EUROPÄISCHE
KOMMISSION

Straßburg, den 18.4.2023
COM(2023) 208 final

2023/0108 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

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

(Text von Bedeutung für den EWR)

BEGRÜNDUNG

1. KONTEXT DES VORSCHLAGS

• Gründe und Ziele des Vorschlags

Diese Begründung ist dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) 2019/881[1] im Hinblick auf verwaltete Sicherheitsdienste beigefügt.

Die vorgeschlagene gezielte Änderung soll es der Kommission ermöglichen, im Wege von Durchführungsrechtsakten europäische Systeme für die Cybersicherheitszertifizierung für „verwaltete Sicherheitsdienste“ einzuführen, und zwar zusätzlich zu denen für IKT-Produkte, -Dienste und -Prozesse, die bereits unter den Rechtsakt zur Cybersicherheit fallen. Verwaltete Sicherheitsdienste spielen eine immer größere Rolle bei der Verhütung und Eindämmung von Cybersicherheitsvorfällen.

In seinen Schlussfolgerungen vom 23. Mai 2022 zur Entwicklung der Cyberabwehr der Europäischen Union[2] forderte der Rat die Union und ihre Mitgliedstaaten auf, ihre Bemühungen um die Erhöhung des allgemeinen Cybersicherheitsniveaus zu verstärken, indem beispielsweise vertrauenswürdige Anbieter von Cybersicherheitsdiensten gefördert werden, und betonte, dass es eine Priorität der Industriepolitik der EU im Bereich Cybersicherheit sein sollte, die Etablierung solcher Anbieter zu fördern. Ferner ersuchte er die Kommission, Optionen vorzuschlagen, um die Herausbildung einer Branche für vertrauenswürdige Cybersicherheitsdienste zu fördern. Die Zertifizierung verwalteter Sicherheitsdienste ist ein wirksames Mittel, um Vertrauen in die Qualität solcher Dienste aufzubauen und dadurch das Entstehen einer europäischen Branche für vertrauenswürdige Cybersicherheitsdienste zu erleichtern.

In der Gemeinsamen Mitteilung der Kommission und des Hohen Vertreters vom 10. November 2022 zur EU-Cyberabwehrpolitik[3] wurde angekündigt, dass die Kommission die Entwicklung von Systemen für die Cybersicherheitszertifizierung auf EU-Ebene für die Cybersicherheitsbranche und für private Unternehmen prüfen werde. Die Anbieter verwalteter Sicherheitsdienste werden auch eine wichtige Rolle im Hinblick auf die EU-Cybersicherheitsreserve spielen, deren schrittweiser Aufbau durch das parallel zu dieser Verordnung vorgeschlagene Cybersolidaritätsgesetz unterstützt wird. Die EU-Cybersicherheitsreserve soll eingesetzt werden, um die Reaktion und sofortige Wiederherstellung im Falle von schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes zu unterstützen. Die im Cybersolidaritätsgesetz genannten einschlägigen Cybersicherheitsdienste, die von „vertrauenswürdigen Anbietern“ erbracht werden, entsprechen den „verwalteten Sicherheitsdiensten“ im vorliegenden Vorschlag.

Einige Mitgliedstaaten haben bereits mit der Einführung von Zertifizierungssystemen für verwaltete Sicherheitsdienste begonnen. Daher besteht zunehmend die Gefahr einer Fragmentierung des Binnenmarkts für verwaltete Sicherheitsdienste, wenn in der Union uneinheitliche Systeme für die Cybersicherheitszertifizierung eingeführt werden. Der

---

1 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).

2 Dok. 9364/22.

3 JOIN(2022) 49 final.

vorliegende Vorschlag ermöglicht die Schaffung europäischer Systeme für die Cybersicherheitszertifizierung solcher Dienste, womit eine solche Fragmentierung verhindert werden soll.

- **Kohärenz mit den bestehenden Vorschriften in diesem Politikbereich**

Dieser Vorschlag steht im Einklang mit dem Rechtsakt zur Cybersicherheit, der durch diesen Vorschlag geändert werden soll. Er beruht auf den Bestimmungen dieser Verordnung und passt diese so an, dass auch verwaltete Sicherheitsdienste einbezogen werden. Die vorgeschlagenen Änderungen sind auf das absolut Notwendige beschränkt und verändern weder die Merkmale noch das Funktionieren des Rechtsakts zur Cybersicherheit.

