKT-Produkten, -Diensten und -Prozessen und verwalteten Sicherheitsdiensten 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 Bewertungen fest, welche IKT-Produkte, -Dienste und -Prozesse und verwalteten Sicherheitsdienste, die unter ein bestehendes Zertifizierungssystem fallen, unter ein verpflichtendes Zertifizierungssystem fallen müssen.“

ii) Unterabsatz 3 wird wie folgt geändert:

aa) Buchstabe a erhält folgende Fassung:

„a) Sie berücksichtigt die Auswirkungen der Maßnahmen auf die Hersteller oder Anbieter solcher IKT-Produkte, -Dienste und -Prozesse oder verwalteten Sicherheitsdienste 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 oder verwalteten Sicherheitsdienste ergibt;“;

bb) Buchstabe d erhält folgende Fassung:

„d) sie berücksichtigt die Umsetzungsfristen sowie die Übergangsmaßnahmen oder -zeiträume, insbesondere im Hinblick auf die möglichen Auswirkungen der Maßnahme auf die Anbieter oder Hersteller von IKT-Produkten, -Diensten und -Prozessen oder verwalteten Sicherheitsdiensten, einschließlich ***der besonderen Interessen und Bedürfnisse von Kleinstunternehmen und KMU;“***.

c) Absätze 7 und 8 erhalten folgende Fassung:

„(7) Die natürliche oder juristische Person, die ihre IKT-Produkte, -Dienste und -Prozesse oder verwalteten Sicherheitsdienste 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, -Prozesses oder verwalteten Sicherheitsdienstes, 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.“;

15. Artikel 57 Absätze 1 und 2 erhalten folgende Fassung:

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

(2) Die Mitgliedstaaten führen für die Cybersicherheitszertifizierung von IKT-Produkten, -Diensten und -Prozessen und verwalteten Sicherheitsdiensten, die unter ein geltendes europäisches System für die Cybersicherheitszertifizierung fallen, keine neuen nationalen Systeme ein.“

16. Artikel 58 wird wie folgt geändert:

a) Absatz 7 wird wie folgt geändert:

i) Die Buchstaben a und b erhalten folgende Fassung:

„a) Überwachung und Durchsetzung der Vorschriften im Rahmen der europäischen Systeme für die Cybersicherheitszertifizierung gemäß Artikel 54 Absatz 1 Buchstabe j im Hinblick auf die Überwachung der Übereinstimmung der IKT-Produkte, -Dienste und -Prozesse und verwalteten Sicherheitsdienste 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 und -Prozessen und verwalteten Sicherheitsdiensten, 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 System für die Cybersicherheitszertifizierung;“

ii) Buchstabe h erhält folgende Fassung:

„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 und verwalteten Sicherheitsdiensten mit den Anforderungen dieser Verordnung oder mit den Anforderungen bestimmter europäischer Systeme für die Cybersicherheitszertifizierung; und“;

b) Absatz 9 erhält folgende Fassung:

„(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*** und verwalteten Sicherheitsdiensten austauschen.“;

17. Artikel 59 Absatz 3 Buchstaben b und c erhalten folgende Fassung:

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

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

18. Artikel 67 Absätze 2 und 3 erhalten folgende Fassung:

(2) Die Bewertung erstreckt sich auch auf die Wirkung, Wirksamkeit und Effizienz der Bestimmungen des Titels III dieser Verordnung***, einschließlich der Verfahren, die zur Annahme von Systemen für die Cybersicherheitszertifizierung und ihrer faktengesicherten Grundlagen führen***, im Hinblick auf die Ziele, für IKT-Produkte, -Dienste und -Prozesse und verwaltete Sicherheitsdienste in der Union ein angemessenes Maß an Cybersicherheit und einen besser funktionierenden Binnenmarkt zu gewährleisten.

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

19. Der Anhang erhält die Fassung des Textes im Anhang dieser Verordnung.

Artikel 2

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

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

Geschehen zu ... am …

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Die Präsidentin	*Der Präsident*

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 und -Prozessen oder verwalteten Sicherheitsdiensten, die er bewertet, in keinerlei Verbindung steht.***

3. ***Eine Stelle, die einem Wirtschaftsverband oder einem Fachverband angehört und die IKT-Produkte, -Dienste und -Prozesse oder verwaltete Sicherheitsdienste 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 und -Prozesses oder verwalteten Sicherheitsdienstes 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, Bereitstellung, Vermarktung, Installation, Verwendung oder Instandsetzung dieser IKT-Produkte, -Dienste und -Prozesse oder verwalteten Sicherheitsdienste 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, alle 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 und -Prozessen oder verwalteten Sicherheitsdiensten 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 und -Prozesse oder verwalteten Sicherheitsdienste 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. Mit Ausnahme von Nummer 16 schließen die Anforderungen dieses Anhangs den

Austausch von technischen Informationen und regulatorischen Leitlinien zwischen einer Konformitätsbewertungsstelle und einer Person, die eine Zertifizierung beantragt oder deren Beantragung in Erwägung zieht, nicht 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 von 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 und -Prozessen oder verwalteten Sicherheitsdiensten 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.

Or. en