Der Vorschlag steht auch im Einklang mit der 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)[4]. Nach der Richtlinie (EU) 2022/2555 gelten Anbieter verwalteter Sicherheitsdienste als wesentliche oder wichtige Einrichtungen, die zu einem Sektor mit hoher Kritikalität gehören. Nach Erwägungsgrund 86 dieser 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.

Der vorliegende Vorschlag zielt darauf ab, die Qualität der verwalteten Sicherheitsdienste und ihre Vergleichbarkeit zu verbessern. Dadurch soll er wesentliche und wichtige Einrichtungen in die Lage versetzen, ihre Anbieter verwalteter Sicherheitsdienste mit der in der Richtlinie (EU) 2022/2555 geforderten erhöhten Sorgfalt auszuwählen. Ferner ist die Begriffsbestimmung der „verwalteten Sicherheitsdienste“ in diesem Vorschlag von der Begriffsbestimmung des „Anbieters verwalteter Sicherheitsdienste“ in der Richtlinie (EU) 2022/2555 abgeleitet und ihr daher sehr ähnlich. Aus diesen Gründen ergänzt dieser Vorschlag in hohem Maße die NIS-2-Richtlinie.

Schließlich ergänzt dieser Vorschlag auch das vorgeschlagene Cybersolidaritätsgesetz. Mit dem vorgeschlagenen Cybersolidaritätsgesetz wird ein Verfahren zur Auswahl der Anbieter für die Bildung einer EU-Cybersicherheitsreserve festgelegt, bei dem unter anderem zu berücksichtigen ist, ob diese Anbieter eine europäische oder nationale Cybersicherheitszertifizierung erhalten haben. Künftige Zertifizierungssysteme für verwaltete Sicherheitsdienste werden somit eine wichtige Rolle bei der Umsetzung des Cybersolidaritätsgesetzes spielen.

[4] ABl. L 333 vom 27.12.2022, S. 80.

- **Kohärenz mit der Politik der Union in anderen Bereichen**

Der vorliegende Vorschlag berührt nicht die Vereinbarkeit des Rechtsakts zur Cybersicherheit mit der Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung, im Folgenden „DSGVO“)[5] und ihren Bestimmungen über die Einführung von Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen zum Nachweis der Einhaltung der genannten Verordnung bei Verarbeitungsvorgängen durch Verantwortliche und Auftragsverarbeiter. Der Rechtsakt zur Cybersicherheit lässt die Zertifizierung von Datenverarbeitungsvorgängen, die unter die Datenschutz-Grundverordnung fallen, auch wenn solche Vorgänge in Produkte und Dienste eingebettet sind, unberührt.

Darüber hinaus berührt der vorliegende Vorschlag auch nicht die Vereinbarkeit des Rechtsakts zur Cybersicherheit mit der Verordnung (EG) Nr. 765/2008 über Akkreditierung und Marktüberwachung[6], insbesondere in Bezug auf den Rahmen für die nationalen Akkreditierungsstellen und Konformitätsbewertungsstellen sowie die nationalen Aufsichtsbehörden für die Zertifizierung.

2. RECHTSGRUNDLAGE, SUBSIDIARITÄT UND VERHÄLTNISMÄßIGKEIT

- **Rechtsgrundlage**

Dieser Vorschlag bezweckt die Änderung des Rechtsakts zur Cybersicherheit, der auf Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) beruht. Wie schon der Rechtsakt zur Cybersicherheit zielt dieser Vorschlag darauf ab, eine Fragmentierung des Binnenmarkts zu verhindern, insbesondere indem die Einführung europäischer Systeme für die Cybersicherheitszertifizierung nun auch für verwaltete Sicherheitsdienste ermöglicht wird. Die Mitgliedstaaten haben damit begonnen, nationale Zertifizierungssysteme für verwaltete Sicherheitsdienste einzuführen. Daher besteht die konkrete Gefahr einer Fragmentierung des Binnenmarkts für diese Dienste, der mit dem vorliegenden Vorschlag begegnet werden soll. Deshalb ist Artikel 114 AEUV die einschlägige Rechtsgrundlage für diese Initiative.

- **Subsidiarität (bei nicht ausschließlicher Zuständigkeit)**

Das Ziel, für verwaltete Sicherheitsdienste die Einführung europäischer Systeme für die Cybersicherheitszertifizierung zu ermöglichen und so eine Fragmentierung des Binnenmarkts zu vermeiden, kann nicht auf nationaler Ebene, sondern nur auf Unionsebene erreicht werden. Darüber hinaus werden verwaltete Sicherheitsdienste, die Gegenstand der vorgeschlagenen Änderungen sind, von Anbietern erbracht, die – ebenso wie ihre größten potenziellen Kunden – unionsweit tätig sind. Ein Vorgehen auf Unionsebene ist daher sowohl notwendig als auch wirksamer als Maßnahmen auf nationaler Ebene.

- **Verhältnismäßigkeit**

Bei diesem Vorschlag handelt es sich um eine gezielte Änderung des Rechtsakts zur Cybersicherheit. Er bleibt auf das unbedingt erforderliche Maß zur Erreichung seines Ziels beschränkt, nämlich die Einführung europäischer Systeme für die Cybersicherheitszertifizierung für verwaltete Sicherheitsdienste zusätzlich zur Zertifizierung von IKT-Produkten, -Diensten und -Prozessen zu ermöglichen. Mit den vorgeschlagenen Änderungen wird insbesondere der Anwendungsbereich des europäischen Rahmens für die Cybersicherheitszertifizierung dahin gehend angepasst, dass „verwaltete Sicherheitsdienste“

[5] ABl. L 119 vom 4.5.2016, S. 1.
[6] ABl. L 218 vom 13.8.2008, S. 30.

darin einbezogen werden, dass eine Begriffsbestimmung dieser Dienste im Einklang mit der NIS-2-Richtlinie eingeführt wird und dass die Sicherheitsziele der europäischen Cybersicherheitszertifizierung geändert werden, um sie an „verwaltete Sicherheitsdienste“ anzupassen. Die übrigen Änderungen sind technischer Art und sollen sicherstellen, dass die einschlägigen Artikel auch für „verwaltete Sicherheitsdienste“ gelten. Die vorgeschlagene Initiative steht somit in einem angemessenen Verhältnis zum angestrebten Ziel.

- **Wahl des Instruments**

Da mit dem Vorschlag die Verordnung (EU) 2019/881 geändert wird, ist eine Verordnung das geeignete Rechtsinstrument.

3. ERGEBNISSE DER EX-POST-BEWERTUNG, DER KONSULTATION DER INTERESSENTRÄGER UND DER FOLGENABSCHÄTZUNG

- **Ex-post-Bewertung/Eignungsprüfungen bestehender Rechtsvorschriften**

Entfällt.

- **Konsultation der Interessenträger**

Es wurden gezielte Konsultationen mit den Mitgliedstaaten und der ENISA durchgeführt. In diesen Konsultationen erläuterten die Mitgliedstaaten ihre derzeitigen Tätigkeiten und ihre Ansichten in Bezug auf die Zertifizierung verwalteter Sicherheitsdienste. Die ENISA hat ihre Ansichten und ihre Schlussfolgerungen aus Gesprächen mit den Mitgliedstaaten und mit Interessenträgern dargelegt. Diese Stellungnahmen und Informationen der Mitgliedstaaten und der ENISA sind in diesen Vorschlag eingeflossen.

- **Einholung und Nutzung von Expertenwissen**

Entfällt.

- **Folgenabschätzung**

Es wurde eine Befreiung von der Durchführung einer Folgenabschätzung beantragt, da es sich bei dem Vorschlag um eine sehr begrenzte und gezielte Änderung des Rechtsakts zur Cybersicherheit handelt. Dadurch würde die Kommission dazu ermächtigt, im Wege von Durchführungsrechtsakten Systeme für die Cybersicherheitszertifizierung für „verwaltete Sicherheitsdienste“ einzuführen, und zwar zusätzlich zu denen für IKT-Produkte, -Dienste und -Prozesse, die bereits unter den Rechtsakt zur Cybersicherheit fallen. Die Änderung würde jedoch erst dann Wirkung zeigen, wenn solche Zertifizierungssysteme zu einem späteren Zeitpunkt angenommen werden. Außerdem würde die Änderung nichts am freiwilligen Charakter der Zertifizierungssysteme ändern.

- **Effizienz der Rechtsetzung und Vereinfachung**

Entfällt.

- **Grundrechte**

Der Vorschlag hat keine absehbaren Auswirkungen auf den Schutz der Grundrechte.

4. AUSWIRKUNGEN AUF DEN HAUSHALT

Keine.

5. WEITERE ANGABEN

- **Durchführungspläne sowie Monitoring-, Bewertungs- und Berichterstattungsmodalitäten**

Die Bestimmungen, die durch den Vorschlag geändert werden sollen, werden im Rahmen der regelmäßigen Bewertung des Rechtsakts zur Cybersicherheit bewertet, die die Kommission gemäß Artikel 67 des Rechtsakts zur Cybersicherheit durchzuführen hat. Diese Bewertung erstreckt sich u. a. auch auf die Wirkung, Wirksamkeit und Effizienz der Bestimmungen über den Zertifizierungsrahmen für die Cybersicherheit im Hinblick auf die Ziele, ein angemessenes Maß an Cybersicherheit für IKT-Produkte, -Dienste und -Prozesse in der Union und einen besser funktionierenden Binnenmarkt zu gewährleisten. Der Vorschlag enthält eine Änderung, mit der sichergestellt wird, dass die Bewertung auch die verwalteten Sicherheitsdienste erfasst. Überdies übermittelt die Kommission dem Europäischen Parlament, dem Rat und dem Verwaltungsrat der ENISA einen Bericht über die Bewertung und ihre Schlussfolgerungen und veröffentlicht die Ergebnisse des Berichts.

- **Ausführliche Erläuterung einzelner Bestimmungen des Vorschlags**

Der Vorschlag umfasst zwei Artikel. Artikel 1 betrifft die Änderungen an der Verordnung (EU) 2019/881 und Artikel 2 regelt das Inkrafttreten. Artikel 1 enthält gezielte Änderungen, um den Anwendungsbereich des europäischen Rahmens für die Cybersicherheitszertifizierung im Rechtsakt zur Cybersicherheit dahin gehend zu ändern, dass auch „verwaltete Sicherheitsdienste“ darin einbezogen werden (Artikel 1 und Artikel 46 des Rechtsakts zur Cybersicherheit). Es wird eine Begriffsbestimmung dieser Dienste eingeführt, die sehr eng an die Begriffsbestimmung des „Anbieters verwalteter Sicherheitsdienste“ in der NIS-2-Richtlinie (Artikel 2 des Rechtsakts zur Cybersicherheit) angelehnt ist. Außerdem wird ein neuer Artikel 51a über die Sicherheitsziele der europäischen Cybersicherheitszertifizierung eingefügt, die auf „verwaltete Sicherheitsdienste“ abgestimmt sind. Schließlich enthält der Vorschlag auch eine Reihe technischer Änderungen, um sicherzustellen, dass die einschlägigen Artikel auch für „verwaltete Sicherheitsdienste“ gelten.

2023/0108 (COD)

Vorschlag für eine

VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES

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,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses,

nach Stellungnahme des Ausschusses der Regionen,

gemäß dem ordentlichen Gesetzgebungsverfahren,

in Erwägung nachstehender Gründe:

(1) Durch die Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates[7] wird ein Rahmen für die Schaffung europäischer Systeme für die Cybersicherheitszertifizierung eingeführt, um für IKT-Produkte, -Dienste und -Prozesse in der Union ein angemessenes Maß an Cybersicherheit zu gewährleisten und eine Fragmentierung des Binnenmarkts für Zertifizierungssysteme in der Union zu verhindern.

(2) Verwaltete Sicherheitsdienste, d. h. Dienste, die in der Durchführung oder Unterstützung von Tätigkeiten im Zusammenhang mit dem Cybersicherheitsrisikomanagement ihrer Kunden bestehen, haben bei der Verhütung und Eindämmung von Cybersicherheitsvorfällen an Bedeutung gewonnen. Dementsprechend gelten die Anbieter dieser Dienste gemäß der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates[8] als wesentliche oder wichtige Einrichtungen, die zu einem Sektor mit hoher Kritikalität gehören. Nach Erwägungsgrund 86 dieser Richtlinie spielen die Anbieter verwalteter Sicherheitsdienste in Bereichen wie Reaktion auf Sicherheitsvorfälle, Penetrationstests, Sicherheitsaudits und Beratung eine überaus wichtige Rolle, indem

[7] 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).

[8] 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).

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.

(3) Die Anbieter verwalteter Sicherheitsdienste spielen auch eine wichtige Rolle im Hinblick auf die EU-Cybersicherheitsreserve, deren schrittweiser Aufbau durch die Verordnung (EU) …/… [über Maßnahmen zur Stärkung der Solidarität und der Kapazitäten in der Union für die Erkennung, Vorsorge und Bewältigung von Cybersicherheitsbedrohungen und -vorfällen] unterstützt wird. Die EU-Cybersicherheitsreserve soll eingesetzt werden, um die Reaktion und sofortige Wiederherstellung im Falle von schwerwiegenden Cybersicherheitsvorfällen und Cybersicherheitsvorfällen großen Ausmaßes zu unterstützen. In der Verordnung (EU) …/… [über Maßnahmen zur Stärkung der Solidarität und der Kapazitäten in der Union für die Erkennung, Vorsorge und Bewältigung von Cybersicherheitsbedrohungen und -vorfällen] wird ein Verfahren zur Auswahl der Anbieter für die Bildung der EU-Cybersicherheitsreserve festgelegt, bei dem unter anderem zu berücksichtigen ist, ob der betreffende Anbieter eine europäische oder nationale Cybersicherheitszertifizierung erhalten hat. Die einschlägigen Dienste, die von „vertrauenswürdigen Anbietern“ gemäß der Verordnung (EU) …/… [über Maßnahmen zur Stärkung der Solidarität und der Kapazitäten in der Union für die Erkennung, Vorsorge und Bewältigung von Cybersicherheitsbedrohungen und -vorfällen] erbracht werden, entsprechen den „verwalteten Sicherheitsdiensten“ gemäß der vorliegenden Verordnung.

(4) 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 benutzen 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 vermeiden. Diese Verordnung zielt daher darauf ab, das Funktionieren des Binnenmarkts zu verbessern.

(5) 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 einem Zertifizierungssystem erfasst werden können, ist es daher erforderlich, die Verordnung (EU) 2019/881 zu ändern.

Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 42 Absatz 1 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates angehört und hat am [DD.MM.JJJJ] eine Stellungnahme abgegeben —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

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 Zertifizierungssysteme 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 Dienst, der in der Durchführung oder Unterstützung von Tätigkeiten im Zusammenhang mit dem Cybersicherheitsrisikomanagement besteht und unter anderem die Reaktion auf Sicherheitsvorfälle sowie Penetrationstests, Sicherheitsaudits und Beratung 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 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 Cybersicherheitszertifizierungsrahmens 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 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) Der europäische Zertifizierungsrahmen für die Cybersicherheit legt einen Mechanismus fest, 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, Funktionen oder Diensten, 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 sehr hohen 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, oder bestimmter Kategorien davon, oder verwalteter Sicherheitsdienste in das fortlaufende Arbeitsprogramm der Union 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 verwalteten Sicherheitsdiensten, 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 Systems durch die Europäische Gruppe für die Cybersicherheitszertifizierung.“

7. Artikel 49 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, 52 und 54 erfüllen, ein europäisches System für die Cybersicherheitszertifizierung festgelegt wird. Diese Durchführungsrechtsakte werden nach dem in Artikel 66 Absatz 2 genannten Prüfverfahren erlassen.“

8. 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:“

9. 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 sehr hohes 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 sehr hoher 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 [und die Hardware], die zur Erbringung der verwalteten Sicherheitsdienste eingesetzt werden, sind durch Voreinstellungen und Technikgestaltung sicher, weisen keine bekannten Sicherheitslücken auf und enthalten die neuesten Sicherheitsaktualisierungen.“

10. 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“ und/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.“

11. 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.“

12. 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;“

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;“

13. 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 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 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 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.“

14. 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.“

15. 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.“

16. 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;“

17. 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 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.“

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 Straßburg am […]

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